Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακάκαι Επικοινωνιακά Συστήματα

Τεχνικές Ανάλυσης Ψηφιακών Πειστηρίων

Ανδρέας Αγιώτης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Αύγουστος2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Τεχνικές Ανάλυσης Ψηφιακών Πειστηρίων

Ανδρέας Αγιώτης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

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

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Αύγουστος2014

Περίληψη

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάζονται θέματα διαδικαστικά, νομικά και τεχνικά που αφορούν στη διαδικασία λήψης των ψηφιακών πειστηρίων με σκοπό, είτε την παρουσίασή τους στο δικαστήριο, είτε την άντληση πληροφοριών. Αρχικά αναφέρονται βασικές έννοιες και ένα σύντομο ιστορικό της επιστήμης της ψηφιακής δικανικής με σκοπό να γίνει πιο κατανοητή η διαδικασία λήψης τους που ακολουθείται, καθώς και τα νομικά θέματα που τη διέπουν. Ακολουθεί σύντομη αναφορά στην ψηφιακή δικανική στον κυβερνοπόλεμο και περιεκτική ανάλυση των τριών κλάδων της. Τέλος παρουσιάζονται εργαλεία που έχουν αναπτυχθεί για λήψη και ανάλυση των ψηφιακών πειστηρίων με τρόπο που να αναδεικνύεται η συμβολή τους στο έργο των ερευνητών σε αυτή την πολύπλοκη και χρονοβόρα διαδικασία.

Επιπλέον παρουσιάζονται προβλήματα και δυσχέρειες που δημιουργούνται από το νομικό καθεστώς που διέπει την Κυπριακή και Ευρωπαϊκή νομοθεσία, από την εξέλιξη της επιστήμης της πληροφορικής με τη συνεχή αναβάθμιση των συσκευών, αλλά και των κακόβουλων πρακτικών που ακολουθούνται.

Summary

In this thesis, procedural, legal and technical issues are presented that concern the process of collecting digital evidence, with the purpose either to present them in court, or to extract information. Initially, basic concepts and a brief historical background regarding the field of digital forensics are mentioned, in order to obtain a better understanding on the procedures followed for their collection, as well as on the legal issues governing them. Thereinafter, a brief reference is included concerning the issue of digital forensics in the field of cyber security, with a comprehensive analysis of the three respective branches. Finally, specific tools are presented that have been developed for the purpose of acquiring and analysing digital evidence, in a manner that underlines their contribution to the work of researchers, within this complex and time - consuming process.

Moreover, existent problems and difficulties are underlined, which emerge from the legal status quo in Cypriot and European Legislation, the evolution of computer science with the continuous upgrading of equipment and the malicious practices followed.

Ευχαριστίες

Ευχαριστώ θερμά τον Επιβλέποντα καθηγητή Δρ. Λιμνιώτη Κωνσταντίνο για τη σημαντική βοήθεια και καθοδήγησή του καθ' όλη τη διάρκεια της εκπόνησης της παρούσας μεταπτυχιακής διατριβής και την οικογένειά μου για την πολύτιμη συμπαράστασή της.

Ιδιαίτερες ευχαριστίες στο τμήμα Ψηφιακής Δικανικής της Κυπριακής Αστυνομίας για την πολύτιμη βοήθεια που προσέφερε με την επίλυση απορριών ως προς τα νομικά θέματα και την επίδειξη εργαλείων.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Την τελευταία δεκαετία διαφαίνεται όλο και περισσότερο η ανάγκη για επαρκή ασφάλεια ενός οργανισμού σε κακόβουλες επιθέσεις. Παρόλα αυτά η εξέλιξη των τρόπων δράσης, η αφοσίωση στον σκοπό και η πρωτοβουλία κινήσεων που έχουν οι κακόβουλοι καθιστούν τα ολοένα αυξημένα μέτρα ασφαλείας του οργανισμού μη επαρκή σε αρκετές περιπτώσεις. Σε αυτό το ζήτημα τα συστήματα ασφαλείας, η εκπαίδευση των χρηστών και διαχειριστών, καθώς και τα συστήματα ανίχνευσης και πρόληψης επιθέσεων δεν μπορούν ν' απαντήσουν και οι ερευνητές καλούνται να καταγράψουν, ερευνήσουν και αναλύσουν τα ψηφιακά ίχνη – πειστήρια που άφησε ο κακόβουλος με σκοπό να αποδειχθεί η υπαιτιότητα μιας δραστηριότητας και να εντοπισθεί ο ύποπτος πέραν κάθε αμφιβολίας [07].

Η ανάλυση των ψηφιακών πειστηρίων είναι αναγκαίο μέσο αντίδρασης ενάντια σε μια επιτυχημένη επίθεση από έναν κακόβουλο που έχει καταφέρει να παρακάμψει όλα τα συστήματα ασφαλείας ενός οργανισμού και ίσως ο μοναδικός αποτρεπτικός παράγοντας για κακόβουλους που γνωρίζουν ότι υπάρχει αυτή η δυνατότητα. Το να μπορεί ένας οργανισμός να εντοπίσει και να οδηγήσει ενώπιον της δικαιοσύνης τον ύποπτο μιας κακόβουλης επίθεσης, σε συνδυασμό με τα υπόλοιπα προληπτικά μέτρα ασφαλείας που λαμβάνει, ολοκληρώνει το φάσμα

των μέτρων προστασίας που μπορεί να λάβει και δίνει το μήνυμα ότι κανείς δε μπορεί να προκαλεί ζημιά χωρίς επιπτώσεις.

Οι ηλεκτρονικές απάτες και τα ηλεκτρονικά εγκλήματα έχουν συνεχή αύξηση και δυστυχώς ποσοστό λιγότερο του 2% από τις αναφερόμενες υποθέσεις καταλήγουν στη δικαιοσύνη και αυτό οφείλεται κυρίως στη μεθοδολογία που ακολουθείται [01]. Το γεγονός αυτό αναδεικνύει την αυξανόμενη ανάγκη για συλλογή και ανάλυση ψηφιακών πειστηρίων, που αναγάγει τους ερευνητές σε λήπτες αποφάσεων από χειριστές εργαλείων, κάτι το οποίο συνεπάγεται και αύξηση στην ποιότητα παροχής υπηρεσιών προς τους οργανισμούς [03].

1.1 Τι είναι η Ψηφιακή Δικανική

Ο ορισμός της ψηφιακής δικανικής όπως διαμορφώθηκε στο πρώτο DigitalForensicsResearchWorkshop (DFRWS) το 2001 και συνεχίζει να παραμένει σχετικός ακόμα και σήμερα είναι : Η χρήση επιστημονικά εξαγμένων και αποδεδειγμένων μεθόδων προς τη διατήρηση, συλλογή, αξιολόγηση, αναγνώριση, ανάλυση, ερμηνεία, καταγραφή και παρουσίαση των ψηφιακών πειστηρίων που εξάγονται από ψηφιακές πηγές με σκοπό τη διευκόλυνση ή την προώθηση ανακατασκευής συμβάντων που φέρονται να είναι εγκληματικά, ή υποβοηθούν στην πρόληψη μη εξουσιοδοτημένων ενεργειών που αποδιοργανώνουν τον αρχικό σχεδιασμό [15].

1.2. Αρχές Ψηφιακής Δικανικής

Το δόγμα που αφορά στα τεκμήρια μπορεί να απλοποιηθεί ως εξής : Το βάρος είναι στον κατήγορο να δείξει στο δικαστήριο πως τα αποδεικτικά στοιχεία που παρουσιάστηκαν είναι ακριβώς όπως λήφθηκαν αρχικά και περιήλθαν στην κατοχή του ερευνητή.

Όπου είναι δυνατόν πρέπει να λαμβάνεται εικόνα ολόκληρου του αποθηκευτικού μέσου των δεδομένων. Αν αυτό δεν είναι τεχνικά δυνατόν και ο ερευνητής πρέπει να πάρει τμήμα αυτού, τότε θα πρέπει να προσέξει να πάρει το κατάλληλο για να μπορεί να στηρίξει την υπόθεσή του. Στις ελάχιστες περιπτώσεις που θα πρέπει να εκτελέσει την ανάλυση στον ύποπτο υπολογιστή, τότε θα πρέπει να το κάνει παρουσία μαρτύρων. Είναι πολύ βασικό να δείξει αντικειμενικότητα στο δικαστήριο όπως και την ακεραιότητα των πειστηρίων που θα παρουσιάσει. Επίσης θα πρέπει να παρουσιάσει τον τρόπο με τον οποίο τα δεδομένα ανακτήθηκαν και να διατηρηθούν

έτσι ώστε όταν ένας τρίτος ακολουθήσει την ίδια διαδικασία να καταλήξει στο ίδιο αποτέλεσμα. Οι γενικές αρχές που διέπουν την ψηφιακή δικανική σύμφωνα με το ISO 27037/2012 είναι οι παρακάτω [21,22,46]:

1. Καμία ενέργεια δεν πρέπει να προκαλεί αλλαγές στα δεδομένα που βρίσκονται σε έναν υπολογιστή ή αποθηκευτικό μέσο στα οποία μετά θα βασιστεί στο δικαστήριο.

2. Σε ειδικές περιπτώσεις που η προσπέλαση σε αυθεντικά δεδομένα είναι υποχρεωτική, τότε το πρόσωπο που θα το κάνει πρέπει να είναι αρμόδιο και να είναι σε θέση να δώσει στοιχεία δίνοντας εξηγήσεις για το πόσο σχετικά είναι με την υπόθεση και τις επιπτώσεις της ενέργειάς του.

3. Όλες οι ενέργειες που έγιναν στα ηλεκτρονικά μέσα που τέθηκαν προς εξέταση πρέπει να καταγράφονται επ' ακριβώς και σε περίπτωση που κάποιος τρίτος ακολουθήσει ακριβώς τα ίδια βήματα θα πρέπει να εξάγει το ίδιο αποτέλεσμα.

4. Ο επικεφαλής της έρευνας έχει την πλήρη ευθύνη για να εξασφαλίσει την πιστή τήρηση του νόμου και τις αρχές που τον διέπουν.

1.3. Ιστορική Αναδρομή

Η ψηφιακή δικανική δεν είναι κάτι άλλο, παρά ένας κλάδος της δικανικής. Ακολουθεί τις ίδιες επιστημονικές μεθόδους όπως κι οι υπόλοιποι κλάδοι κάτι το οποίο την κάνει μια εξέλιξη της τεχνικής για καταπολέμηση του εγκλήματος.

Σαν κλάδος έχει κάνει τα αρχικά του βήματα από τη δεκαετία του 70 όπου οι πρώτες υποθέσεις που εμπλέκονταν υπολογιστές είχαν σχέση με οικονομικές απάτες στο μεγαλύτερο ποσοστό. Στα πρώτα της βήματα πραγματοποιούταν από επαγγελματίες στους ηλεκτρονικούς υπολογιστές οι οποίοι εργάζονταν με τα όργανα επιβολής του νόμου σε ad-hocπεριπτώσεις. Στη δεκαετία του 80 σε ορισμένες υποθέσεις όλα τα στοιχεία βρίσκονταν μόνο σε υπολογιστές. Εκείνη την εποχή δημιουργήθηκε και το πρώτο εργαλείο από τη NortonUtilities το "Un-erase". Δεν υπήρχε και μεγάλη ανάγκη για διεξαγωγή ψηφιακής δικανικής λόγω του ότι τα στοιχεία πολύ συχνά συλλέγονταν χωρίς την ανάγκη χρήσης εργαλείων, καθώς οι δίσκοι ήταν πολύ μικρής χωρητικότητας και πολλοί δράστες έκαναν μεγάλες εκτυπώσεις.

Η πρώτη επίσημα οργανωμένη προσπάθεια έγινε το 1984 από το FBI με τη δημιουργία του FBI MagneticMediaProgram, με μόνο 3 εξετάσεις την πρώτη χρονιά, το οποίο αργότερα μετατράπηκε σε ComputerAnalysisandRespondTeam (CART) το οποίο υπάρχει και σήμερα. Το 1987 δημιουργήθηκε η εταιρεία Access Data η οποία ήταν η πρώτη με αποκλειστική ενασχόληση που αφορούσε στην ψηφιακή δικανική.

Ο πρώτος διεθνής οργανισμός δημιουργήθηκε το 1995 και ήταν ο InternationalOrganizationonComputerEvidence (IOCE) και μόλις το 1997 οι G8 στη Μόσχα δήλωσαν ότι τα όργανα επιβολής του νόμου πρέπει να εκπαιδευτούν και να εξοπλιστούν για την αντιμετώπιση τέτοιου είδους εγκλημάτων. Το Μάρτιο του 1998 οι G8 όρισαν τον IOCE να δημιουργήσει διεθνείς αρχές, οδηγίες – κατευθύνσεις και διαδικασίες σχετικές με τα ψηφιακά πειστήρια.

Η οκταετία μεταξύ 1999 – 2007 ήταν η χρυσή εποχή για την ψηφιακή δικανική. Έκανε δυνατό το «πάγωμα» του χρόνου και την εξιχνίαση εγκλημάτων αρκετούς μήνες μετά την εκτέλεσή τους. Χαρακτηριζόταν από την εξάπλωση των windowsXP, τη μικρή σχετικά ποικιλία διαμόρφωσης αρχείων, περιορισμένη αξιοποίηση δικτύων στο εσωτερικό των οργανισμών και εργαλεία που ήταν ικανοποιητικά για την επαναφορά αρχείων από διάφορους κατασκευαστές. Τα εργαλεία αυτά επέτρεπαν σε κάποιον με σχετικά περιορισμένη εκπαίδευση να μπορεί να εκτελέσει βασική ανάλυση αρχείων [06].

Παρά το γεγονός ότι η εξέλιξη του κλάδου φαίνεται αργή, στην πραγματικότητα ήταν πολύ γρήγορη λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας, τη ραγδαία αύξηση των διεπαφών και τις νέες μορφές εγκλημάτων που παρουσιάζονταν καθημερινά τα οποία για τις αρμόδιες αρχές ήταν πρωτόγνωρα χωρίς καμιά προηγούμενη εμπειρία. Αυτή η ταχεία εξέλιξη είχε ως αποτέλεσμα την έλλειψη τυποποίησης και εκπαίδευσης.

Για να αντιμετωπιστεί αυτή η έλλειψη πολλοί οργανισμοί άρχισαν να εκδίδουν δικούς τους οδηγούς στην αρχή της δεκαετίας του 2000 και το 2005 εκδόθηκε το ISO 17025 (Generalrequirementsforthecompetence of testingandcalibrationlaboratories). Ένα χρόνο νωρίτερα υπογράφτηκε από 43 κράτη η Σύμβαση του Συμβουλίου της Ευρώπης κατά του Εγκλήματος μέσω Διαδικτύου (ΣΣΕΕΔ), στο οποίο βασίζεται και η σχετική νομοθεσία της Κυπριακής Δημοκρατίας. Ταυτόχρονα δόθηκε σημασία στην εκπαίδευση και στην πιστοποίηση κυρίως από εμπορικές εταιρείες που ειδικεύονται στην παραγωγή σχετικού λογισμικού.

Σήμερα η ψηφιακή Δικανική έχει φτάσει πλέον στο σημείο όπου είναι λιγότερο τέχνη και περισσότερο επαναλαμβανόμενες και καλά καταγραμμένες επιστημονικές διαδικασίες [15]. Απότο 2012 έχειεκδοθείτοδιεθνέςπρότυπο ISO/IEC 27037 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.

1.4. Χαρακτηριστικά Ψηφιακών Τεκμηρίων

Τα χαρακτηριστικά που θα πρέπει να πληροί ένα ψηφιακό τεκμήριο για να μπορεί να χρησιμοποιηθεί σε μια υπόθεση στο δικαστήριο δε διαφέρουν από τα χαρακτηριστικά των υπολοίπων τύπων τεκμηρίων και είναι τα παρακάτω :

1.4.1. Αποδεκτό

Για να είναι αποδεκτό ένα τεκμήριο πρέπει να ακολουθεί κάποιους πολύπλοκους κανόνες με πολλές εξαιρέσεις, βάσει του νομικού συστήματος, ανεξαρτήτως του είδους της υπόθεσης. Η διαφορά που υπάρχει στα ψηφιακά πειστήρια είναι ότι πέραν των εν λόγω κανόνων, που δεν αναφέρονται στη συγκεκριμένη μελέτη λόγω του ότι δεν είναι ο σκοπός της, δεν πρέπει να είναι προϊόν υποκλοπής ή οποιοδήποτε είδος επικοινωνίας του υπόπτου οι οποίες προφυλάσσονται απόλυτα από το Σύνταγμα.

1.4.2. Αυθεντικό

Να συνδέεται ειδικά στο υποτιθέμενο γεγονός και φυσικά ή νομικά πρόσωπα.

1.4.3. Ακριβές

Να μην υπάρχει αμφιβολία για τη διαδικασία συλλογής, ανάλυσής και παρουσίασης του πειστηρίου στο δικαστήριο. Η μέθοδος που ακολουθήθηκε πρέπει να μπορεί να εφαρμοστεί από ανεξάρτητο εξειδικευμένο προσωπικό και να καταλήξει στο ίδιο αποτέλεσμα. Σε περίπτωση που το πειστήριο είναι κάποιο έγγραφο θα πρέπει να διατηρηθεί η ακρίβεια και των αναγραφομένων.

1.4.4. Συνοχή τεκμηρίου – Αλυσίδα Φύλαξης

Είναι η ικανότητα να αναφερθεί οτιδήποτε έγινε σε ένα πειστήριο από τη στιγμή που έγινε η συλλογή του μέχρι και τη στιγμή που παρουσιάστηκε στο δικαστήριο. Σκοπός είναι να περιοριστούν οι πιθανότητες αλλοίωσης του πειστηρίου, είτε ηθελημένα, είτε όχι ή να εντοπιστεί το πότε έγινε η οποιαδήποτε αλλοίωση [12].

Σε περιπτώσεις που αφορούν σε συσκευές, όπως υπολογιστές ή κινητά τηλέφωνα, ισχύει ότι και στα υπόλοιπα τεκμήρια, δηλαδή τοποθέτηση σε ειδική σακούλα ή ειδικά μεταλλικά κιβώτια για αποκλεισμό ασύρματων δικτύων, τοποθέτηση ετικέτας, φωτογράφηση και καταγραφή. Για τα ψηφιακά τεκμήρια όμως απαιτείται η χρήση της συνάρτησης κατακερματισμού (HashValue) όπου υπολογίζεται η τιμή αυτής επί του πρωτότυπου πειστηρίου, όσο και επί των αντιγράφων όπου θα πραγματοποιηθεί η ανάλυση. Αν οι παραγόμενες τιμές ταυτίζονται τότε αποδεικνύεται η ακεραιότητά τους. Οι συνήθεις συναρτήσεις κατακερματισμούπου χρησιμοποιούνται είναι οι MD5 που παράγει αλφαριθμητική τιμή 32 χαρακτήρων (128 bits) και ο SHA1 που παράγει αλφαριθμητική τιμή 40 χαρακτήρων (160 bits). Επειδή έχουν παρατηρηθεί περιπτώσεις να ταυτιστούν τιμές δύο διαφορετικών αρχείων που υπολογίστηκαν με τον αλγόριθμο MD5 (MD5 collision) είναι καλύτερα να γίνεται χρήση του SHA1.

Αυτό το χαρακτηριστικό έχει και ευρύτερη σημασία καθώς τα πλείστα ψηφιακά πειστήρια που παρουσιάζονται στο δικαστήριο πηγάζουν όχι από τις κατασχόμενες συσκευές, αλλά από την επεξεργασία και ανάλυση των δεδομένων τους. Πρακτικά ο αναλυτής παρουσιάζει τα αποτελέσματα της έρευνας που έκανε σε μια βάση δεδομένων, ή σε ένα αρχείο καταγραφής μιας συσκευής, ή ακόμα και στον αδιάθετο χώρο της. Βάσει αυτού συνοχή σημαίνει να είναι σε θέση να μπορεί το υλικό που παρουσιάστηκε να εντοπιστεί ακέραιο στην αρχική του μορφή στο πρωτότυπο τεκμήριο πριν να γίνει η ανάλυση και να οδηγηθεί στο ίδιο αποτέλεσμα. Έτσι εξασφαλίζεται ότι δεν έγιναν λάθη στη διαδικασία και δεν εξάχθηκαν λάθος συμπεράσματα.

1.5. Ψηφιακά Πειστήρια στην Πράξη

Όπως έχει προαναφερθεί τα ψηφιακά πειστήρια από τα παραδοσιακά δε διαφέρουν στην πραγματικότητα σε τίποτα. Έχουν την ίδια αποδεικτική αξία και ο τρόπος διαχείρισής τους δε διαφέρει σε τίποτε εκτός από το γεγονός ότι είναι πολύ πιο επιρρεπή σε καταστροφή ή αλλαγές

οι οποίες μπορούν να απαγορεύσουν την αποδοχή τους από ένα δικαστήριο. Συνήθως αποτελούνται από :

1. Περιεχόμενα ενός αρχείου, μιας βάσης δεδομένων, συλλογή ηλεκτρονικής αλληλογραφίας, ιστοσελίδες, αναφορές.

2. Μεταδεδομένα (meta-data) τα οποία είναι δεδομένα για δεδομένα τα οποία δε φαίνονται αμέσως και αφορούν, για παράδειγμα, στο ποιος δημιούργησε ένα αρχείο, πόσες φορές τροποποιήθηκε και πότε τυπώθηκε τελευταία φορά.

3. Δεδομένα καταλόγου, πληροφορίες για ένα αρχείο το οποίο είναι αποθηκευμένο σε ένα αποθηκευτικό μέσο και περιέχουν λεπτομέρειες για την ονομασία του, ημερομηνία και ώρα που προσπελάστηκε και μέγεθος.

4. Δεδομένα διαμόρφωσης, αρχεία και δεδομένα καταλόγου που βοηθούν έναν υπολογιστή ή μια εφαρμογή να συμπεριφέρεται με συγκεκριμένο τρόπο και τα οποία να παρέχουν πληροφορίες για το πότε ένας και πως ένας υπολογιστής χρησιμοποιήθηκε ή αν τροποποιήθηκαν.

5. Δεδομένα καταγραφής, αρχεία που δημιουργήθηκαν από λειτουργικά συστήματα ή εφαρμογές που είτε καταγράφουν δραστηριότητα του τύπου διαδρομής ελέγχου (audittrail) και καταγραφής πληκτρολογίου, είτε μπορούν να χρησιμοποιηθούν για αναπαραγωγή γεγονότων.

6. Υλικό από αντίγραφα ασφαλείας, αναλόγως της κατάστασης, μπορεί να είναι οτιδήποτε από τα παραπάνω, αλλά επιπλέον μπορεί να είναι και δεδομένα που έχουν συλλεχθεί από το λειτουργικό σύστημα ως τμήμα του συστήματος ανάκτησης, για παράδειγμα τα Microsoft RestorePoints.

7. Δικανικά ανακτώμενα δεδομένα, υλικό που αποκτήθηκε από μέσα αποθήκευσης το οποίο υπό κανονικές συνθήκες δε θα ήταν ορατό, όπως διαγραμμένα αρχεία, αρχεία από τον αδιάθετο χώρο, ακόμα και πρόσθετα δεδομένα.

8. Υποκλαπέντα δεδομένα, υλικό που αποκτήθηκε με τη χρήση συσκευών υποκλοπής σε μια δικτυακή ή τηλεφωνική σύνδεση (υπάρχουν νομικά θέματα που πρέπει να ελεγχθούν).

1.6 Βασικές Έννοιες

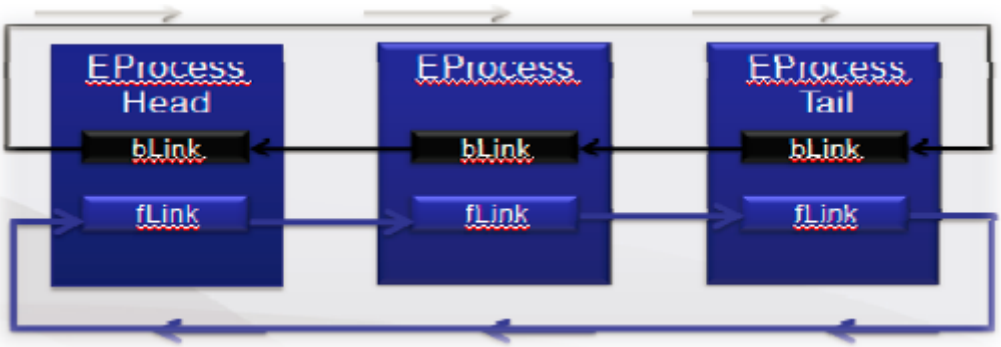
1.6.1 Πτητική Μνήμη – VolatileMemory

Πτητική μνήμη (volatilememory) είναι εκείνη η οποία "χάνει" την πληροφορία που είναι αποθηκευμένη σε αυτή, μόλις σταματήσει η παροχή ηλεκτρικής ισχύος. Στην αντίθετη περίπτωση η μνήμη είναι μη-πτητική (non-volatilememory). Για παράδειγμα, η δευτερεύουσα μνήμη είναι μη-πτητική, αφού η πληροφορία διατηρείται στους δίσκους, τα CD ROMs, τις ταινίες, ακόμη και όταν απενεργοποιήσουμε το υπολογιστικό σύστημα.

Η εκμετάλλευση της πτητικής μνήμης από τους κακόβουλους έγινε με σκοπό να μειωθούν τα ίχνη τους στους σκληρούς δίσκους των θυμάτων γνωρίζοντας ότι η πρώτη ενέργεια του ερευνητή θα ήταν το σβήσιμο του υπολογιστή.

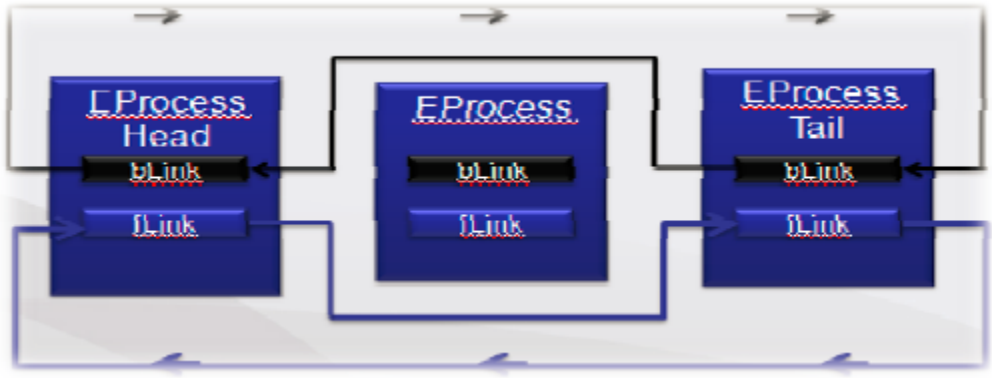
Η νέα ερευνητική προσέγγιση ξεκινά με την κατανόηση του τι εδρεύει στην πτητική μνήμη με τη χρήση εργαλείων που αναλύουν γρήγορα τη RAMκαι επιτρέπουν στον ερευνητή να την περιλάβουν ως μέρος των πειστηρίων που θα παρουσιάσουν. Ερευνητές που περιόρισαν την ανάλυσή τους σε μη πτητικά δεδομένα μόνο, όχι μόνο άφησαν πολύτιμα ψηφιακά πειστήρια πίσω, αλλά τα κατέστρεψαν ολοσχερώς με το σβήσιμο του υπολογιστή [09].

Οι διεργασίες στην πτητική μνήμη συνδέονται μεταξύ τους ως μια διπλή συνδεδεμένη λίστα. Το κακόβουλο λογισμικό φροντίζει ώστε να μην μπαίνει στη αλυσίδα των διεργασιών, παρόλο που εκτελείται κανονικά και δεν είναι δυνατόν να γίνει αντιληπτό από το λειτουργικό σύστημα, όπως για παράδειγμα από τον TaskManagerτων Windows.



Εικόνα 1.1 : Λίστα διπλά συνδεδεμένων διεργασιών με δείκτες προς την προηγούμενη και προς την επόμενη διεργασία. Όταν το λειτουργικό σύστημα λειτουργεί κανονικά οι διεργασίες και οι δείκτες τους συγκροτούν μια αλυσίδα γνωστή ως διπλή συνδεδεμένη λίστα. Αυτή η αλυσίδα είναι αποθηκευμένη στη

μνήμη και ανανεώνεται κάθε φορά που μια διεργασία ξεκινά ή τερματίζεται. Από εδώ τα Windowsξεκινούν από την κεφαλή μέχρι την ουρά και ενημερώνουν το TaskManager από όπου μπορεί να τις δει ο χρήστης [09].



Εικόνα 1.2 : Η πιο συνηθισμένη μέθοδος που χρησιμοποιείται από δημιουργούς κακόβουλου λογισμικού για να κρύβουν τις διεργασίες από τα Windows. ΗμέθοδοςείναιγνωστήωςDirectkernelObjectManipulation (DKOM) και περιλαμβάνει την αποσύνδεση μιας διεργασίας από την αλυσίδα με τη μετακίνηση του δείκτη από τη διεργασία 3 προς την 1 και από την 1 προς την 3, με αποτέλεσμα η διεργασία 2 που είναι του κακόβουλου να μην είναι πλέον μέρος της λίστας. Από τη στιγμή που δεν είναι μέρος της ο TaskManagerδε θα την παρουσιάσει παρά το ότι εκτελείται κανονικά. Με την ανάλυση της μνήμης αυτή η διεργασία μπορεί να βρεθεί και να χαρακτηριστεί ως ύποπτη για περαιτέρω έλεγχο [09].

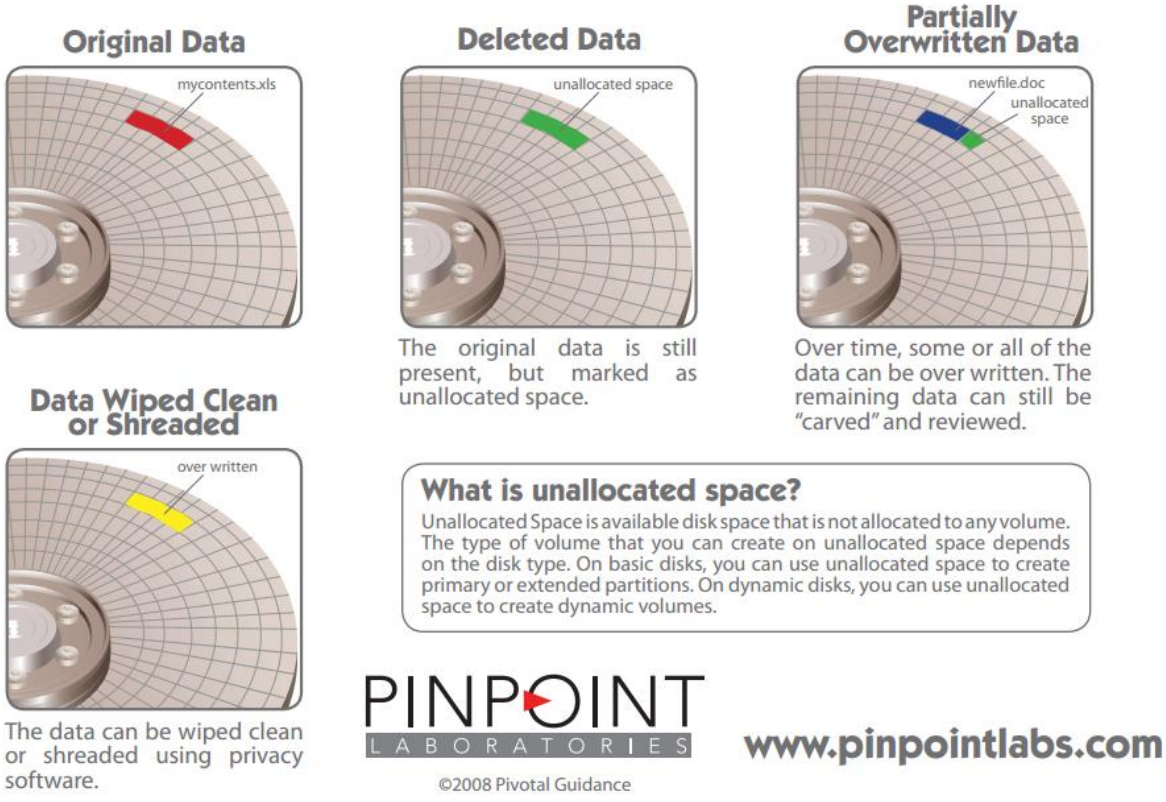
Οι πληροφορίες που μπορούν να ανακτηθούν από την ανάλυση της πτητικής μνήμης είναι οι τρέχουσες διεργασίες, δικτυακές συνδέσεις (πχ ανοικτές και κλειστές θύρες) και δεδομένα αποθηκευμένα στη μνήμη όπως κωδικοί χρηστών σε ιστοσελίδες, πληροφορίες συστήματος, συνδεδεμένους χρήστες, πληροφορίες δικτύου (ανοικτές – κλειστές θύρες, vpnσυνδέσεις) [22].

Αν τα παραπάνω ληφθούν πριν αφαιρεθεί η τροφοδοσία τότε ο ερευνητής θα έχει συλλέξει πληροφορίες οι οποίες σε συνδυασμό με το ακριβές αντίγραφο του δίσκου του υπολογιστή θα προσφέρει τις μέγιστες δυνατές πληροφορίες που θα μπορούσαν να εξασφαλιστούν.

Λαμβάνοντας υπόψη την πιθανή γραμμή υπεράσπισης ενός υπόπτου που μπορεί να επικαλεστεί κακόβουλο πρόγραμμα τύπου Δούρειου Ίππου (trojandefence), η εξέταση της πτητικής μνήμης μπορεί να βοηθήσει τον ερευνητή να υποστηρίξει, ή να αρνηθεί την ύπαρξη και τη λειτουργία ενός τέτοιου λογισμικού [22, 46].

1.6.2. Αδιάθετος Χώρος – UnallocatedSpace

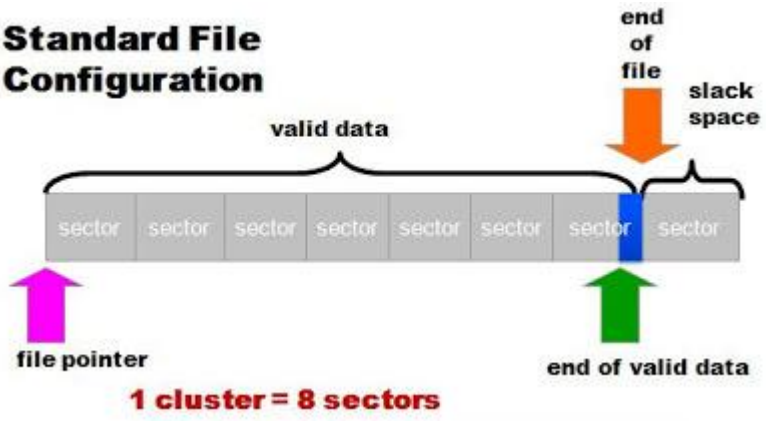
Αδιάθετος χώρος μνήμης είναι ο κενός χώρος που εμφανίζεται σε κάποιο αποθηκευτικό μέσο. Η πραγματική του σημασία είναι ότι είναι διαθέσιμος χώρος προς εγγραφή νέων δεδομένων, χωρίς να σημαίνει ότι δεν υπάρχουν παλιά δεδομένα τα οποία έχουν «διαγραφτεί». Στην πραγματικότητα όταν διαγράφονται αρχεία σε κάποιο σύστημα, αν δεν έχει χρησιμοποιηθεί ειδικό λογισμικό, τα δεδομένα παραμένουν σε αυτό το χώρο και μπορεί να φανούν πολύ χρήσιμα σε μια διαδικασία αναζήτησης ψηφιακών πειστηρίων. Η ύπαρξη των δεδομένων σε αυτό τον χώρο είναι τις περισσότερες φορές εν αγνοία των χρηστών. Για παράδειγμα ένας χρήστης που δίνει τον παλιό του σκληρό δίσκο τον οποίο έχει φροντίσει να κάνει formatδεν μπορεί να φανταστεί ότι όλα του τα δεδομένα μπορούν να ανακτηθούν με τα εργαλεία που θα εξεταστούν στο κεφάλαιο 6 αυτής της μεταπτυχιακής διατριβής [02].



Εικόνα 1.3 : Ακριβής σχηματική αναπαράσταση δημιουργίας αδιάθετου χώρου μετά από «διαγραφή» δεδομένων [32].

1.6.3. Πρόσθετα Δεδομένα – FileSlack

Οι υπολογιστές αποθηκεύουν τα δεδομένα σε καθορισμένου μεγέθους μπλοκ δεδομένων. Επειδή πολύ σπάνια τυχαίνει τα δεδομένα που επιθυμεί ένας χρήστης να αποθηκεύσει να έχουν το ακριβές μέγεθος, το υπόλοιπο του αποθηκευτικού χώρου του μπλοκ «γεμίζει» με τυχαία δεδομένα τα οποία λαμβάνονται από την πτητική μνήμη του υπολογιστή (RAM). Αυτά τα δεδομένα είναι δυνατόν να είναι ακόμα και κωδικοί χρήστη για ιστοσελίδες ή οτιδήποτε άλλο ο χρήστης δεν θα ήθελε να βρεθεί από κάποιον που θα είχε τη δυνατότητα να το κάνει. Αυτός ο χώρος επιβάλλεται από έναν ερευνητή ψηφιακής δικανικής να ελεγχτεί γιατί υπάρχει περίπτωση να βρεθούν πολύ σημαντικά πειστήρια για μια υπόθεση, ή στοιχεία τα οποία θα μπορούσαν να βοηθήσουν στην εξέλιξη της έρευνας[02].

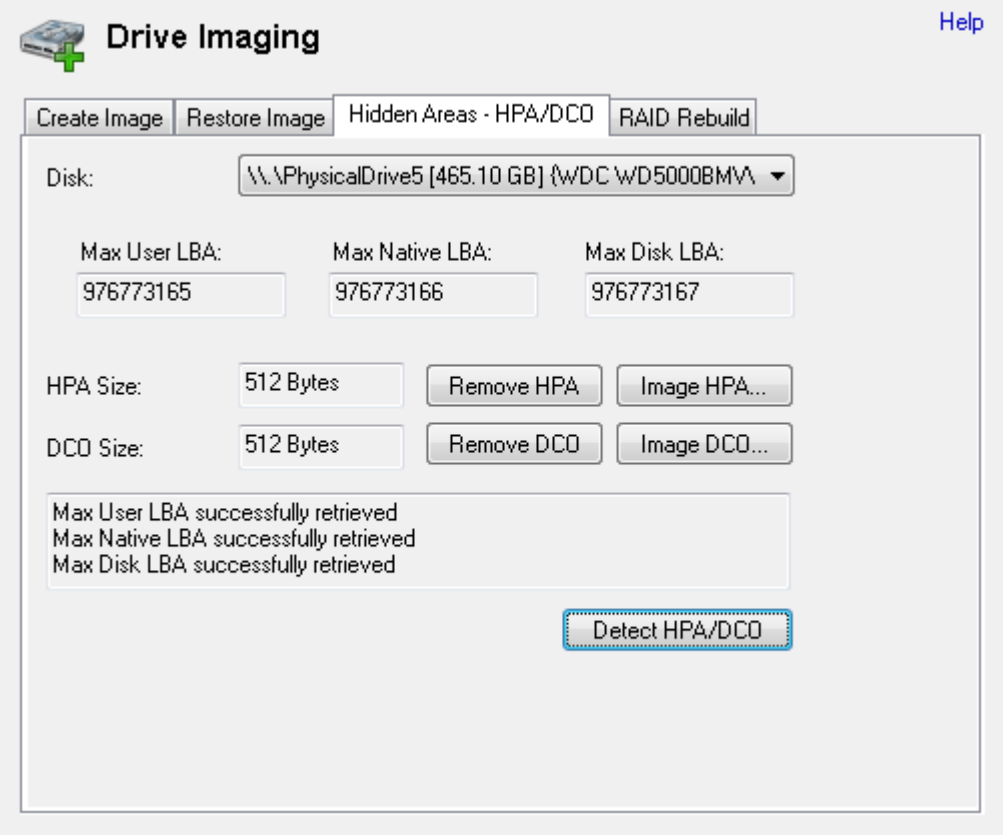


Εικόνα 1.4 : Γραφική αναπαράσταση δημιουργίας του χώρου όπου το λειτουργικό σύστημα αναγκάζεται να γεμίσει με δεδομένα πλούσια σε πληροφορίες από την πτητική μνήμη.

1.6.4. Host Protected Areas and Device Configuration Overlay (HPA and DCO)

Είναι κρυφές περιοχές, στην αρχή ή στο τέλος, των σκληρών δίσκων τις οποίες οι κατασκευαστές τους χρησιμοποιούν για να προστατεύσουν τμήματα τα οποία χρησιμοποιούν σε περίπτωση που χρειαστεί να γίνει ανάκτηση δεδομένων. Ο τρόπος εντοπισμού ύπαρξης ή μη αυτών των περιοχών γίνεται συνήθως μέσω του BIOS ή με τη σύγκριση των τιμών από μια σειρά ATAεντολών. Συνήθως οι ερευνητές ψηφιακής δικανικής δεν ερευνούν τους συγκεκριμένους χώρους διότι είναι προστατευόμενος χώρος από το λειτουργικό σύστημα και ο χρήστης δε μπορεί να αποθηκεύσει αρχεία. Έχουν παρατηρηθεί όμως περιπτώσεις από εξειδικευμένους εγκληματίες να έχουν αποθηκεύσει ενοχοποιητικά δεδομένα και στους δύο αυτούς χώρους. Από τη στιγμή που ένας χρήστης μπορεί να κάνει εγγραφές σε αυτές τις περιοχές, οι οποίες είναι

κρυφές από το λειτουργικό σύστημα και τον χρήστη και υπάρχει η δυνατότητα να έχουν μέγεθος που να μπορούν να αποθηκεύσουν μεγάλο όγκο δεδομένων, ο ερευνητής μιας υπόθεσης θα πρέπει οπωσδήποτε να δώσει τη δέουσα προσοχή με σκοπό τη συλλογή των δεδομένων που βρίσκονται εκεί και την ανάλυσή τους [17].



Εικόνα 1.5 : Εντοπισμός HPAκαι DCOσε σκληρό δίσκο από εργαλείο ψηφιακής δικανικής.

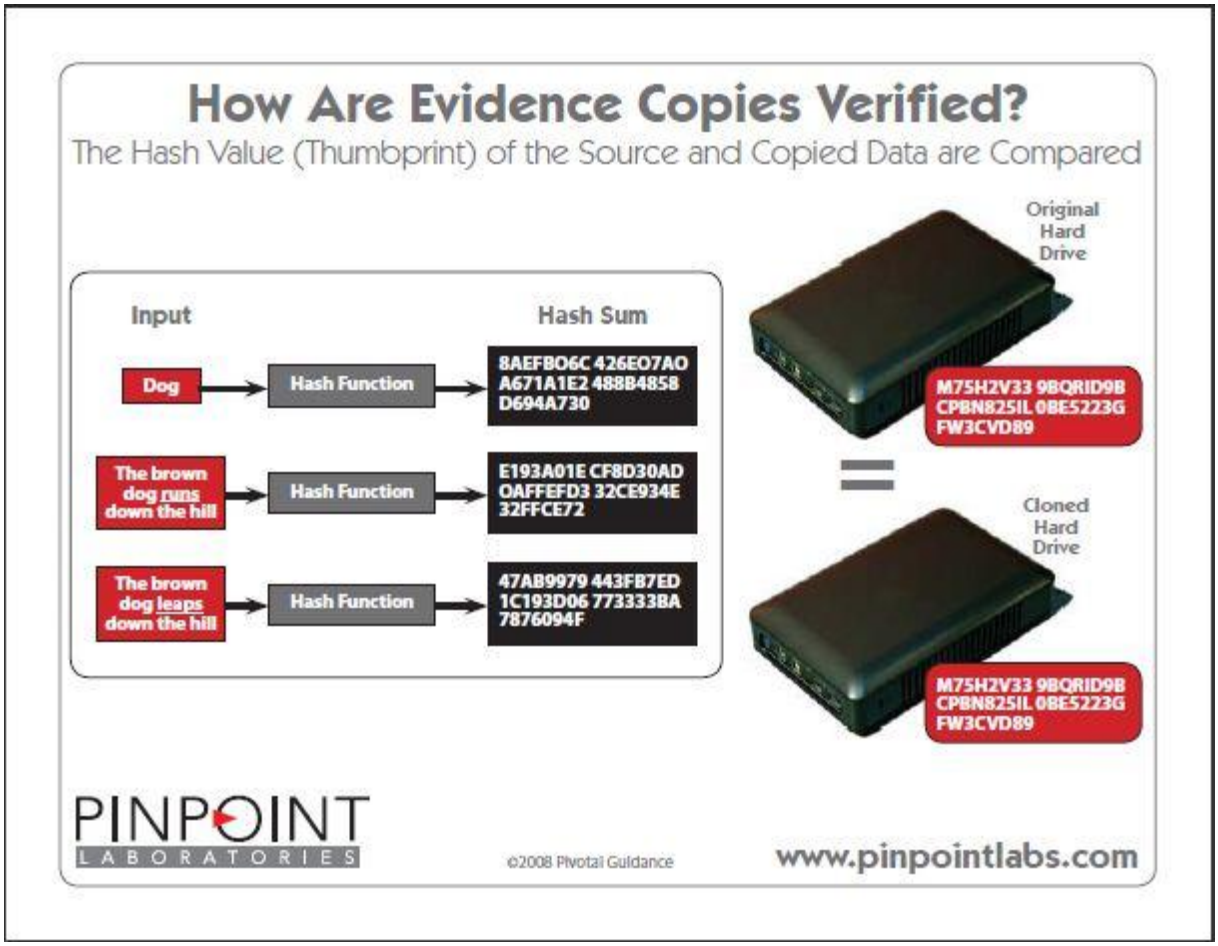
1.6.5. Συνάρτηση Κατακερματισμού (HashValue)

Είναι μια συνάρτηση η οποία δέχεται δεδομένα τυχαίου μεγέθους και επιστρέφει μια τιμή σταθερού μεγέθους από 32 bitμέχρι 256 bitαναλόγως της συνάρτησης που θα χρησιμοποιηθεί. Η τιμή που θα επιστραφεί εξαρτάται άμεσα από όλα τα bitενός αρχείου και οποιαδήποτε τροποποίηση, ή προσθήκη, ή αφαίρεση bitαπό ένα αρχείο προκαλεί και την αλλαγή της τιμής.

Η χρήση της στη ψηφιακή δικανική επιβάλλεται για να αποδειχτεί στο δικαστήριο ότι τα δεδομένα που λήφθηκαν ως ακριβές αντίγραφο από ένα ψηφιακό μέσο δεν έχουν υποστεί καμία αλλοίωση σε σχέση με το πρωτότυπο και η ανάλυση που έγινε στα αντίγραφά τους είναι αποδεκτή από το δικαστήριο σαν αποδεικτικό στοιχείο.

Αυτή την τιμή οφείλει ο ερευνητής να την εξάγει αμέσως μετά τη λήψη ενός αντιγράφου και να τη συγκρίνει αμέσως με την τιμή του πρωτότυπου. Επίσης όταν κάνει διαλογή αρχείων μέσα από το ακριβές αντίγραφο για να το παρουσιάσει στην τελική του αναφορά θα πρέπει για κάθε αρχείο να εκτελεί τη συνάρτηση κατακερματισμού και να παραθέτει την τιμή μαζί με το αρχείο που παρουσιάζει.

Τις τιμές αυτές χρησιμοποιούν και τα λογισμικά ασφαλείας στη βάση δεδομένων τους για να υπολογίζουν και καταγράψουν τις υπογραφές των κακόβουλων λογισμικών που έχουν αναγνωρίσει. Αυτό το γεγονός μπορούν να εκμεταλλευτούν οι κακόβουλοι και να κάνουν μικρές τροποποιήσεις σε ένα κακόβουλο λογισμικό, το οποίο προϋπήρχε και είχε αναγνωριστεί, με αποτέλεσμα να αλλαχτεί η υπογραφή του και να περάσει απαρατήρητο από τα λογισμικά ασφαλείας [11].



Εικόνα 1.6 : Πώς επιβεβαιώνεται η ακεραιότητα των ψηφιακών πειστηρίων με τη χρήση της συνάρτησης κατακερματισμού [32].

1.7. Δομή Διατριβής

Ακολουθεί η δομή της παρούσας διατριβής όπου θα παρουσιαστεί εν συντομία το περιεχόμενο κάθε κεφαλαίου.

1.7.1. Κεφάλαιο 2: Μέθοδοι Λήψης και Ανάλυσης Ψηφιακών πειστηρίων

Σε αυτό το κεφάλαιο θα παρουσιαστούν αναλυτικά οι μέθοδοι και διαδικασίες λήψης των ψηφιακών πειστηρίων από τη στιγμή που θα αναφερθεί το περιστατικό μέχρι και την παρουσίαση των πειστηρίων στο δικαστήριο, ή σε κάποιο διεθνή οργανισμό.

1.7.2. Κεφάλαιο 3 : Ψηφιακή Δικανική στον Κυβερνοπόλεμο

Θα γίνει γενική αναφορά στις ενέργειες του κυβερνοπολέμου, στις συνέπειες χρήσης εμπορικών τεχνολογιών από τους οργανισμούς και τα κράτηενώ επίσης θα παρουσιαστεί η σύνδεση της ψηφιακής δικανικής με τον κυβερνοπόλεμο και τα πλεονεκτήματα που θα προσδώσει σε αυτόν που θα τη χρησιμοποιήσει με το σωστό τρόπο.

1.7.3. Κεφάλαιο 4 : Κλάδοι Ψηφιακής Δικανικής

Παρουσιάζονται σύντομα και περιεκτικά οι τρεις κλάδοι της ψηφιακής δικανικής και τα χαρακτηριστικά που τους κάνουν να ξεχωρίζουν καθώς και η αναγκαιότητα εξειδίκευσης στον κάθε ένα από αυτούς.

1.7.4. Κεφάλαιο 5 : Νομικά Θέματα

Γίνεται αναλυτική παρουσίαση στα νομικά θέματα που διέπουν την ψηφιακή δικανική στην Κυπριακή Δημοκρατία και παρουσιάζονται τα κωλύματα που τίθενται στο έργο της Κυπριακής Αστυνομίας εξ' αιτίας αυτής.

1.7.5. Κεφάλαιο 6 : Εργαλεία Ψηφιακής Δικανικής

Παρατίθενται εμπορικά και ανοικτού κώδικα εργαλεία λήψης, ανάλυσης και παρουσίασης ψηφιακών πειστηρίων τα οποία κρίθηκαν ως αντιπροσωπευτικά δείγματα με σκοπό την

προβολή των μέσων που έχουν στη διάθεσή τους οι ερευνητές για να αντιμετωπίσουν τις προκλήσεις που τους παρουσιάζονται.

1.7.6. Κεφάλαιο 7 : Προβλήματα – Δυσχέρειες

Καταγράφονται τα προβλήματα και οι δυσχέρειες που αντιμετωπίζονται από τους ερευνητές και τους οργανισμούς στην προσπάθειά τους να αντιμετωπίσουν το ηλεκτρονικό έγκλημα και τους διάφορους κακόβουλους χρήστες

1.7.7. Κεφάλαιο 8 : Συμπεράσματα

Τέλος εξάγονται συμπεράσματα που αφορούν στις ακολουθούμενες διαδικασίες και στα εργαλεία και γίνεται σύντομη αναφορά στο μέλλον της ψηφιακής δικανικής.

Κεφάλαιο 2
Μέθοδοι Λήψης και Ανάλυσης Ψηφιακών Πειστηρίων

Τα ψηφιακά πειστήρια είναι πολύτιμα και πρέπει να διαχειρίζονται με τον ίδιο τρόπο που διαχειρίζονται και τα παραδοσιακά αποδεικτικά στοιχεία, με σεβασμό και προσοχή.

Οι κανόνες των αποδεικτικών στοιχείων εφαρμόζονται ισάξια και στα ψηφιακά πειστήρια, όπως ακριβώς θα γινόταν σε οποιαδήποτε υλικά στοιχεία θα συλλέγονταν από κάποια πηγή. Είναι ευθύνη του επικεφαλής της έρευνας να εξασφαλίσει τη νομική συμμόρφωσή τους και το ότι η διαδικασία που ακολουθήθηκε για την απόκτησή τους ήταν η προβλεπόμενη από τη νομοθεσία.

Κατά τη διάρκεια μια έρευνας ενός εγκλήματος, όχι απαραίτητα ηλεκτρονικού, είναι πολύ πιθανό να βρεθούν στη σκηνή του εγκλήματος ηλεκτρονικές συσκευές οι οποίες μπορεί να περιέχουν πολύτιμα αποδεικτικά στοιχεία σχετικά με την υπόθεση. Τέτοιου είδους συσκευές, λόγω της εξέλιξης της τεχνολογίας βρίσκονται πολλές φορές και σε μέρη εκτός της σκηνής του

εγκλήματος, αλλά η ύπαρξη των συσκευών εκεί υποχρεώνει τους ερευνητές να τη διαχειριστούν ως τέτοια. Οι ενέργειες που πρέπει να γίνουν εξαρτούνται απόλυτα από το είδος της συσκευής καθώς και από το αν είναι ενεργοποιημένη ή όχι κατά την άφιξη των ερευνητών. Οι διαδικασίες που ακολουθούνται ανάλογα της περίπτωσης είναι καθορισμένες λεπτομερώς στα εγχειρίδια της αστυνομίας και είναι σχεδόν ίδιες σε όλα τα αστυνομικά σώματα παγκοσμίως καθώς από τον Οκτώβριο του 2012 έχει εκδοθεί το ISO 27037. Η επικαιροποίησή του, για την Κυπριακή Αστυνομία, γίνεται τακτικά και όχι σε μεγαλύτερο διάστημα του ενός έτους.

2.1. Προτεινόμενη από ISO 27037/2012

Η διαδικασία λήψης ψηφιακών πειστηρίων, σύμφωνα με το προτεινόμενο μοντέλο στο ISO 27037/2012, περιλαμβάνει γενικά, αλλά δεν περιορίζεται μόνο σε αυτές, τέσσερις φάσεις -τη συλλογή, την εξέταση, την ανάλυση και την παρουσίαση. Οι ερευνητικές αρχές των κρατών ή και μεγάλων οργανισμών, όπως για παράδειγμα ο OLAF (EuropeanAnti-Fraud Office) οι οποίοι έχουν εξειδικευμένα τμήματα πλέον για τη διενέργεια ερευνών που αφορούν στο ηλεκτρονικό έγκλημα και στη λήψη ψηφιακών πειστηρίων με σκοπό την παρουσίασή τους στο δικαστήριο, αποκλίνουν ελάχιστα από αυτό το μοντέλο, κυρίως με την προσθήκη ενδιάμεσων φάσεων οι οποίες στην πραγματικότητα κάνουν πιο εύκολη την κατανόηση και λειτουργία της κάθε φάσης που θα αναφερθεί παρακάτω και επιτρέπουν την πιο εύκολη κατανομή αρμοδιοτήτων στο προσωπικό [16]. Επιπλέον στα εγχειρίδιά τους τα εξειδικευμένα τμήματα αναλύουν πλήρως και επιτρέπουν ακόμα και σε μη εξειδικευμένο, με την ψηφιακή δικανική, προσωπικό να αντιληφθεί τη σημασία της τήρησης της διαδικασίας από την αρχή ως το τέλος γιατί οποιαδήποτε παράλειψη ή λανθασμένος χειρισμός μπορεί να ρίξει την όποια υπόθεση σε ένα δικαστήριο ή ακόμη χειρότερα να οδηγήσει σε λανθασμένο αποτέλεσμα.

2.1.1. Η συλλογή

Περιλαμβάνει την αναζήτηση, αναγνώριση, συλλογή και καταγραφή των ψηφιακών πειστηρίων [05,10,13,46]. Αναλύεται στα παρακάτω στάδια :

1. Προετοιμασία

   Σε ιδιωτικές περιπτώσεις μπορεί να περιλαμβάνει επιμόρφωση των πελατών σχετικά με την προετοιμασία των συστημάτων τους, για παράδειγμα η εξέταση θα δώσει περισσότερα στοιχεία αν ένας εξυπηρετητής έχει ενεργοποιημένα όλα τα αρχεία καταγραφής του το οποίο μπορεί να γίνει με τη βοήθεια του διαχειριστή από τη στιγμή που δεν είναι ύποπτος. Σε περίπτωση που υπάρχει ύποπτος εργαζόμενος τότε μπορεί να γίνει η εξέταση σε προσυμφωνημένη ώρα που θα απουσιάζει ή και συγκαλυμμένα για να ληφθούν αποτελέσματα σε πραγματικό χρόνο.

   Για τον εξεταστή η προετοιμασία περιλαμβάνει ανάλογη εκπαίδευση, τακτικές δοκιμές και επιβεβαίωση του εξοπλισμού του, εξοικείωση με τη νομοθεσία, προετοιμασία για εμπλοκή με μη αναμενόμενες καταστάσεις και διασφάλιση ότι ο εξοπλισμός του για την επί τόπου ανάκτηση δεδομένων είναι πλήρης και σε λειτουργήσιμη κατάσταση.

2. Εκτίμηση

   Το στάδιο της εκτίμησης περιλαμβάνει τη λήψη σαφών οδηγιών, διαχείριση κινδύνου και ανάθεση ρόλων και πόρων.

3. Συλλογή

   Αν η λήψη των πειστηρίων θα γίνει στον τόπο που βρίσκεται ο υπολογιστής και όχι σε ένα εργαστήριο ψηφιακής δικανικής τότε αυτή η φάση περιλαμβάνει την αναγνώριση, την εξασφάλιση και την καταγραφή της σκηνής. Τυχόν συνεντεύξεις από το εμπλεκόμενο προσωπικό περιλαμβάνονται σε αυτή τη φάση. Επίσης περιλαμβάνει την σήμανση και την αποθήκευση σε ειδικές θήκες των αποδεικτικών στοιχείων από τον χώρο. Πρέπει να δοθεί ιδιαίτερη προσοχή στην ασφαλή μεταφορά των υλικών στο εργαστήριο της δικανικής.

   Η μέθοδος που θα ακολουθηθεί για τη συλλογή των πειστηρίων εξαρτάται από την κατάσταση στη σκηνή του εγκλήματος, αν είναι ενεργοποιημένες οι συσκευές που θα ερευνηθούν ή όχι, από το αν υπάρχει στη σκηνή το αρμόδιο εξειδικευμένο προσωπικό με τα κατάλληλα εργαλεία (συσκευές και λογισμικό) και από τη φύση του περιστατικού.

4. Διατήρηση Πειστηρίων

Η συλλογή μόνο των πειστηρίων και η ανάλυσή τους δεν είναι αρκετή για να μπορέσουν τα πειστήρια να γίνουν αποδεκτά σε ένα δικαστήριο. Απαιτείται η διατήρησή τους στην αρχική τους μορφή, όχι μόνο των αντιγράφων που έχουν ληφθεί, αλλά και των συσκευών όπου φέρονται τα πρωτότυπα. Η διατήρηση των ψηφιακών πειστηρίων περιλαμβάνει όλες εκείνες τις ενέργειες που απαιτούνται για την προστασία των ψηφιακών τεκμηρίων και τη διατήρηση της δυνατότητας πρόσβασής τους σε βάθος χρόνου, μέχρι το οριστικό κλείσιμο μιας υπόθεσης. Ιδιαίτερα για συσκευές που λειτουργούν με τη χρήση μπαταρίας απαιτείται η διατήρηση της φόρτισής της μέχρι και τη λήξη της υπόθεσης για να μην αλλοιωθούν τα δεδομένα. Επίσης όλες οι συσκευές πρέπει να διατηρούνται σε συνθήκες με κατάλληλη θερμοκρασία και υγρασία και ταυτόχρονα να είναι αποκλεισμένες από οποιαδήποτε ασύρματα ή ενσύρματα δίκτυα τα οποία θα μπορούσαν να αξιοποιηθούν για αλλοίωση των δεδομένων. Οι συσκευασίες αποθήκευσης που θα χρησιμοποιηθούν πρέπει να είναι αντιστατικές και κατά τη μεταφορά τους πρέπει να παραμένουν απομονωμένα από οποιαδήποτε ραδιοσυχνότητα.

Για όλα τα ηλεκτρονικά μέσα αποθήκευσης που έχουν κατασχεθεί και για όλα τα ακριβή αντίγραφά τους πρέπει να υπολογιστεί και να καταγραφεί η τιμή της συνάρτησης κατακερματισμού (hashvalue) για ολόκληρο το μέσο και αν γίνει διαλογή αρχείων και για κάθε αρχείο. Η τιμή μπορεί να υπολογιστεί με τους αλγόριθμους MD5 και SHA1. Σε περίπτωση λήψης των αντιγράφων με τις συσκευές σε λειτουργία η τιμή των αλγορίθμων μεταξύ των πρωτότυπων δεδομένων και των αντιγράφων δεν είναι δυνατόν να είναι σε όλα τα αρχεία η ίδια και ο εξεταστής είναι υπεύθυνος να αποδείξει στο δικαστήριο, καταθέτοντας το αρχείο καταγραφής ενεργειών του, την ακεραιότητα των πειστηρίων που καταθέτει.

2.1.2. Η εξέταση

Αυτή η φάση βοηθά στο να εμφανίσει τα τεκμήρια, να εξηγήσει την προέλευσή τους και τη σπουδαιότητά τους. Περιλαμβάνεται επίσης και την αναζήτηση πληροφοριών οι οποίες κρύφτηκαν ή επισκιάστηκαν. Εδώ είναι που θα γίνει ο έλεγχος του ακριβούς αντιγράφου που

έχει συλλεχθεί από την προηγούμενη φάση και είναι απαραίτητη η παρουσία του ανακριτή της υπόθεσης ο οποίος με τη βοήθεια του εξειδικευμένου προσωπικού θα εντοπίσει τα απαραίτητα για την υπόθεση ψηφιακά πειστήρια ακλουθώντας τη δικανική διαδικασία με σκοπό να τα παρουσιάσει στο δικαστήριο. Για να γίνει αυτό θα πρέπει να παραχθεί και ο ανάλογος αριθμός αντιγράφων πριν την εξέταση έτσι ώστε να υπάρχει πάντα αντίγραφο με ακέραια δεδομένα σε περίπτωση κάποιου λάθους [05,10,13].

Φιλτράρισμα των ευρετηρίων που δημιουργούνται, εξέταση κρυφών δεδομένων και αδιάθετου χώρου, ανάκτηση διαγραφέντων αρχείων και αναζήτηση με λέξεις ή και φράσεις κλειδιά είναι μερικές από τις εργασίες που γίνονται σε αυτή τη φάση. Επίσης καταγραφή του ηλεκτρονικού ταχυδρομείου του υπόπτου, παρόλο που είναι προστατευμένο από το Σύνταγμα είναι πολύ εύκολο να γίνει και μπορεί να οδηγήσει σε νέες πηγές αποδεικτικών στοιχείων παρά το ότι δε μπορεί να γίνει αποδεκτό σαν πειστήριο από το δικαστήριο. Για κάθε πειστήριο που ελέγχεται και κατατίθεται ο ερευνητής θα πρέπει να μπορεί να αποδείξει την ακεραιότητά του.

2.1.3. Η ανάλυση

Η διαφορά αυτής της φάσης από την εξέταση είναι ότι παίρνει το προϊόν της εξέτασης και εξετάζει τη σημασία και την αποδεικτική του αξία στην υπόθεση. Η εξέταση είναι ένα τεχνικό θέμα και εμπίπτει στη δικαιοδοσία του εξεταστή ψηφιακών πειστηρίων ενώ η ανάλυση μπορεί να διεξαχθεί και από προσωπικό που δεν είναι πιστοποιημένο ως εξεταστές ψηφιακών πειστηρίων [05,10,13].

Ο εξεταστής συνήθως παρέχει πληροφόρηση στον επικεφαλής της έρευνας κατά τη διάρκεια της ανάλυσης και από αυτόν τον διάλογο η ανάλυση είναι πιθανό να πάρει διαφορετική πορεία ή και να περιοριστεί σε συγκεκριμένες περιοχές. Η ανάλυση πρέπει να είναι ακριβής, εξονυχιστική, αμερόληπτη, καταγεγραμμένη και ολοκληρωμένη εντός των χρονικών πλαισίων και βάσει των διαθέσιμων πόρων.

2.1.4. Η παρουσίαση – αναφορά

Περιλαμβάνει την παρουσίαση από τον εξεταστή μιας δομημένης αναφοράς για τα ευρήματα, καταδεικνύοντας τα σημεία στις αρχικές οδηγίες καθώς και οποιεσδήποτε συμπληρωματικές. Η αναφορά θα πρέπει να συνταχθεί με σκοπό να είναι κατανοητή από τον αναγνώστη ο οποίος

κατά πάσα πιθανότητα δε θα είναι γνώστης τεχνικών ορολογιών που θα χρησιμοποιηθούν. Επίσης θα πρέπει ο ερευνητής να είναι προετοιμασμένος να συμμετέχει σε συναντήσεις όπου θα συζητηθεί η αναφορά και θα τύχει επεξεργασίας, ή ακόμα και να κληθεί να καταθέσει σχετικά, όχι μόνο για τη διεξαγωγή της εξέτασης, αλλά και για την εγκυρότητα της διαδικασίας καθώς και για τα δικά του προσόντα – πιστοποιήσεις για να διεξάγει την εξέταση. Ο ρόλος του εξεταστή είναι να εξασφαλίσει από κάθε κατασχεμένο υλικό ένα ακριβές αντίγραφο των δεδομένων που περιέχονται. Αυτό πρέπει να επιτευχθεί χωρίς να αλλοιωθούν τα αρχικά δεδομένα για να είναι δυνατή η αποδοχή τους ως αποδεικτικό στοιχείο στο δικαστήριο[05,10,13].

2.2. Λεπτομερής Διαδικασία Λήψης Ψηφιακών Πειστηρίων από τη Σκηνή του Εγκλήματος

Οι 4 προαναφερθείσες φάσεις της ψηφιακής δικανικής είναι αρκετές για να δώσουν το γενικό πλαίσιο μιας διαδικασίας που αφορά στη λήψη, εξέταση και αξιοποίηση των τεκμηρίων από έναν οργανισμό ή από τις αστυνομικές αρχές ενός κράτους, δε μπορούν όμως να εξηγήσουν την ακριβή τήρησης μιας αυστηρά καθοριζόμενης διαδικασίας την οποία οφείλουν να ακολουθήσουν όλοι όσοι εμπλέκονται με τη συλλογή και διαφύλαξη των τεκμηρίων με σκοπό την παρουσίασή τους στο δικαστήριο.

Το αρμόδιο τμήμα της Αστυνομίας Κύπρου έχει διαμορφώσει ειδικό εγχειρίδιο που αφορά στην εν λόγω διαδικασία και είναι σύμφωνο με το αντίστοιχο της Βρετανικής Αστυνομίας που μαζί με το ISO 27037/2012 θεωρούνται τα πρότυπα παγκοσμίως. Το εγχειρίδιο έχει συνταχθεί με τρόπο που να επιτρέπει τη λιγότερη δυνατή πρόκληση ζημιάς ή απώλειας δεδομένων ακόμα και σε περιπτώσεις που δεν ήταν δυνατή η παρουσία αρμόδιου – εξειδικευμένου προσωπικού και η λήψη θα γίνει αναγκαστικά από μη εξειδικευμένο. Είναι πολύ σημαντική η έμφαση στη λεπτομέρεια που δίνεται και κυρίως η συνεχής επισήμανση για καταγραφή όλων των ενεργειών του προσωπικού που πραγματοποιεί τη λήψη. Οι οδηγίες στο εγχειρίδιο είναι χωρισμένες σε κατηγορίες, αναλόγως το είδος των συσκευών και με την κατάσταση στην οποία έχουν βρεθεί. Δηλαδή αν ήταν σε λειτουργία ή όχι.

Από τη διαδικασία είναι εμφανές ότι οι αρμόδιες αστυνομικές αρχές εστιάζουν το ενδιαφέρον τους περισσότερο στα αποθηκευμένα δεδομένα σε μια συσκευή και ενδιαφέρονται λιγότερο ή και καθόλου για τα δεδομένα που βρίσκονται στην πτητική μνήμη. Αυτό μπορεί να εξηγηθεί και από τη φύση των εγκλημάτων που ερευνούν, τα οποία αφορούν κατά το πλείστο θέματα

ηλεκτρονικού εγκλήματος, παιδική πορνογραφία και οικονομικά εγκλήματα για τα οποία τα τεκμήρια που απαιτούνται να παρουσιαστούν στο δικαστήριο είναι κυρίως έγγραφα, φωτογραφίες και βίντεο. Εξ αιτίας αυτής της εστίασης θα φανεί στη διαδικασία ότι αφήνεται πολλές φορές, σε περίπτωση απουσίας αρμόδιου – εξειδικευμένου προσωπικού, να χαθεί το περιεχόμενο της πτητικής μνήμης το οποίο ακόμα και στα προαναφερθέντα εγκλήματα μπορεί να φανεί πολύτιμο και θα αναλυθεί η σημασία του στο κεφάλαιο 3.

Ακολουθεί η παρουσίαση της διαδικασίας λήψης των ψηφιακών πειστηρίων από τη σκηνή του εγκλήματος μέχρι και τη μεταφορά τους στο δικανικό εργαστήριο για ανάλυση και φύλαξη.

2.2.1. Ηλεκτρονικοί Υπολογιστές και Φορητοί Ηλεκτρονικοί Υπολογιστές.

1. Περίπτωση εντοπισμού του εξοπλισμού που να μοιάζει απενεργοποιημένος.
    1.1. Εξασφάλιση και ανάληψη του ελέγχου της περιοχής που περιλαμβάνει τον εξοπλισμό.
    1.2. Απομάκρυνση όλων από τον εξοπλισμό και τους διακόπτες ηλεκτρικής τροφοδοσίας του χώρου.
    1.3. Φωτογράφιση ή βιντεοσκόπηση του χώρου, που να περιλαμβάνει όλο τον εξοπλισμό. Τοποθέτηση ετικετών στα καλώδια και στις θύρες έτσι ώστε να είναι δυνατή η επανασύνδεσή τους αργότερα.
    1.4. Επιτρέπεται σε εκτυπωτές να ολοκληρώσουν τυχόν εργασίες.
    1.5. Δεν ενεργοποιούμε σε καμία περίπτωση τον υπολογιστή.
    1.6. Επιβεβαιώνουμε ότι ο υπολογιστής είναι απενεργοποιημένος.
    1.7. Αφαιρούμε από τους φορητούς την μπαταρία, εφόσον είναι επιβεβαιωμένα απενεργοποιημένοι αλλιώς θα χαθούν δεδομένα.
    1.8. Βγάζουμε την τροφοδοσία και τις υπόλοιπες συσκευές που είναι συνδεδεμένες στον υπολογιστή. Ένας υπολογιστής που φαίνεται απενεργοποιημένος και είναι σε κατάσταση αδράνειας (sleepmode) είναι δυνατόν να προσπελαστεί μεμακρυσμένα και να αλλοιωθούν ή διαγραφούν τα δεδομένα του.
    1.9. Ελέγχουμε την περιοχή για τυχόν σημειωματάρια ή κομμάτια χαρτιού που να έχουν σημειωμένους κωδικούς (συνήθως βρίσκονται κοντά στον υπολογιστή), ή άλλα στοιχεία τα οποία θα μπορούσαν να χρησιμοποιηθούν από τον αναλυτή.

1.10. Εξετάζουμε την πιθανότητα να ρωτήσουμε τον χρήστη σχετικά με τη διαμόρφωση του συστήματος, περιλαμβανομένων κωδικών, αν το επιτρέπουν οι περιστάσεις. Αν δοθούν καταγράφονται πολύ προσεκτικά και εξετάζονται με επιφύλαξη.

1.11. Κρατούμε λεπτομερείς σημειώσεις για όλες τις ενέργειες που έλαβαν χώρα σε σχέση με τον πληροφοριακό εξοπλισμό.

2. Περίπτωση εντοπισμού ενεργοποιημένου εξοπλισμού

1.1. Εξασφάλιση και ανάληψη του ελέγχου της περιοχής που περιλαμβάνει τον εξοπλισμό.

1.2. Απομάκρυνση όλων από τον εξοπλισμό και τους διακόπτες ηλεκτρικής τροφοδοσίας του χώρου.

1.3. Φωτογράφιση ή βιντεοσκόπηση του χώρου, που να περιλαμβάνει όλο τον εξοπλισμό. Τοποθέτηση ετικετών στα καλώδια και στις θύρες έτσι ώστε να είναι δυνατή η επανασύνδεσή τους αργότερα.

1.4. Επιτρέπεται σε εκτυπωτές να ολοκληρώσουν τυχόν εργασίες.

1.5. Εξετάζουμε την πιθανότητα να ρωτήσουμε τον χρήστη σχετικά με τη διαμόρφωση του συστήματος, περιλαμβανομένων κωδικών, αν το επιτρέπουν οι περιστάσεις. Αν δοθούν καταγράφονται πολύ προσεκτικά και εξετάζονται με επιφύλαξη.

1.6. Καταγραφή όσων παρουσιάζονται στην οθόνη με φωτογράφηση και γραπτές σημειώσεις.

1.7. Δεν ακουμπούμε το πληκτρολόγιο και το ποντίκι αν δεν ληφθούν πρώτα δακτυλικά αποτυπώματα και δείγμα DNA. Κατόπιν μετακινούμε το ποντίκι για να φύγει το screensaver και φωτογραφίζουμε ότι έχει η οθόνη εκείνη τη στιγμή. Η στιγμή μετακίνησης του ποντικιού καταγράφεται.

1.8. Όπου είναι δυνατό, συλλέγουμε δεδομένα που σε περίπτωση απενεργοποίησης θα χαθούν, όπως εκτελούμενες εργασίες, πτητική μνήμη και πληροφορίες σχετικά με την κατάσταση των θυρών δικτύου. Εξασφαλίζουμε ότι οι ενέργειές μας δε θα προκαλέσουν οποιαδήποτε αλλαγή στο σύστημα, είναι κατανοητές και καταγράφονται.

1.9. Αν δεν υπάρχει ειδικός ερευνητής ψηφιακών πειστηρίων στη σκηνή, αφαιρούμε την τροφοδοσία χωρίς να κλείσουμε κανένα πρόγραμμα. Η αφαίρεση γίνεται με την αποκόλληση του καλωδίου πίσω από τον υπολογιστή και όχι από την πρίζα. Αυτό θα αποτρέψει οποιαδήποτε

αυτοματοποιημένη ενέργεια μπορεί να υπάρχει σε περίπτωση ύπαρξης συσκευής αδιάλειπτης παροχής ενέργειας .

1.10. Αφαιρούμε όλα τα υπόλοιπα καλώδια που οδηγούν στον υπολογιστή.

1.11. Εξασφαλίζουμε ότι σε όλα τα εξαρτήματα – καλώδια έχουν τοποθετηθεί ετικέτες που να καταδεικνύουν με ακρίβεια τη θέση τους.

1.12. Επιτρέπουμε στον εξοπλισμό να πέσει η θερμοκρασία του πριν τη μετακίνηση.

1.13. Ελέγχουμε την περιοχή για τυχόν σημειωματάρια ή κομμάτια χαρτιού που να έχουν σημειωμένους κωδικούς (συνήθως βρίσκονται κοντά στον υπολογιστή), ή άλλα στοιχεία τα οποία θα μπορούσαν να χρησιμοποιηθούν από τον αναλυτή.

1.14. Επιβεβαιώνουμε ότι έχουν ληφθεί λεπτομερείς σημειώσεις σε σχέση με τον εξοπλισμό πληροφορικής.

3. Τι πρέπει να κατασχεθεί

Όλα τα παρακάτω πρέπει να τοποθετούνται σε ειδικές θήκες τεκμηρίων και να τους τοποθετείται η ανάλογη ετικέτα.

3.1. Υπολογιστές

3.2. Οθόνες, πληκτρολόγια και ποντίκια (σε ειδικές περιπτώσεις)

3.3. Ειδικά καλώδια - leads (σε ειδικές περιπτώσεις)

3.4. Τροφοδοσία

3.5. Σκληροί δίσκοι που δεν βρίσκονται εντός των υπολογιστών

3.6. Dongles Μικρές Συσκευές Αυθεντικοποίησης

3.7. Modems (Κάποια περιέχουν στοιχεία που μπορεί να βοηθήσουν τον ανακριτή, όπως κωδικούς ή τηλέφωνα ή vpn συνδέσεις)

3.8. Εξωτερικά μέσα αποθήκευσης δεδομένων (Δίσκοι, flashdrives, cds – dvds, backuptapes)

3.9. Ασύρματες κάρτες δικτύου

3.10. Δρομολογητές

3.11. Ψηφιακές Φωτογραφικές μηχανές

3.12. PCMCIA cards (Κάρτες που επιτρέπουν σε φορητούς υπολογιστές να εκτελούν λειτουργίες που συνήθως δεν έχουν προεγκατεστημένες)

3.13. Εγχειρίδια υπολογιστών και λογισμικού

3.14. Οτιδήποτε μπορεί να περιέχει κωδικούς (κινητά τηλέφωνα, ημερολόγια, σημειωματάρια κλπ κλπ)

3.15. Κλειδιά κρυπτογράφησης

3.16. Κλειδιά ασφαλείας (απαραίτητα για την φυσική πρόσβαση στο εσωτερικό ορισμένων υπολογιστών και μέσων αποθήκευσης.)

2.2.2. Έξυπνα Τηλέφωνα – Ταμπλέτες

Τα κινητά τηλέφωνα και οι ταμπλέτες πλέον έχουν επεξεργαστική ισχύ ίση και μερικές φορές και μεγαλύτερη από έναν υπολογιστή και είναι ικανές συσκευές να εκτελούν όλες τις εργασίες που μπορεί να εκτελέσει κι ένας υπολογιστής. Επίσης έχουν και αποθηκευτικό χώρο αρκετό για την αποθήκευση και επεξεργασία μεγάλου όγκου δεδομένων ο οποίος στις πλείστες των περιπτώσεων επεκτείνεται σχεδόν απεριόριστα με τη χρήση καρτών μνήμης με πολύ μικρό μέγεθος. Οι εγκληματίες, ανεξαρτήτως είδους, τείνουν να τα χρησιμοποιούν όλο και περισσότερο για την εκτέλεση των πράξεών τους ή για την αποθήκευση δεδομένων που θα μπορούσαν να βοηθήσουν στην εξιχνίαση ενός εγκλήματος. Η μεγάλη τους διαφορά με τους υπολογιστές είναι ότι λόγω της μη ύπαρξης σκληρού δίσκου (στις περισσότερες) για να αποκτηθεί πρόσβαση στα δεδομένα της συσκευής, η συσκευή θα πρέπει να τεθεί σε λειτουργία (πρέπει να αποφεύγεται στις σκηνές εγκλήματος), που σημαίνει ότι αυτόματα παραβιάζεται η πρώτη αρχή. Η δυνατότητα παραγωγής ενός αντιγράφου της συσκευής για ανάλυση υπάρχει με τη χρήση πολύ εξειδικευμένου λογισμικού το οποίο έχει αρχίσει να παρέχεται και από τα εργαλεία που θα παρουσιαστούν σε αυτή τη μελέτη τα τελευταία χρόνια [19,20,21].

Κοινό τους χαρακτηριστικό είναι η χρήση της μπαταρίας για τη λειτουργία τους η οποία σε περίπτωση κατάσχεσής τους θα πρέπει να ληφθεί μέριμνα για τη μη αποφόρτισή της λόγω του ότι υπάρχει η πιθανότητα να διαγραφούν όλα τα δεδομένα, είτε γιατί το μοντέλο δεν έχει δεύτερη μπαταρία για τη διατήρησή τους σε περίπτωση αποφόρτισης, είτε γιατί η δεύτερη μπαταρία έχει αχρηστευτεί με την πάροδο του χρόνου.

Κατά την κατάσχεση δεν πρέπει να ενεργοποιούνται. Πρέπει να σφραγίζονται σε ένα φάκελο πριν να τοποθετηθούν στη σακούλα τεκμηρίων για να μην υπάρχει πρόσβαση στην οθόνη και τα πλήκτρα και να προσπελαστούν τα δεδομένα του από αναρμόδιους. Η σακούλα αυτή θα πρέπει να τοποθετείται σε μεταλλικό κουτί το οποίο δεν θα επιτρέπει τη διακίνηση δεδομένων από και προς αυτά είτε με δίκτυα κινητής τηλεφωνίας είτε με ασύρματα δίκτυαwifi.

Σε περίπτωση που βρεθεί ανοικτό είναι προτιμότερο να παραμείνει έτσι γιατί κατά πάσα πιθανότητα θα προστατεύεται από κωδικό κατά την ενεργοποίησή του και υπάρχει ο κίνδυνος

να μην καταφέρουν οι ερευνητές να αποκτήσουν πρόσβαση. Γι αυτόν το λόγο θα πρέπει η εξέτασή του να γίνει το συντομότερο δυνατό και να γίνει προσπάθεια να επαναφορτίζεται η μπαταρία του από αρμόδιο πρόσωπο έτσι ώστε να μη χαθούν πολύτιμα δεδομένα. Πέραν τούτου η διαχείρισή του πρέπει να είναι όπως στην περίπτωση που βρεθεί ένας υπολογιστής ενεργοποιημένος.

Η ταμπλέτα ή το έξυπνο κινητό δεν πρέπει σε καμία περίπτωση να παραδοθούν στον ιδιοκτήτη τους πριν να ολοκληρωθούν οι διαδικασίες λήψης τεκμηρίων.

Εξαιτίας της μεγάλης ποικιλίας μοντέλων και λειτουργικών συστημάτων η διαδικασία πιθανόν να διαφέρει κατά πολύ από μοντέλο σε μοντέλο, ειδικά σε ότι αφορά το είδος του λειτουργικού συστήματος που χρησιμοποιείται και στην πρόσβαση σε προστατευόμενες από κωδικό περιοχές.

Τέλος πρέπει να ληφθεί υπόψη ότι η κρυπτογράφηση αρχείων ή και ολόκληρης της συσκευής είναι πολύ πιθανή και σε περίπτωση που βρέθηκε ενεργοποιημένη και αποκρυπτογραφημένη θα πρέπει να γίνει η λήψη του αντιγράφου το συντομότερο δυνατό για να αποφευχθεί η κρυπτογράφησή λόγω απενεργοποίησής της.

2.2.3. Ψηφιακά Πειστήρια στο Διαδίκτυο

Το Διαδίκτυο είναι ένα μέσο όπου μπορούν να διακινηθούν, αποθηκευτούν και διαμοιραστούν δεδομένα. Ανεξάρτητα με το μέγεθός του στην πραγματικότητα δεν είναι τίποτα παραπάνω από ένα μεγάλο δίκτυο υπολογιστών. Οποιαδήποτε πληροφορία στο Διαδίκτυο βρίσκεται αποθηκευμένη σε έναν ή περισσότερους υπολογιστές, επομένως μπορεί να ανακτηθεί για μια εξέταση ψηφιακής δικανικής. Ωστόσο κάποιες από αυτές τις πληροφορίες είναι πτητικές, για παράδειγμα μηνύματα μεταξύ των χρηστών σε chat, ή μπορούν να αλλαχτούν ή να διαγραφούν πριν από τον εντοπισμό τους και την εξέτασή των συσκευών, πχ περιεχόμενα ιστοσελίδας ή φόρουμ. Σε τέτοιες περιπτώσεις είναι απαραίτητη η συλλογή των τεκμηρίων απευθείας από το Διαδίκτυο, είτε με αλληλεπίδραση με τον ύποπτο, είτε με συλλογή του περιεχομένου μιας ιστοσελίδας. Η συλλογή πληροφοριών από ιστοσελίδες είναι μια μεγάλη πρόκληση για τους ερευνητές λόγω του ότι είναι πολύ πιθανό ο εξυπηρετητής που φιλοξενεί την ιστοσελίδα να βρίσκεται εκτός της αρμοδιότητας της υπηρεσίας ασφαλείας που διεξάγει την έρευνα. Για παράδειγμα η έρευνα να διεξάγεται από την Αστυνομία Κύπρου και ο εξυπηρετητής να βρίσκεται στην Τουρκία. Σε τέτοιες περιπτώσεις η λύση είναι να συλλέγονται όλα τα δεδομένα

συγκεκριμένων ιστοσελίδων με ειδικό λογισμικό και σε περίπτωση απλών ιστοσελίδων να φωτογραφίζονται και να καταγράφονται προκειμένου να προληφθεί πιθανή αλλαγή τους.

Πέραν των παραπάνω είναι πολύ πιθανόν ο ύποπτος να χρησιμοποιήσει έναν φυλλομετρητή για να συλλέξει πληροφορίες είτε για το στόχο του, είτε για τη μέθοδο που θα χρησιμοποιήσει για την εκτέλεση της εγκληματικής του πράξης.Η αναζήτηση ψηφιακών πειστηρίων που έχουν μείνει από τη δραστηριότητα στο Διαδίκτυο είναι ένα πολύ σημαντικό μέρος της έρευνας στην ψηφιακή δικανική. Σχεδόν κάθε κίνηση που πραγματοποιείται από τον ύποπτο κατά τη διάρκεια της χρήσης ενός φυλλομετρητή αφήνει στοιχεία στον υπολογιστή, ακόμα και η αναζήτηση πληροφοριών [12]. Η πληθώρα φυλλομετρητών που υπάρχει σήμερα επιτρέπει στον ύποπτο να κάνει αναζητήσεις και να περιηγηθεί στο Διαδίκτυο με πολλούς διαφορετικούς ταυτόχρονα, γεγονός το οποίο δυσκολεύει την αναζήτηση και συλλογή των πειστηρίων από τον ερευνητή.

Για να θεωρείται αποτελεσματική η ανάλυση των φυλλομετρητών θα πρέπει:

1. να είναι ολοκληρωμένη ανάλυση όλων των εγκατεστημένων φυλλομετρητών στον ύποπτο υπολογιστή,

2. να δημιουργεί έναν χρονολογικό πίνακα της δραστηριότητας του υπόπτου,

3. να συλλέγει σημαντικές πληροφορίες για τις αναζητήσεις του υπόπτου και τη δραστηριότητά του,

4. να ανακτήσει τη διαγραμμένη, από τον ύποπτο, ιστορία περιήγησης σε αυτούς όπου αυτό είναι δυνατό.

2.2.4. Ηλεκτρονικό Ταχυδρομείο

Το ηλεκτρονικό ταχυδρομείο είναι πλέον η πρώτη επιλογή επικοινωνίας και αποστολής πληροφοριών. Μπορεί να συλλεχθεί για σκοπούς δικανικής εξέτασης από τους υπολογιστές που το έχουν αποθηκευμένο και να εξεταστεί. Είναι σημαντικό να λαμβάνεται η επικεφαλίδα (header) του κάθε μηνύματος επειδή εκεί αναγράφονται όλες οι σημαντικές πληροφορίες σχετικά με τον αποστολέα, τον παραλήπτη και την ημερομηνία αποστολής και λήψης. Οι ερευνητές που χρειάζονται να βρουν τα στοιχεία του αποστολέα ή του παραλήπτη ενός

μηνύματος πρέπει να αποταθούν στον πάροχο του ηλεκτρονικού ταχυδρομείου ο οποίος είναι υπόλογος στις διατάξεις του κανονισμού Regulation of InvestigatoryAct (RIPA 2000).

Εδώ παρουσιάζεται και ένα μεγάλο νομικό κώλυμα για τις ερευνητικές αρχές της Κυπριακής Δημοκρατίας όπου λόγω της απόλυτης προστασίας των επικοινωνιών, εκτός δύο εξαιρέσεων, απαγορεύεται να ληφθεί, να ερευνηθεί και να κατατεθεί ως τεκμήριο στο δικαστήριο η ηλεκτρονική αλληλογραφία ενός υπόπτου όταν πρόκειται για έρευνα που διεξάγεται εντός της Κυπριακής Δημοκρατίας για έγκλημα που είναι στην αρμοδιότητά της. Σε περίπτωση όμως που ζητηθεί να ερευνηθεί ύποπτος εντός της Κυπριακής Δημοκρατίας από αρχές της Ευρωπαϊκής Ένωσης ή κράτους μέλους, τότε η ηλεκτρονική αλληλογραφία και γενικά όλες οι επικοινωνίες του υπόπτου μπορούν να κατατεθούν ως τεκμήρια λόγω της υποχρέωσης της Κυπριακής Δημοκρατίας προς τη Σύμβαση του Συμβουλίου της Ευρώπης κατά του Εγκλήματος μέσω Διαδικτύου του 2001 και του άρθρου 1^{A} του Συντάγματος. Περισσότερη ανάλυση επί του θέματος υπάρχει στο κεφάλαιο που αφορά στα νομικά θέματα.

2.3 Συλλογή των Ψηφιακών Πειστηρίων

Η διαδικασία της συλλογής των ψηφιακών πειστηρίων ακολουθεί τη διαδικασία λήψης η οποία είναι πιθανόν να γίνει και από μη εξειδικευμένο προσωπικό, αναλόγως της κατάστασης και του είδους της υπόθεσης. Η απόφαση για το αν θα κληθεί επί τόπου αρμόδιο προσωπικό ή όχι λαμβάνεται από τον επικεφαλής της έρευνας. Σύμφωνα με το αρμόδιο τμήμα της Αστυνομίας Κύπρου οι επικεφαλής καλούν πάντα αρμόδιο προσωπικό για τη λήψη των πειστηρίων επί τόπου όταν πρόκειται για υποθέσεις που αφορούν σε ηλεκτρονικό έγκλημα ή παιδική πορνογραφία ενώ για τις υπόλοιπες υποθέσεις αποφασίζουν επί τόπου.

Η παρουσία του αρμόδιου προσωπικού στη σκηνή του εγκλήματος μπορεί να δώσει σημαντικό πλεονέκτημα στις ερευνητικές αρχές, ειδικά αν βρεθούν υπολογιστές ενεργοποιημένοι. Σε τέτοια περίπτωση το εξειδικευμένο προσωπικό μπορεί με τα κατάλληλα εργαλεία να εντοπίσει ακόμα και κωδικούς πρόσβασης για κρυπτογραφημένα αρχεία, να τα βρει αυτά τα αρχεία ανοικτά, ή και κωδικούς πρόσβασης σε ιστοσελίδες και γενικά να συλλέξει πληροφορίες οι οποίες βρίσκονται στην πτητική μνήμη του υπολογιστή η οποία με την απενεργοποίησή του για μεταφορά στο εργαστήριο θα διαγραφεί πλήρως. Επίσης το προσωπικό στη σκηνή μπορεί να ερευνήσει και να συλλέξει στοιχεία σχετικά με το δίκτυο υπολογιστών, εφόσον υπάρχει, ή και για

πιθανά εικονικά ιδιωτικά δίκτυα στα οποία ο υπολογιστής του υπόπτου μπορεί να είναι συνδεδεμένος και να διακινεί πληροφορίες.

Βάσει των παραπάνω ο τρόπος συλλογής των ψηφιακών πειστηρίων από το αρμόδιο προσωπικό χωρίζεται σε 2 γενικές κατηγορίες όπου εκτελείται και συλλέγονται διαφορετικού είδους στοιχεία στις οποίες η φιλοσοφία είναι ακριβώς η ίδια, τα συλλεγμένα στοιχεία να παραμείνουν ακέραια.

2.3.1. Συλλογή σε ενεργοποιημένες συσκευές

Επειδή στα αρχικά στάδια της ψηφιακής δικανικής η μέθοδος που ακολουθούσαν οι ερευνητές προέβλεπε την απενεργοποίηση του υπολογιστή πριν τη διεξαγωγή της συλλογής των ψηφιακών πειστηρίων, οι δημιουργοί κακόβουλου λογισμικού ξεκίνησαν να μειώνουν τα ίχνη τους στους σκληρούς δίσκους και να κάνουν περισσότερη χρήση της πτητικής μνήμης. Πλέον οι ερευνητές με τη χρήση των σύγχρονων εργαλείων που έχουν στη διάθεσή τους, αναλύουν γρήγορα την πτητική μνήμη και τη συμπεριλαμβάνουν ως μέρος των ψηφιακών πειστηρίων που είτε θα παρουσιάσουν, είτε θα κάνουν χρήση για περαιτέρω έρευνα [09].

Μετά τη συλλογή όλων των δεδομένων της πτητικής μνήμης, ο ερευνητής καλείται να δημιουργήσει ένα ακριβές αντίγραφο του σκληρού δίσκου του υπολογιστή που θα κληθεί να ελέγξει. Αυτό το αντίγραφο μπορεί να γίνει με τον υπολογιστή απενεργοποιημένο, όπως ήταν η παλαιότερη μέθοδος, αλλά τυχόν αρχεία, είτε ακόμα και ολόκληρος ο σκληρός δίσκος, είναι πολύ πιθανόν να είναι κρυπτογραφημένα με ειδικά προγράμματα τα οποία μπορεί ο καθένας πλέον να βρει και να χρησιμοποιήσει, όπως το truecrypt ή κατευθείαν από το λειτουργικό του σύστημα. Αν αυτά τα αρχεία βρεθούν ανοικτά τότε η λήψη του αντίγραφου μπορεί να γίνει κανονικά από τον ερευνητή και είναι και πολύ πιθανό να εντοπίσει και τον κωδικό κρυπτογράφησής τους είτε στην πτητική μνήμη είτε στον αδιάθετο χώρο, είτε ακόμα και στα δεδομένα που προστίθενται αυτόματα από τον υπολογιστή για τη συμπλήρωση μιας συστάδας δεδομένων.

Ο ερευνητής κατά τη διάρκεια συλλογής των πειστηρίων από ενεργοποιημένο υπολογιστή πρέπει να προσέξει να κάνει μόνο τα απαραίτητα, προκειμένου τα πειστήρια που θα συλλέξει να μπορούν να γίνουν αποδεκτά σε δικαστήριο, γιατί οποιαδήποτε ενέργειά του τροποποιεί το σύστημα. Επίσης θα πρέπει η διαδικασία που θα ακολουθήσει να καταγραφεί πλήρως και να μπορεί να αναπαραχθεί, παρόλο που τα αποτελέσματα είναι πολύ πιθανό να μην είναι τα ίδια καθώς η κατάσταση του συστήματος, που θα ελεγχθεί, δε θα είναι ποτέ η ίδια όπως ήταν πριν

τον έλεγχο.Σε αυτή την περίπτωση θα συλλεγούν επιπλέον στοιχεία με το κλείσιμο των εφαρμογών που τρέχουν, με την προϋπόθεση ότι θα γίνει από εξειδικευμένο προσωπικό. Για παράδειγμα όταν κλείσει ο Microsoft Internet Explorer θα αποθηκεύσει τα δεδομένα στο σκληρό δίσκο τα οποία αν απενεργοποιούταν ο υπολογιστής, θα διαγράφονταν [22]. Η σειρά ενεργειών, η οποία μπορεί να διαφέρει αναλόγως της κατάστασης, είναι η παρακάτω :

1. Πρώτα αποφασίζει αν η συλλογή θα γίνει τοπικά ή μέσω του δικτύου και αν θα γίνει απροκάλυπτα ή συγκαλυμμένα. Αυτή η απόφαση εξαρτάται άμεσα από τα εργαλεία που έχει στη διάθεσή του, από τις δυνατότητες που υπάρχουν στο εσωτερικό δίκτυο και από το ποιος είναι ο ύποπτος που θα ερευνηθεί.
2. Εφαρμόζει σύστημα προστασίας εγγραφής (writeblocker), είτε συσκευή, είτε λογισμικό με σκοπό να αποφύγει οποιαδήποτε εγγραφή δεδομένων η οποία θα κατάστρεφε την ακεραιότητα των αρχικών στοιχείων [14].

Εικόνα 2.1 :Φορητό writeblocker

3. Εντοπίζει τη στιγμή που θα πάρει το ακριβές αντίγραφο του υπολογιστή, αν ο χρήστης που είναι συνδεδεμένος έχει δικαιώματα διαχειριστή ή όχι. Από αυτό εξαρτάται άμεσα το τι εργασίες θα μπορέσει να εκτελέσει ο ερευνητής.

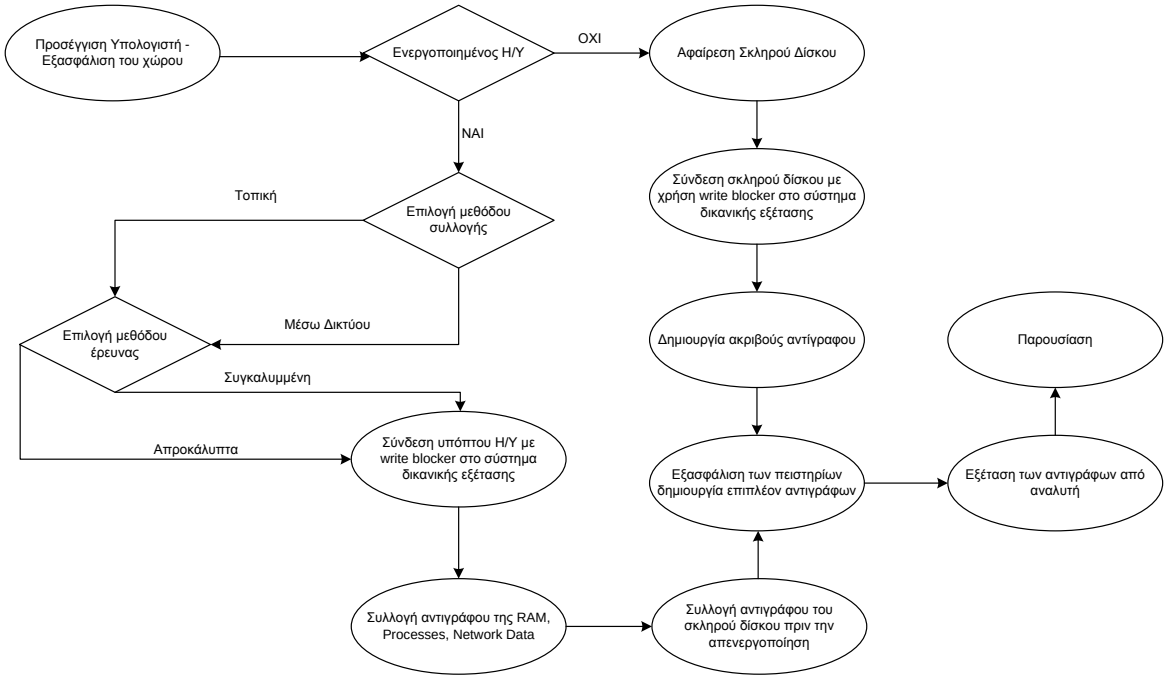
4. Απαραίτητος είναι και ο καθορισμός αν ο λογαριασμός που θα εξεταστεί είναι σε πραγματικό ή εικονικό περιβάλλον. Αν και στην ουσία η διαδικασία που θα ακολουθηθεί είναι η ίδια, ο ερευνητής θα χρειαστεί περαιτέρω ανάλυση για να συλλέξει το ακριβές αντίγραφο του αρχικού συστήματος και ταυτόχρονα και όλων των πιθανών εικονικών που θα υπάρχουν. Ο καθορισμός δεν είναι εύκολος αν και υπάρχουν ορισμένα στοιχεία τα οποία μπορούν να εντοπισθούν και εξαρτάται άμεσα από το λειτουργικό σύστημα.
5. Συλλέγει αντίγραφα της πτητικής μνήμης (RAM), των διεργασιών (process), πληροφορίες για το σύστημα και για το δίκτυο (ports, ipaddresses, macaddresses, arptable).
6. Συλλέγει αντίγραφο του σκληρού δίσκου και των λοιπών μέσων αποθήκευσης πριν απενεργοποιήσει τον υπολογιστή καθώς είναι πολύ πιθανό να μην μπορεί να το πράξει μετά λόγω κρυπτογράφησης τους. Πολύ πιθανό λόγω τεχνικών περιορισμών ο ερευνητής να μην καταφέρει να συλλέξει όλα τα δεδομένα του προς εξέταση υπολογιστή και να χρειαστεί να κάνει διαλογή των αρχείων που θεωρεί ως πιο σημαντικά για συλλογή και εξέταση.
7. Με το πέρας της συλλογής εξάγει τη hashvalue των πρωτοτύπων και των αντιγράφων που έλαβε για να αποδείξει στο δικαστήριο ότι οι εργασίες που έκανε στα επόμενα αντίγραφα που θα αναπαράγει δεν τα αλλοίωσαν.[14]

2.3.2. Συλλογή σε μη ενεργοποιημένες συσκευές

Η μέθοδος αυτή ακολουθείται συνήθως στο εργαστήριο ψηφιακής δικανικής του εκάστοτε οργανισμού ασφαλείας εκτός και αν οι περιστάσεις προστάζουν να γίνει στη σκηνή του εγκλήματος. Σαν διαδικασία μειονεκτεί σε σχέση με τη διαδικασία με ενεργοποιημένες συσκευές στο ότι χάνονται όλα τα στοιχεία που βρίσκονται στην πτητική μνήμη, καθώς επίσης και τα δεδομένα δικτύου. Επίσης μπορεί να υπάρξει απώλεια εισοδήματος για τον οργανισμό ή το φυσικό πρόσωπο στις συσκευές του οποίου γίνεται ο έλεγχος σε περίπτωση που η λειτουργία τους είναι απαραίτητη προϋπόθεση για την παραγωγή εισοδήματος ή την εξυπηρέτηση πελατών. Υπάρχει τέλος μεγάλη πιθανότητα να μην καταφέρουν να αποκρυπτογραφήσουν τα δεδομένα που θα συλλεγούν σε περίπτωση που ο ιδιοκτήτης του συστήματος δεν είναι συνεργάσιμος και δε δίνει τους κωδικούς.

Πρακτικά δε διαφέρει σε τίποτα από την προηγούμενη σαν διαδικασία, πλεονεκτεί όμως στο γεγονός ότι είναι πιο εύκολο για τον ερευνητή να αποδείξει στο δικαστήριο ότι δεν αλλοίωσε κανένα από τα πειστήρια που παρουσιάζει και ότι μπορεί να συλλέξει όλα τα δεδομένα χωρίς να αναγκαστεί να κάνει διαλογή στη φάση της συλλογής.

2.3.3. Συνοπτικό Σχεδιάγραμμα Διαδικασίας Συλλογής Ψηφιακών Πειστηρίων [14]



Κεφάλαιο 3
Ψηφιακή Δικανική στον Κυβερνοπόλεμο

Μέχρι στιγμής δεν έχει υπάρξει συμφωνία για το τι ακριβώς είναι ο κυβερνοπόλεμος. Επίσης δεν υπάρχει συμφωνία για το τι είναι ο κυβερνοχώρος και γι αυτό θα χρησιμοποιηθεί ο όρος του Αμερικανικού Υπουργείου Άμυνας που τον ορίζει ως ένα παγκόσμιο πεδίο, όπου το πληροφοριακό περιβάλλον αποτελείται από αλληλοεξαρτώμενα δίκτυα τεχνολογικών υποδομών. Αυτά περιλαμβάνουν εκτός από το Διαδίκτυο, τα τηλεπικοινωνιακά δίκτυα, τα συστήματα Η/Υ και ενσωματωμένους επεξεργαστές και ελεγκτές. Ο κυβερνοχώρος είναι ευρέως αναγνωρισμένος ως το 5ο πεδίο επιχειρήσεων μαζί με τα 4 παραδοσιακά αναγνωρισμένα από τον στρατό, ξηρά, θάλασσα, αέρα και διάστημα, με τη διαφορά ότι μπορεί να λειτουργήσει αυτόνομα και χωρίς την απαραίτητη εμπλοκή κάποιου από τα υπόλοιπα 4, ενώ δε νοείται πλέον η εκμετάλλευση κάποιου από τα παραδοσιακά χωρίς την απαραίτητη υποστήριξη από τον κυβερνοχώρο [15,23].

Βάσει του ορισμού του κυβερνοχώρου θα χρησιμοποιήσουμε και πάλι το λεξικό του Αμερικανικού Υπουργείου Άμυνας και θα πούμε ότι ο κυβερνοπόλεμος αντιστοιχεί με τις επιχειρήσεις στον κυβερνοχώρο και είναι η εκμετάλλευση των δυνατοτήτων του κυβερνοχώρου με κύριο σκοπό να επιτευχθούν αντικειμενικοί σκοποί μέσα ή μέσω αυτού. Θα μπορούσαμε όμως να πούμε και ότι είναι κάθε εικονική σύγκρουση που ξεκίνησε ως μια πολιτικά υποκινούμενη επίθεση στον υπολογιστή και τα συστήματα πληροφοριών του εχθρού. Γενικά περιλαμβάνει στρατιωτικές δραστηριότητες, επιθετικές ή αμυντικές, που συνεπάγονται δίκτυα πληροφοριών, και ειδικότερα το Διαδίκτυο, περιλαμβανόμενων κατασκοπίας και αντικατασκοπίας.

3.1. Ενέργειες Κυβερνοπολέμου

Οι ενέργειες που είναι δυνατόν να παρουσιαστούν σε επιχειρήσεις στον κυβερνοχώρο είναι διαφόρων τύπων και είναι ανάλογες του επιπέδου των δυνατοτήτων του κάθε αντιπάλου καθώς και του αντικειμενικού του σκοπού. Όπως και στον παραδοσιακό πόλεμο η πρωτοβουλία ανήκει στον επιτιθέμενο με τη μεγάλη διαφορά ότι ο δεχόμενος την επίθεση δεν είναι υποχρεωμένος να περιμένει την απορρόφηση της επιθετικής ορμής του αντιπάλου για να αναλάβει την πρωτοβουλία διεξαγωγής επιθετικών επιχειρήσεων. Μια τυπική ταξινόμηση των ενεργειών κυβερνοπολέμου είναι η παρακάτω :

3.1.1. Εκμετάλλευση – Exploitation

Αυτές οι ενέργειες κατευθύνονται σε στόχους στον κυβερνοχώρο και έχουν ως σκοπό την κυρίευση δεδομένων και πληροφοριών, κυρίως χωρίς να προκαλούν ζημιές στα στοχοποιημένα συστήματα. Αυτό συνήθως επιτυγχάνεται με την απόκτηση πρόσβασης σε δίκτυα ή μεμονωμένα συστήματα. Μπορεί να περιλαμβάνει κυβερνοκατασκοπία είτε για λήψη μόνο στρατιωτικών πληροφοριών, είτε και για πολιτικοοικονομικών [15].

3.1.2. Αποδιοργάνωση – Disruption

Ενέργειες τέτοιου είδους έχουν ως σκοπό την πρόκληση ζημιών σε πληροφοριακά συστήματα, περιορίζοντας με διάφορους τρόπους τις ικανότητές τους. Αυτές οι επιθέσεις μπορεί να είναι από απλές επιθέσεις άρνησης υπηρεσίας DOS/DDOS (DenialOfService) μέχρι στοχοποιημένες εισχωρήσεις. Σε περιπτώσεις βιομηχανικών δικτύων τέτοιου είδους ενέργειες είναι πιθανόν να

δημιουργήσουν και υλικές καταστροφές σε φυσικά αγαθά και όχι μόνο σε πληροφοριακά συστήματα [15].

3.1.3. Πληροφοριακές Επιχειρήσεις – InformationWarfare

Σε στρατιωτικό πλαίσιο οι ψυχολογικές επιχειρήσεις (ΨΕΠ) υπήρχαν ανέκαθεν, όμως τα σύγχρονα πληροφοριακά δίκτυα και ο κυβερνοχώρος έχουν δώσει στην προπαγάνδα ένα τελείως καινούριο πεδίο ανάπτυξης. Η επιρροή μπορεί να επιτευχθεί στις σύγχρονες κοινωνίες μέσω Διαδικτυακών επιχειρήσεων, όπως για παράδειγμα με τη χρήση κοινωνικών δικτύων, μπλογκς και ιστοσελίδων [15].

3.1.4. ΚυβερνοφυσικέςΕπιθέσεις – Cyberphysicalattacks

Όταν συστήματα βιομηχανικών αυτοματισμών ή ελέγχου υποδομών γίνονται στόχοι, ενέργειες αποδιοργάνωσης μπορούν να προκαλέσουν ζημιά σε φυσικά αγαθά και όχι μόνο σε πληροφοριακά συστήματα. Κλασσικό παράδειγμα το οποίο έκανε ευρέως γνωστή αυτή την κατηγορία κυβερνοπολέμου ήταν το Stuxneto οποίος θεωρείται και το μέλλον του κυβερνοπολέμου [15,26].

3.2. Χρήση Εμπορικών Τεχνολογιών και Συνέπειες

Ο διαχωρισμός των πρωτοκόλλων που χρησιμοποιούνταν σε παλαιότερα χρόνια καθώς και τεχνολογιών που αναπτύσσονταν ανεξάρτητα από κάθε παραγωγό εταιρία τείνει να εκλείψει. Ακόμα και ο στρατός που είχε πληθώρα αποκλειστικών τεχνολογιών, μέχρι και λειτουργικά - δικτυακά συστήματα, έχει οδηγηθεί στη χρήση εμπορικών τεχνολογιών σε εκπληκτικά μεγάλο βαθμό. Το γεγονός αυτό καθώς και η αυξανόμενη διεπαφή των υποδομών και των στρατιωτικών συστημάτων, προφανώς διευκολύνει τους επιτιθέμενους.

Το μέλλον θα φέρει ακόμα περισσότερες διεπαφές και διάχυτα δίκτυα με την προοδευτική ανάπτυξη του IPv6 και το διευρυμένο πεδίο διευθύνσεών του. Το αποτέλεσμα θα είναι μεγαλύτερη τρωτότητα του ελέγχου και των οπλικών συστημάτων. Έχουμε ήδη γίνει θεατές επιθέσεων σε λογισμικό μη επανδρωμένων αεροσκαφών από κακόβουλο λογισμικό το οποίο θα μπορούσε να χρησιμοποιηθεί και για την προσβολή ενός συστήματος σε ένα επιτελικό γραφείο

για υποκλοπή πληροφοριών ακόμα και για παραμόρφωση ιστοτόπων για ψυχολογικές επιχειρήσεις [15].

3.3. Ψηφιακή Δικανική στα Πλαίσια του Κυβερνοπολέμου

Οι αρχές και οι διαδικασίες της ψηφιακής δικανικής, αρχίζοντας από την επίγνωση και την προπαρασκευή διαδικασιών, έχουν ενσωματωθεί στη διαχείριση των δικτυακών θεμάτων με τον κίνδυνο εκδήλωσης μιας κυβερνοεπίθεσης. Αυτό αφορά κυρίως συστήματα στρατιωτικού τύπου και λιγότερο πολιτικού, όπως κρίσιμες δικτυακές υποδομές. Είναι πολύ βασικό γιατί επιτρέπουν τη συλλογή τεκμηρίων επιθέσεων ή από απόπειρες επιθέσεων, ενώ ταυτόχρονα αποκαθιστούν τη λειτουργικότητα των συστημάτων. Η χρήση των συλλεγόμενων τεκμηρίων μπορεί να αφορά από εσωτερική χρήση μέχρι και παρουσίασή τους σε διεθνές δικαστήριο ή σε διεθνή οργανισμό όπως το συμβούλιο ασφαλείας των Ηνωμένων Εθνών. Στα πλαίσια του κυβερνοπολέμου τα τεκμήρια που θα συλλεχθούν και θα τύχουν ανάλυσης δε θα περιορίζονται σε αυτά που βρίσκονται στους υπολογιστές και σε συσκευές έξυπνων κινητών, αλλά θα επεκταθούν και στα δίκτυα πλησιάζοντας τη χρήση και λειτουργία των συστημάτων ανίχνευσης επιθέσεων, καθώς και στην ανάλυση κακόβουλου λογισμικού [15].

Η δικανική δικτύων είναι ίσως το πιο σημαντικό πεδίο δικανικής στις στρατιωτικές επιχειρήσεις, κυρίως λόγω του ότι η πλειονότητα των επιθέσεων χρησιμοποιεί δίκτυα, είτε δημόσια είτε ιδιωτικά. Επίσης είναι και η πιο προβληματική, όπου η ανάπτυξη της διαδικασίας ετοιμότητας είναι κυρίαρχη. Η κίνηση στο δίκτυο που ασφαλίζεται πρέπει να παρακολουθείτε και να συλλέγεται σε τακτική βάση, έτσι ώστε μετά από τις συνέπειες μιας επίθεσης να υπάρχουν δεδομένα για να αναλυθούν για να βρεθεί η αιτία και η πηγή της επίθεσης. Επίσης να ελεγχθεί η φορά της επίθεσης και κατά πόσο συνεχίζεται ή όχι. Πολύτιμα εργαλεία για τέτοια ανάλυση είναι οι διάφοροι ανιχνευτές δικτύων οι οποίοι έχουν δυνατότητα να κάνουν διαχωρισμό πρωτοκόλλων σε διάφορα επίπεδα, από το φυσικό μέχρι και το επίπεδο μεταφοράς λαμβάνοντας υπόψη τους διάφορους συμπερασμούς των ενθυλακώσεων [15].

Πέραν αυτών, λογισμικό ενσωματωμένο σε συσκευές δικτύων ή βιομηχανικών συστημάτων αποτελεί λογισμικό το οποίο δεν είναι εύκολο να αναλυθεί με τα σημερινά υπάρχοντα εργαλεία είναι επικίνδυνο να στοχοποιηθεί σε μια κυβερνοεπίθεση. Η καλύτερη λύση για τον έλεγχο της ακεραιότητας αυτών των συστημάτων είναι η διατήρηση εκτός σύνδεσης αντίγραφου του

λογισμικού αυτού και η σύγκρισή του με τα εν λειτουργία σε περίπτωση που υπάρχει υποψία για επίθεση.

3.4. Εντοπισμός και Ανάλυση Κακόβουλου Λογισμικού

Το 2012 ανακοινώθηκε από τη Symantec ότι περισσότερα από 403 εκατομμύρια δείγματα κακόβουλου λογισμικού αναγνωρίστηκαν από όλους τους κατασκευαστές λογισμικών ασφαλείας, αναλύθηκαν και έγιναν υπογραφές που τοποθετήθηκαν στις βάσεις δεδομένων που χρησιμοποιούν για τον εντοπισμό τους. Παρά την ύπαρξη όλων αυτών των υπογραφών κάθε χρόνο είναι πάρα πολύ συνηθισμένο το κακόβουλο λογισμικό να μπορεί να ξεφύγει από τον έλεγχο των λογισμικών ασφαλείας και να εισέρχεται στα υπολογιστικά συστήματα. Από τη στιγμή που ένα σύστημα έχει δεχτεί τέτοιου είδους επίθεση αυτόματα θεωρείται ότι δεν είναι έμπιστο αν δε διαμορφωθεί από την αρχή καθώς είναι αδύνατο να είναι κάποιος απόλυτα σίγουρος ότι οποιοσδήποτε καθαρισμός με ένα λογισμικό ασφαλείας μπορεί να είναι τέλειος [11].

Κάθε κακόβουλο λογισμικό είναι διαφορετικό και έχει διαφορετική συμπεριφορά σε κάθε συσκευή. Το μόνο τους κοινό χαρακτηριστικό είναι ότι βρίσκουν τρόπο να εισχωρήσουν στον υπολογιστή του θύματος με τη χρήση ενός αρχείου, το οποίο θεωρείται ωφέλιμο από τον υπολογιστή, και προσπαθούν να παραμείνουν κρυμμένα. Αυτό που πρέπει να βρεθεί είναι το αρχείο φορέας που εισήλθε στο σύστημα στην αρχή έτσι ώστε να απαγορευτεί η επανεμφάνισή του. Για να γίνει αυτό τα λογισμικά ασφαλείας συγκρίνουν τις γνωστές υπογραφές της βάσης δεδομένων που διαθέτουν για κακόβουλο λογισμικό με όλα τα αρχεία που βρίσκονται στον υπολογιστή. Αν όμως έχει αλλάξει μόνο ένα bit από το κακόβουλο λογισμικό τότε η υπογραφή του δε θα είναι η ίδια και θα περάσει από τον έλεγχο υπογραφών χωρίς να εντοπισθεί.

Το να εντοπιστεί κακόβουλο λογισμικό του οποίου η υπογραφή δεν έχει περαστεί στις βάσεις δεδομένων των λογισμικών ασφαλείας είναι κάτι πολύ δύσκολο να γίνει ακόμα και από εξειδικευμένο προσωπικό. Σε έναν υπολογιστή όπου υπάρχει εγκατεστημένο λογισμικό ασφαλείας, νόμιμο λειτουργικό και λοιπό λογισμικό τα οποία είναι και ενημερωμένα, θα πρέπει να παρατηρήσουμε για τυχόν συμπτώματα όπως μειωμένη λειτουργικότητα, περίεργη συμπεριφορά, ύποπτη κίνηση στο δίκτυο, αρχεία που δε γνωρίζουμε τι είναι και με περίεργες ονομασίες κλπ. Το να απαλλαγούμε από αυτά δεν είναι και ότι πιο εύκολο, αλλά δεν είναι και αδύνατο. Σε έναν ιδιωτικό υπολογιστή όπου δεν υπάρχει υποψία κυβερνοπολέμου το μόνο που

έχουμε να κάνουμε είναι να ακολουθήσουμε τη διαδικασία για να επανέλθουμε σε μια προηγούμενη ημερομηνία, πριν να παρατηρήσουμε τα συμπτώματα, και κατά πάσα πιθανότητα θα έχουμε πετύχει την απαλλαγή μας από το κακόβουλο λογισμικό.

Στην περίπτωση όμως του κυβερνοπολέμου ο στόχος δεν είναι μόνο η απαλλαγή από το κακόβουλο λογισμικό, αλλά ο εντοπισμός του και η ανάλυσή του. Να αντιληφθούμε δηλαδή τι ενέργειες εκτελεί, αν στέλνει δεδομένα και σε ποιον, πότε εισήλθε στο σύστημα, μέσω ποιου λογαριασμού και αν δημιουργεί επιπλέον προβλήματα που δε φαίνονται από τα συμπτώματα [04]. Σε αυτή την περίπτωση ο ερευνητής θα πρέπει να ξεκινήσει μια σειρά ελέγχων, όσο το δυνατόν πιο διακριτικά με σκοπό ο επιτιθέμενος να μην αντιληφθεί την έρευνα. Η μέθοδος που ακολουθείται είναι συγκαλυμμένη έρευνα μέσω δικτύου σε ενεργοποιημένο υπολογιστικό σύστημα. Καταγράφεται η πτητική μνήμη RAM, όλες οι διεργασίες που εκτελούνται και τα δεδομένα δικτύου. Γίνεται έλεγχος αρχικά για ύποπτες διεργασίες, όπως για παραποιημένα ονόματα διεργασιών, άγνωστες διεργασίες ή ύποπτη κατανάλωση πόρων. Επίσης ελέγχουμε τα δεδομένα δικτύου, αν έχει δημιουργηθεί κάποια εικονική σύνδεση με μια άγνωστη διεύθυνση, αν έχουν ανοιχτεί θύρες που δεν θα έπρεπε να είναι ανοιχτές, ή μη αναμενόμενες συνδέσεις σε μη αναμενόμενες θύρες και τέλος ελέγχουμε και τα αρχεία καταγραφής του αναχώματος ασφαλείας (firewall) και του δρομολογητή για καταγραμμένες προσπάθειες αποστολής δεδομένων σε απαγορευμένες διευθύνσεις. Επίσης ελέγχουμε τις διαμορφώσεις των δρομολογητών, μεταγωγέων και αναχωμάτων ασφαλείας, συγκρίνοντάς τις με τις εκτός δικτύου που έχουμε αποθηκεύσει για ενδεχόμενο αλλαγής τους από τον κακόβουλο.

Αφού έχουν γίνει τα παραπάνω κι έχουν συγκεντρωθεί οι απαραίτητες πληροφορίες και αναλόγως των οδηγιών που θα πάρει ο ερευνητής τότε μπορεί να ξεκινήσει την προσπάθεια για τον εντοπισμό του κακόβουλου λογισμικού εντός του υπολογιστή η οποία είναι μια διαδικασία που είναι καλύτερα να γίνει σε safemode. Η διαδικασία μπορεί να περιλαμβάνει αρχεία με άγνωστα ονόματα ή παραποιημένα, αρχεία μέσα σε φακέλους του λειτουργικού συστήματος, ή ακόμα και μέσα σε AlternateDataStreams (ADS) όπου τα περισσότερα λογισμικά ασφαλείας δεν ελέγχουν για κακόβουλο λογισμικό. Όταν το κακόβουλο λογισμικό εντοπιστεί είναι καλύτερα να διαγραφεί όταν ο υπολογιστής είναι στο safemode.

Γενικά οι διαδικασία για εντοπισμό, ανάλυση και διαγραφή ενός κακόβολου λογισμικού είναι μια πολύ δύσκολη διαδικασία η οποία δε μπορεί να εκτελεστεί από κάποιον εξειδικευμένο μόνο στην ψηφιακή δικανική και στα εργαλεία της. Ο ερευνητής θα πρέπει να γνωρίζει άριστα το εκάστοτε λειτουργικό που ερευνά και η χρήση των εργαλείων είναι για διευκόλυνση της εργασίας του,

αύξηση της ταχύτητας και να του παρέχει δυνατότητα συγκάλυψης στα αρχικά στάδια μέχρι να αποκαλύψει την πηγή της επίθεσης.

3.5. Παραδείγματα Κυβερνοπολέμου

Δύο παραδείγματα κυβερνοπολέμου υπάρχουν επίσημα καταγραμμένα παρά το ότι δεν είναι κοινά αποδεκτά από όλους τους εμπλεκομένους. Και στα δύο φαίνεται η αδυναμία εντοπισμού των δραστών με δικανικό τρόπο έτσι ώστε να μπορέσουν τα θύματα να αντιδράσουν νομικά είτε σε διεθνές δικαστήριο, είτε σε διεθνείς οργανισμούς.

3.5.1. Εσθονία 2007

Τα γεγονότα από τις 27 Απρ 2007 και διάρκειας τριών εβδομάδων χαρακτηρίστηκαν ως ο πρώτος κυβερνοπόλεμος από πολλούς. Οι γεωπολιτικές εξελίξεις της περιοχής οδήγησαν στη διαμάχη της Ρωσίας με την Εσθονία με αφορμή τη μετακίνηση ενός αγάλματος. Ταυτόχρονα με όσα έλαβαν χώρα στο φυσικό χώρο εκδηλώθηκε και μια πρωτοφανώς συντονισμένη επίθεση στον κυβερνοχώρο εναντίον της Εσθονίας η οποία ήταν (και παραμένει μέχρι και σήμερα) μια χώρα με κλίση στην τεχνολογία που εφάρμοζε σε μεγάλο βαθμό την ηλεκτρονική διακυβέρνηση. Η επίθεση είχε δύο μέτωπα, το ένα ήταν το κυβερνητικό και το δεύτερο στόχευε την κοινωνία. Η μέθοδος ήταν η κατανεμημένη άρνηση εξυπηρέτησης (dDOS) και κτυπήθηκαν κυβερνητικές υπηρεσίες, τηλεπικοινωνιακές υποδομές, τράπεζες και μεγάλες ιδιωτικές εταιρείες.

Σε αυτό το γεγονός αναδείχτηκε η αδυναμία εντοπισμού των δραστών λόγω μη απαραίτητης προετοιμασίας των αρχών της Εσθονίας, αλλά και αδυναμία αντιμετώπισης της κατάστασης με αποτέλεσμα να μη μπορεί είτε να κινηθεί νομικά, είτε να ενεργοποιήσει την Interpol, αλλά ούτε και να καταφέρει να πετύχει τη συνεργασία της Ρωσίας [28].

3.5.2. Γεωργία 2008

Και σε αυτή την περίπτωση οι λόγοι είναι γεωπολιτικοί όπως και πριν με τη διαφορά ότι εδώ το πεδίο δράσης δεν ήταν ο κυβερνοχώρος μόνο, αλλά επεκτάθηκε και στα υπόλοιπα 4 φυσικά πεδία με τον κυνερνοπόλεμο να είναι υποστηρικτικός στις παραδοσιακές στρατιωτικές επιχειρήσεις που έλαβαν χώρα. Οι στόχοι ήταν στρατιωτικές τηλεπικοινωνιακές υποδομές της Γεωργίας.

Η αδυναμία εντοπισμού των ενόχων γι αυτή την καταστροφική για τη Γεωργία επίθεση είναι ακόμα ένα κοινό χαρακτηριστικό με την επίθεση στην Εσθονία. Το γεγονός ότι στελέχη της κυβέρνησης της Γεωργίας κατηγόρησαν τη Ρωσία για την επίθεση δεν οδήγησε σε κάποιο αποτέλεσμα [28].

Κεφάλαιο4
Κλάδοι Ψηφιακής Δικανικής

Όπως προαναφέρθηκε η ψηφιακή δικανική είναι ένας κλάδος της επιστήμης της δικανικής η οποία αφορά στη συλλογή και ανάλυση πειστηρίων από ψηφιακές συσκευές που έχουν συμμετοχή είτε σε υποθέσεις ηλεκτρονικού ή άλλου είδους εγκλήματος είτε σε κυβερνοεπιθέσεις. Η συμβολή αυτού του κλάδου είναι στην αναγνώριση ενός εγκλήματος, εντοπισμός των ενόχων και προσαγωγή τους στη δικαιοσύνη, επαλήθευση των ισχυρισμών και επαλήθευση αυθεντικότητας εγγράφων. Σήμερα αποτελεί το πιο πολύπλοκο τμήμα της δικανικής, λόγω της ταχείας ανάπτυξης της πληροφορικής και γενικά των ηλεκτρονικών επικοινωνιών και λόγω των προβλημάτων και δυσχερειών που αντιμετωπίζονται.

Οι κλάδοι που την αποτελούν είναι η δικανική υπολογιστών, κινητών συσκευών και δικτύων.

4.1. Δικανική Υπολογιστών

Η δικανική υπολογιστών είναι η εφαρμογή τεχνικών έρευνας και ανάλυσης για συλλογή και διατήρηση τεκμηρίων από συγκεκριμένη συσκευή ηλεκτρονικού υπολογιστή ή ψηφιακού μέσου αποθήκευσης με τρόπο ο οποίος να είναι αποδεκτός για παρουσίασή του στο δικαστήριο. Στόχος είναι η υλοποίηση μιας δομημένης έρευνας με παράλληλη διατήρηση μιας καταγεγραμμένης αλυσίδας φύλαξης για να βρεθεί πέραν κάθε αμφιβολίας το τι συνέβη σε έναν ηλεκτρονικό υπολογιστή και ποιος ήταν ο υπαίτιος. [18]

4.2. Δικανική Κινητών Συσκευών

Η δικανική κινητών συσκευών είναι η ανάκτηση των ψηφιακών πειστηρίων από κινητές συσκευές, όχι υπολογιστές και ψηφιακά μέσα αποθήκευσης, με τρόπο ο οποίος να είναι αποδεκτός από το δικαστήριο. Η εξέλιξη των συσκευών αυτών τα τελευταία χρόνια έχει καταστήσει υποχρεωτική τη δημιουργία και ανάπτυξη του κλάδου διότι αυτές οι συσκευές πλέον έχουν πάρει ένα πολύ μεγάλο μερίδιο της αγοράς των ηλεκτρονικών υπολογιστών και είναι ικανές να αποθηκεύσουν τεράστιο όγκο δεδομένων. Σήμερα αυτός ο κλάδος παρουσιάζει τη μεγαλύτερη δυσκολία στους ερευνητές λόγω της μεγάλης ποικιλομορφίας των συσκευών, λειτουργικών συστημάτων, απουσία σκληρών δίσκων, διαφορετικά συστήματα αρχείων και διαφορετικοί πάροχοι. Τα σημερινά εργαλεία δικανικής έχουν αρχίσει να περιλαμβάνουν εργαλεία για συλλογή και ανάλυση δεδομένων για τέτοιου είδους συσκευές, αλλά με πολλούς περιορισμούς.

Σε σχέση με τη δικανική υπολογιστών υπάρχουν σημαντικές διαφορές καθώς η ανάλυση μιας κινητής συσκευής περιλαμβάνει εκτός από τη συλλογή και ανάλυση αποθηκευμένων αρχείων, την ανάλυση όλων των καρτών SIM που πιθανόν να υπάρχουν, την ενσωματωμένη μνήμη της συσκευής, ανάλυση πληροφοριών του παρόχου, του λειτουργικού συστήματος και έλεγχο των υπηρεσιών που βασίζονται στο cloud [19].

4.3. Δικανική Δικτύων

ΣύμφωναμετοDigitalForensicsResearchWorkshoptου 2001 ηδικανική Δικτύων είναι η χρήση επιστημονικά αποδεδειγμένων στοιχείων από πολλαπλές, ενεργές ψηφιακές πηγές, επεξεργασίας και μετάδοσης, με σκοπό την αποκάλυψη γεγονότων σχετικών με την προσχεδιασμένη πρόθεση, ή τη μετρήσιμη επιτυχία των μη εξουσιοδοτημένων ενεργειών που έχουν ως σκοπό τη διατάραξη, φθορά, ή και τον κίνδυνο των συστατικών ενός συστήματος, καθώς και την παροχή πληροφοριών ώστε να βοηθήσει στην απάντηση ή την επαναφορά από αυτές τις ενέργειες.

Πρακτικά η δικανική δικτύων αφορά περισσότερο στην αντιμετώπιση κακόβουλων ενεργειών από εξωτερικούς κακόβουλους οι οποίες με την ανάπτυξη των δικτύων και ειδικότερα του Διαδικτύου έχουν αυξηθεί. Παλαιότερα αρκούσε μόνο να γίνει μια έρευνα στα αρχεία καταγραφής των δρομολογητών, μεταγωγέων και αναχωμάτων ασφαλείας. Τώρα οι κακόβουλοι έχουν εξελιχθεί και αυτές οι μέθοδοι δε δίνουν ικανοποιητικές απαντήσεις στο τι ακριβώς έγινε, αλλά και στο πώς έγινε, έτσι ώστε όχι μόνο να μην ξανασυμβεί αλλά και να αντιμετωπισθεί με ανάλογο τρόπο.

Συνήθως η δικανική δικτύων δεν έχει να κάνει τόσο με κοινά εγκλήματα που ερευνούν οι αστυνομικές αρχές, όσο με γεγονότα κυβερνοπολέμου ή κατασκοπίας οποιουδήποτε είδους. Όταν ερευνάται ένα τέτοιο γεγονός δε γίνεται μια απλή αντιστοίχιση των δραστηριοτήτων που παρατηρήθηκαν σε ένα δίκτυο, με μια βάση δεδομένων που περιέχει τις υπογραφές γνωστών κακόβουλων ενεργειών, αλλά γίνεται συνεχής καταγραφή όλων των δραστηριοτήτων στο τοπικό δίκτυο τα οποία αναλύονται σε πραγματικό χρόνο από εξειδικευμένα εργαλεία με τη συμβολή του ερευνητή, του οποίου ο ρόλος είναι αναβαθμισμένος σε τέτοιου είδους ενέργειες. Τα εργαλεία που έχουν αναπτυχθεί γι αυτόν τον κλάδο λειτουργούν με τρόπο που να προσομοιάζουν με τα εργαλεία που χρησιμοποιούνται για ανιχνεύσεις παρείσφρησης.

Η διαφορά που υπάρχει μεταξύ των εργαλείων ανιχνεύσεων παρείσφρησης και των εργαλείων δικανικής δικτύων είναι ότι τα πρώτα ενδιαφέρονται για την ανίχνευση εισβολών ή την παραβίαση των πολιτικών ασφαλείας ενώ τα δεύτερα ενδιαφέρονται για την κίνηση η οποία δεν παρουσιάζει οποιοδήποτε πρόβλημα. Επίσης τα συστήματα ανίχνευσης παρείσφρησης δεν καταγράφουν τα δεδομένα που συλλέγουν διότι λόγω του ότι πρέπει να παρακολουθούν πολλά συστήματα ταυτόχρονα σε ένα δίκτυο είναι τόσο μεγάλος ο όγκος των δεδομένων που η ανάλυσή τους γίνεται σε πραγματικό χρόνο, ενώ τα εργαλεία δικανικής δικτύων είναι

αναγκασμένα να κρατούν αντίγραφο της κίνησης του δικτύου το οποίο μπορεί να αναγκαστεί ο ερευνητής να το παρουσιάσει στο δικαστήριο.

Κεφάλαιο 5
Νομικά Θέματα

Στην Κυπριακή Δημοκρατία ο νόμος που αφορά στην αντιμετώπιση του ηλεκτρονικού εγκλήματος είναι ο Ν.22(ΙΙΙ)/2004 [25] που επικυρώνει τη Σύμβαση του Συμβουλίου της Ευρώπης κατά του Εγκλήματος μέσω Διαδικτύου (ΣΣΕΕΔ) [38], ο οποίος έχει υπογραφεί από τους Υπουργούς Εξωτερικών των κρατών μελών στις 23 Νοε 2001 στη Βουδαπέστη.

Κοινό χαρακτηριστικό για τη στοιχειοθέτηση των εγκλημάτων που προβλέπονται στη νομοθεσία είναι ο δράστης να έχει πρόθεση να τελέσει το αδίκημα και να ενεργεί χωρίς δικαίωμα. Το ακριβές νόημα της πρόθεσης δεν καθορίζεται από τη Σύμβαση του 2001, αλλά αφήνεται η ερμηνεία του να δοθεί από την κάθε χώρα. Η έννοια της φράσης χωρίς δικαίωμα ερμηνεύεται από τη Σύμβαση ως ενέργειες που έγιναν χωρίς νομική, πολιτική, δικαστική ή διοικητική εξουσιοδότηση ή ενέργειες που δεν τυγχάνουν οποιασδήποτε νομικής υπεράσπισης, δικαιολογίας, αιτιολογίας ή σχετικής αρχής σύμφωνα με τον νόμο του εκάστοτε κράτους μέλους.

Με αυτόν τον τρόπο αποποινικοποιούνται ενέργειες που έγιναν με νόμιμη κυβερνητική εξουσιοδότηση και ενέργειες που έγιναν με εξουσιοδότηση από τον ιδιοκτήτη του επηρεαζόμενου πληροφοριακού συστήματος.

Ταυτόχρονα όμως αποποινικοποιείται και η μη λήψη μέτρων από τους ιδιοκτήτες ή δικαιούχους, για αποφυγή και αποτροπή τέτοιων ενεργειών μέσω πληροφοριακών συστημάτων ή υπολογιστών που έχουν στην κατοχή τους. Αυτό μπορεί να θεωρηθεί ως η κύρια αιτία διάδοσης κακόβουλων προγραμμάτων αφού η λειτουργία και διάδοσή τους από υπολογιστές, άνευ πρόθεσης των ιδιοκτητών, δεν θεωρείται αξιόποινη πράξη. Ως αποτέλεσμα είναι η μη λήψη των απαραίτητων μέτρων προστασίας από κακόβουλο λογισμικό, όπως η προμήθεια λογισμικού που αφορά στην ασφάλεια των υπολογιστών καθώς και η ενημέρωση του λειτουργικού συστήματος και λοιπών προγραμμάτων.

5.1. Αδικήματα και Στόχοι προς Επίτευξη

Ακολουθεί η επιγραμματική αναφορά των αδικημάτων που αναφέρονται στη σύμβαση κι έχουν επικυρωθεί με το Ν.22(ΙΙΙ)/2004 της Κυπριακής Δημοκρατίας με σύντομη επεξήγηση των σκοπών που έχουν σαν στόχο να επιτύχουν.

5.1.1. Αδικήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών.

Παράνομη Πρόσβαση (άρθρο 4 Ν.22(ΙΙΙ)/2004)

Η ενέργεια αυτή ποινικοποιείται με σκοπό την προστασία της ανάγκης των οργανισμών και των ιδιωτών να ελέγχουν τα συστήματά τους από παρεμβάσεις οι οποίες θα δώσουν πρόσβαση σε εμπιστευτικές πληροφορίες.

Παράνομη Παρέμβαση (άρθρο 5 Ν.22(ΙΙΙ)/2004)

Στόχος είναι η προστασία του δικαιώματος της ιδιωτικότητας από την απόκτηση των δεδομένων, ή παρακολούθηση των επικοινωνιών ενός οργανισμού ή ενός ιδιώτη, είτε έμμεσα με χρήση ηλεκτρονικών συσκευών, είτε άμεσα με πρόσβαση και χρήση ηλεκτρονικού συστήματος αν η φύση της επικοινωνίας δεν είναι δημόσια.

Επέμβαση σε Δεδομένα (άρθρο 6 Ν.22(ΙΙΙ)/2004)

Στοχεύει στην προστασία της ακεραιότητας και της σωστής λειτουργίας ή χρήσης των αποθηκευμένων δεδομένων από οποιαδήποτε πράξη που τα μεταβάλλει αρνητικά, ή καταστρέφει, ή μεταλλάσει, ή τερματίζει, ή εμποδίζει τη διαθεσιμότητα τους στο άτομο που έχει νόμιμη πρόσβαση σε αυτά.

Επέμβαση σε Ηλεκτρονικό Υπολογιστή (άρθρο 7 Ν.22(ΙΙΙ)/2004)

Στόχος είναι η αποτροπή παρεμπόδισης λειτουργίας ενός συστήματος από τον ιδιοκτήτη του, ανεξαρτήτως μέσου που θα χρησιμοποιηθεί. Δεν περιλαμβάνεται όμως η ανεπιθύμητη λήψη ηλεκτρονικού ταχυδρομείου για σκοπούς διαφήμισης εκτός και αν είναι ηθελημένη και προκαλεί αποδεδειγμένα σοβαρή παρενόχληση.

Κατάχρηση Επινοήσεων (άρθρο 8 Ν.22(ΙΙΙ)/2004)

Αφορά στην προστασία από τη διάθεση συσκευών συμπεριλαμβανομένων και κακόβουλου λογισμικού, ή δεδομένων που θα μπορούσαν να επιτρέψουν την πρόσβαση σε ολόκληρο ή μέρος πληροφοριακού συστήματος που θα μπορούσε να προκαλέσει κάποιο από τα προαναφερθέντα 4 αδικήματα.

5.1.2. Αδικήματα Σχετιζόμενα με Υπολογιστές

Πρόκειται για εγκλήματα που συχνά διαπράττονται με τη χρήση ηλεκτρονικού υπολογιστή και όχι για εγκλήματα που διαπράττονται στον κυβερνοχώρο.

Πλαστογραφία Σχετιζόμενη με Ηλεκτρονικό Υπολογιστή (άρθρο 9 Ν.22(ΙΙΙ)/2004)

Σκοπός είναι η συμπλήρωση του κενού στο ποινικό δίκαιο αναφορικά με την παραδοσιακή έννοια της πλαστογραφίας, η οποία απαιτεί την οπτική αναγνωσιμότητα των δηλώσεων που βρίσκονται σε ένα έγγραφο, καθώς δεν εφαρμόζεται σε ηλεκτρονικά αποθηκευμένα δεδομένα.

Απάτη Σχετιζόμενη με Ηλεκτρονικό Υπολογιστή (άρθρο 10 Ν.22(ΙΙΙ)/2004)

Αποσκοπεί στην αποτροπή οποιασδήποτε ανάρμοστης διαχείρισης κατά την επεξεργασία δεδομένων με σκοπό την παράνομη μεταβίβαση περιουσίας.

5.1.3. Αδικήματα Σχετιζόμενα με το περιεχόμενο (άρθρο 11 Ν.22(ΙΙΙ)/2004)

Είναι η κατηγορία η οποία απασχολεί περισσότερο τις αστυνομικές αρχές ως προς το κυβερνοέγκλημα λόγω της ιδιαίτερης φύσης της. Αποσκοπεί στην ποινικοποίηση της παιδικής πορνογραφίας και συμπεριλαμβάνει την πρόκληση άλλων στην απόκτησή της, την προσφορά της στο Διαδίκτυο για χρήση από άλλους, τη διανομή του υλικού, την εξασφάλιση της από το Διαδίκτυο ή άλλο πληροφοριακό σύστημα και τέλος την κατοχή της σε οποιοδήποτε μέσο αποθήκευσης ηλεκτρονικών δεδομένων.

Στόχος αυτού του κεφαλαίου του νόμου είναι να προστατεύσει τα παιδιά που λαμβάνουν μέρος στη σεξουαλική κακοποίηση.

Το Ανώτατο Δικαστήριο έχει υιοθετήσει αγγλική νομολογία στην ποινική Υπόθεση μεταξύ της Δημοκρατίας v. AramMakamian την 19/07/2007 και από την αγγλική απόφαση R. v. Oliver [2003] 2 Cr.App.R. (S) 15 αντλούνται τα παρακάτω που δημιουργούν σημαντικές υποχρεώσεις για έναν ερευνητή ψηφιακής δικανικής :

Είναι χρήσιμο για το δικαστήριο να βλέπει το ίδιο το παιδικό πορνογραφικό υλικό.

Καθοριστικός παράγοντας σοβαρότητας της κάθε υπόθεσης είναι η φύση της παιδικής πορνογραφίας και το μέγεθος συμμετοχής του κατηγορουμένου στην αρχική εκμετάλλευση.

Βάσει του περιεχομένου δημιουργούνται 5 διαφορετικά επίπεδα παιδικής πορνογραφίας :

Επίπεδο 1 : Παραστάσεις με ερωτικές επιδείξεις παιδιών χωρίς σεξουαλική ενέργεια.

Επίπεδο 2 : Σεξουαλική ενέργεια μεταξύ ανηλίκων παιδιών ή αυτοϊκανοποίηση παιδιού

Επίπεδο 3 : Σεξουαλική ενέργεια χωρίς συνουσία μεταξύ ανηλίκων και ενηλίκων

Επίπεδο 4 : Σεξουαλική πράξη που περιλαμβάνει συνουσία μεταξύ ανηλίκων και ενηλίκων

Επίπεδο 5 : Σαδομαζοχισμός και κτηνοβασία.

Είναι εμφανές ότι ο αναλυτής πλέον δεν αρκείται στο να εντοπίσει το υλικό παιδικής πορνογραφίας αλλά καλείται και να το διαχωρίσει για να το κατατάξει αναλόγως επιπέδου το

οποίο θα καθορίσει και τη σοβαρότητα της υπόθεσης. Εδώ είναι και ένα ηθικό δίλλημα για τον ανακριτή κατά πόσο θα παραμείνει αντικειμενικός και εχέμυθος ή όχι. Η αγγλική απόφαση R. v. Thompson [2004] 2 Cr.App.R.262 παρέχει καθοδήγηση για το πως θα πρέπει να συντάσσεται το κατηγορητήριο, η σύνταξη του οποίου εξαρτάται άμεσα από τα ψηφιακά πειστήρια που θα εντοπιστούν κατά τη διάρκεια της έρευνας. Σκοπός της εισήγησης αυτής είναι η υποβοήθηση του δικαστηρίου για την επιβολή της ποινής και περιλαμβάνει την πλήρη αριθμητική καταγραφή του υλικού που ανευρέθηκε αναλόγως επιπέδου, να αναφέρεται στο δικαστήριο κατά πόσο οι φωτογραφίες αυτές είναι πραγματικές ή ρεαλιστικές και όπου είναι δυνατόν να καταγράφεται καθ' υπολογισμό η ηλικία των παιδιών που έλαβαν μέρος.

5.1.4. Αδικήματα σχετιζόμενα με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων. (άρθρο 12 Ν.22(ΙΙΙ)/2004)

Από τα πιο συχνά αδικήματα στο διαδίκτυο. Στόχος είναι η προστασία των πνευματικών δικαιωμάτων και η πάταξη της πειρατείας είτε αφορά διανομή μέσω πληροφοριακού συστήματος μουσικής, ταινιών, λογισμικού, ή άλλης παρόμοιας φύσεως υλικού. Βασίζεται στον Περί Πνευματικής Ιδιοκτησίας και Συγγενικών Δικαιωμάτων Νόμο του 1976

5.1.5. Επικουρική Ευθύνη (άρθρο 13 Ν.22(ΙΙΙ)/20040

Ποινικοποιείται η απόπειρα και η συνέργεια τέλεσης οποιουδήποτε από τα παραπάνω αδικήματα.

5.1.6. Ποινική Ευθύνη Νομικών Προσώπων (άρθρο 14 Ν.22(ΙΙΙ)/2004)

Εδώ το άρθρο 12 της Σύμβασης αναφέρει ότι είναι αναγκαίο να διασφαλισθεί η δυνατότητα ένα νομικό πρόσωπο να θεωρηθεί ένοχογια ποινικό αδίκημα, που καθορίστηκε με βάση τη Σύμβαση αυτή, το οποίο διαπράχθηκε προς όφελός του από οποιοδήποτε φυσικό πρόσωπο που ενεργεί, είτε ατομικά, είτε ως μέρος οργάνου του νομικού προσώπου, το οποίο να κατέχει εξέχουσα θέση στο νομικό πρόσωπο. Η μεταφορά αυτού του άρθρου στην Κυπριακή νομοθεσία εκτιμάται ότι είναι λανθασμένη καθώς δεν αποδίδει τον ουσιαστικό σκοπό του άρθρου 12 της Σύμβασης και ποινικοποιεί μόνο τη συμπεριφορά των φυσικών προσώπων που δρουν προς το συμφέρον μιας εταιρείας και όχι τη συμπεριφορά αυτής της εταιρείας, ή την έλλειψη επιτήρησης ή ελέγχου σε φυσικά πρόσωπα αυτής.

5.2. Δικονομικό Δίκαιο

Στο άρθρο 15 Ν.22(ΙΙΙ)/2004 αναφέρεται πως η εφαρμογή των πιο πάνω δικονομικών διαδικασιών είναι βάση του Μέρους ΙΙ Περί Ποινικής Δικονομίας Νόμου της Κύπρου.

5.2.1. Κεφ. 155 Ποινικής Δικονομίας

Σε αυτό το κεφάλαιο αναφέρονται οι εξουσίες που έχουν οι αστυνομικοί όταν διεξάγουν έρευνα για ποινικά αδικήματα οι οποίες εφαρμόζονται ανάλογα και στη ψηφιακή δικανική και είναι οι εξής :

Γραπτή αστυνομική διαταγή για την παρουσίαση κάποιου αναγκαίου για την ανάκριση εγγράφου σε εύλογο τόπο και χρόνο.

Έκδοση δικαστικού εντάλματος έρευνας. Όταν ο δικαστής ικανοποιείται με ένορκη καταγγελία ότι υπάρχει εύλογη αιτία να πιστεύεται ότι σε οποιοδήποτε τόπο υπάρχει οτιδήποτε στο οποίο ή σε σχέση με το οποίο διαπράχτηκε ποινικό αδίκημα, ή να πιστεύεται ότι θα παρέχει απόδειξη ως προς τη διάπραξη ποινικού αδικήματος ή να πιστεύεται ότι προορίζεται για την ύπαρξη ποινικού αδικήματος.

Οτιδήποτε κατασχεθεί κατόπιν εντάλματος δύναται να κατακρατηθεί μέχρι την ολοκλήρωση της ποινικής διαδικασίας. Στην περίπτωση που κατά την έρευνα κάποιου τόπου βρεθεί υλικό το οποίο δεν αναγράφεται πάνω στο ένταλμα αλλά υπάρχει εύλογη υποψία ότι θα βοηθήσει την εξέταση, ο εξουσιοδοτημένος μπορεί να το κατάσχει και να το παρουσιάσει ενώπιον του δικαστή που εξέδωσε το ένταλμα, ο οποίος μπορεί να εκδώσει διάταγμα σχετικά με την κατάσχεση ή διάθεση του υλικού.

Πρακτικά η Αστυνομία κατά την εκτέλεση ενός εντάλματος για έρευνα θεωρεί έναν ηλεκτρονικό υπολογιστή ως ένα ασφαλισμένο αρχείο εγγράφων για την ασφάλεια του οποίου είναι υπεύθυνος ο ιδιοκτήτης. Κατά την έρευνα το ένταλμα δίνει την εξουσία στους αστυνομικούς να αποκτήσουν πρόσβαση σε οποιοδήποτε γραφείο ή συρτάρι για την ανακάλυψη τυχόν τεκμηρίων για μια υπόθεση. Εξαιτίας αυτού θεωρείται πως μπορεί να αποκτηθεί πρόσβαση σε οποιοδήποτε μέσο αποθήκευσης δεδομένων ενός υπόπτου.

5.3. Δικονομικά – Ανακριτικά μέτρα που επιτρέπουν την επιτυχή δίωξη των διαδικτυακών εγκλημάτιών που προβλέπονται στο μέρος 2 του κεφαλαίου 2 της Σύμβασης του 2001

5.3.1. Έγκαιρη διαφύλαξη δεδομένων υπολογιστή που έχουν αποθηκευτεί (άρθρο 16)

Με το μέτρο αυτό η αστυνομία μπορεί να επιτύχει την έγκαιρη διαφύλαξη δεδομένων που είναι συγκεντρωμένα σε έναν υπολογιστή συμπεριλαμβανομένων και των διακινούμενων. Επίσης μπορούν να ληφθούν μέτρα για την υποχρέωση κάποιου προσώπου να διαφυλάξει και να διατηρήσει την ακεραιότητά τους για χρονική περίοδο που κρίνεται αναγκαία αλλά δεν υπερβαίνει τις 90 ημέρες.

5.3.2. Έγκαιρη διαφύλαξη και μερική αποκάλυψη διακινούμενων δεδομένων. (άρθρο 17)

Με αυτό το άρθρο διασφαλίζεται ότι οι αρχές θα μπορούν να εξασφαλίσουν και να διαφυλάξουν διακινούμενα δεδομένα ενός υπόπτου ανεξάρτητα από τον αριθμό των εμπλεκόμενων παρόχων υπηρεσιών που εμπλέκονται στη διαβίβασή τους.

5.3.3. Ένταλμα υποβολής στοιχείων (άρθρο 18)

Η αστυνομία έχει το δικαίωμα να διατάξει έναν πάροχο που προσφέρει τις υπηρεσίες του στο έδαφος της Κυπριακής Δημοκρατίας, να προσκομίσει πληροφορίες που είναι στην κατοχή του, οποιασδήποτε μορφής που έχει σχέση με συνδρομητές των υπηρεσιών του με την οποία καθορίζεται ο τύπος της υπηρεσίας, οι τεχνικοί όροι, η ταυτότητα του συνδρομητή και οποιαδήποτε άλλη σχετική πληροφορία.

5.3.4. Πραγματικός χρόνος συλλογής διακινουμένων δεδομένων (άρθρο 20)

Αυτό το μέτρο επιτρέπει στην αστυνομία να συλλέγει και να καταγράφει με χρήση τεχνικών μέσων, ή να υποχρεώσει έναν πάροχο να εκτελεί τη συλλογή και καταγραφή, ουσιώδεις πληροφορίες σε πραγματικό χρόνο των καθοριζομένων επικοινωνιών στο έδαφος της Κυπριακής Δημοκρατίας μέσω υπολογιστή.

5.4. Προβλήματα – Δυσχέρειες

Η εφαρμογή της Σύμβασης του 2001 αντιμετωπίζει αρκετά προβλήματα και δυσχέρειες λόγω συγκρούσεων κάποιων άρθρων της σύμβασης με πρόνοιες του Συντάγματος της Κυπριακής Δημοκρατίας. Οι συγκρούσεις αυτές αφορούν κυρίως θέματα διασφάλισης προσωπικών δεδομένων καθώς στο Κυπριακό νομικό σύστημα τα ανθρώπινα δικαιώματα και οι ελευθερίες είναι καλά προστατευμένα από το Σύνταγμα.

Στο άρθρο 17 του Συντάγματος [24] προστατεύεται οποιαδήποτε μορφή επικοινωνίας απόλυτα, με μόνες εξαιρέσεις στις επικοινωνίες μεταξύ υποδίκων και καταδικασμένων προσώπων και στις επικοινωνίες προσώπου που χρεοκόπησε κατά τη διάρκεια της διοίκησης της περιουσίας του. Αυτό είναι ένα πολύ σοβαρό πρόβλημα για την Κυπριακή Αστυνομία γιατί δεν έχει το δικαίωμα να χρησιμοποιήσει τα τεκμήρια που θα βρει, για παράδειγμα, από την ηλεκτρονική αλληλογραφία ενός υπόπτου για να τα παρουσιάσει στο δικαστήριο και να γίνουν αποδεκτά.

Επίσης τα προβλεπόμενα στη Σύμβαση άρθρα (16,17,18,20) δεν έχουν ενσωματωθεί στην Κυπριακή Νομοθεσία μέχρι τη στιγμή που αναγράφεται αυτή η εργασία λόγω του ότι έχουν κριθεί αντισυνταγματικά, κατά παράβαση των προνοιών του άρθρου 17 του Συντάγματος. Από την άλλη, με την Πέμπτη Τροποποίηση του Συντάγματος Ν.127(Ι)/2006 (28/07/2006), προστέθηκε το άρθρο $1^{Α}$, όπου σύμφωνα με αυτό, οποιοσδήποτε νόμος θεσπίζεται για σκοπούς εναρμόνισης της Κυπριακής Δημοκρατίας με το Κοινοτικό κεκτημένο υπερισχύει οποιασδήποτε συνταγματικής διάταξης και οποιοδήποτε μέτρο λαμβάνεται από την Κυπριακή Δημοκρατία ως επιβαλλόμενη ή απορρέουσα υποχρέωση της, ως κράτος μέλος της Ευρωπαϊκής Ένωσης, δε μπορεί να ακυρωθεί από οποιαδήποτε διάταξη του Συντάγματος.

Ως εκ τούτου σε περίπτωση που ένα κράτος μέλος της ΕΕ ζητήσει από την ΚΔ την παρακολούθηση των επικοινωνιών ενός προσώπου που βρίσκεται στην Κυπριακή Δημοκρατία, η Κυπριακή Αστυνομία με βάση το άρθρο $1^{Α}$ του Συντάγματος υποχρεώνεται να το κάνει, ενώ αν

η Κυπριακή Αστυνομία ερευνά έναν ύποπτο στην Κύπρο, δε μπορεί να παρακολουθήσει τις επικοινωνίες του αφού δεν εφαρμόζεται το άρθρο 1[Α] του Συντάγματος.

Κεφάλαιο 6
Εργαλεία Ψηφιακής Δικανικής

Σε αυτό το κεφάλαιο θα παρουσιαστούν κάποια από τα επικρατέστερα εμπορικά εργαλεία που χρησιμοποιούνται κυρίως από οργανισμούς επιβολής του νόμου και από εδικά τμήματα του στρατού. Επίσης θα γίνει σύντομη αναφορά σε εργαλεία ανοικτού κώδικα τα οποία διατίθενται δωρεάν με το μειονέκτημα ότι δεν μπορούν να εκτελέσουν μια πλήρη δικανική ανάλυση ακλουθώντας το μοντέλο που ακολουθούν τα εμπορικά.

Τα περισσότερα εμπορικά εργαλεία εφαρμόζουν το ίδιο μοντέλο για συλλογή και παρουσίαση των ψηφιακών πειστηρίων που είναι το παρακάτω :

1. Όλα τα δεδομένα αναλύονται και παρουσιάζονται σε μια διεπαφή χρήστη.

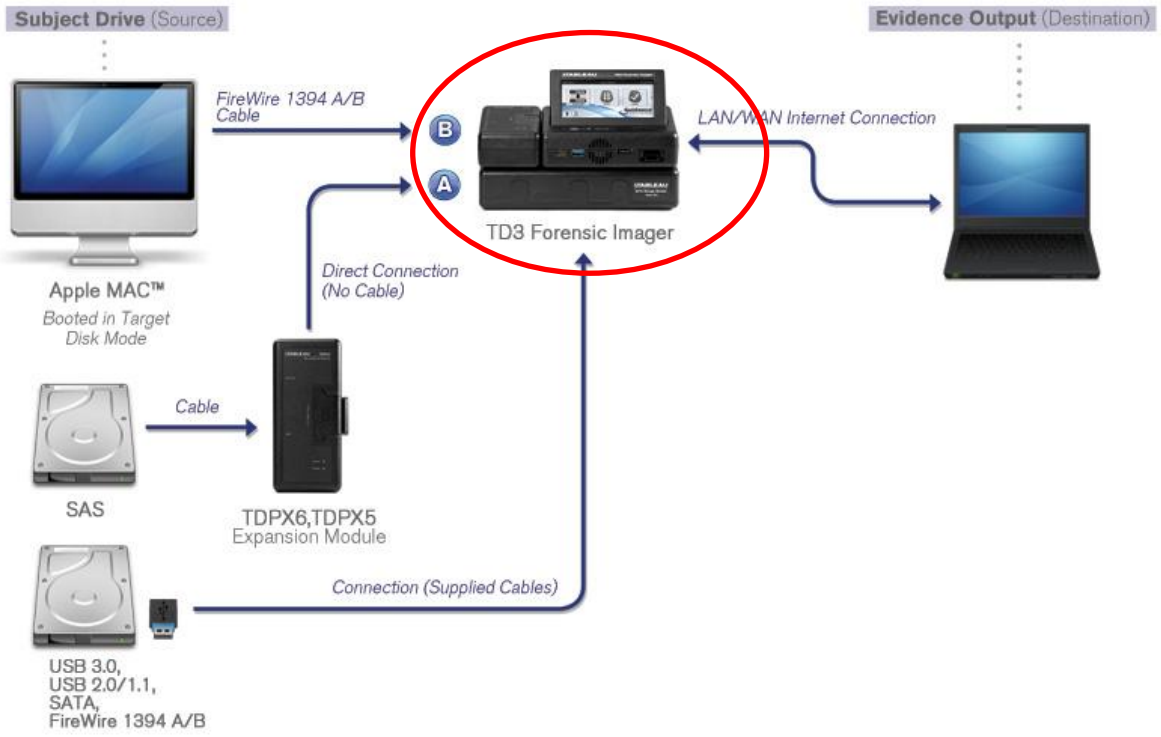
2. Η παρουσίαση όλων των δεδομένων γίνεται μέσω ενός πίνακα όπου μπορεί ο χρήστης να ερευνήσει αυτόνομα στοιχεία.

3. Ο ερευνητής μπορεί να εφαρμόσει φίλτρα και λέξεις κλειδιά για εντοπισμό εγγράφων ή άλλων στοιχείων.

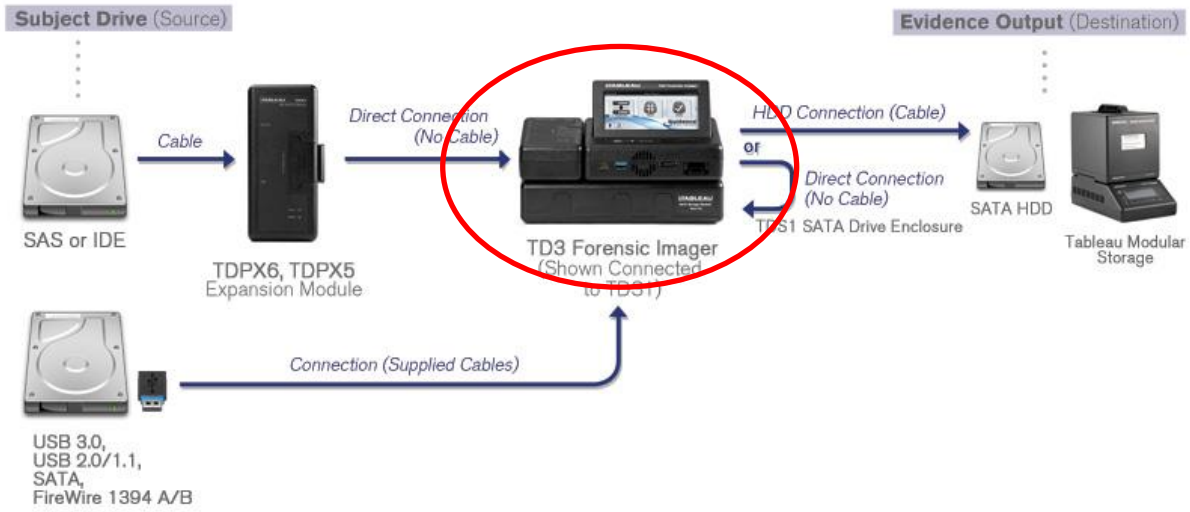
4. Τέλος παρουσιάζεται μια αναφορά για το τι βρέθηκε και με τι τρόπο έχει βρεθεί. Στα περισσότερα εργαλεία η αναφορά είναι μια αυτοματοποιημένη διαδικασία.

6.1 Συσκευές Προστασίας Εγγραφών

Για να διασφαλιστεί η αυθεντικότητα των στοιχείων που έχουν ληφθεί από τον ερευνητή, επιπλέον της απαγόρευσης εγγραφών μέσω του ίδιου του λογισμικού υπάρχουν συσκευέςοι οποία εξασφαλίζουν ότι κατά τη λήψη της εικόνας δεν θα γίνει οποιαδήποτε αλλοίωση των δεδομένων που θα εξεταστούν. Είναι συσκευές (writeblockers) οι οποίες παρεμβάλλονται μεταξύ του υπολογιστή του ερευνητή και των αποθηκευτικών μέσων ή υπολογιστών που θα ερευνήσει. Έχουν τη δυνατότητα σύνδεσης όλων των τύπων συσκευών αποθήκευσης δεδομένων πλην των ειδικά κατασκευασμένων, για στρατιωτικούς κυρίως σκοπούς, που για λόγους ασφαλείας έχουν τις περισσότερες φορές μοναδικές ανά κατασκευαστή διεπαφές. Οι συσκευές δεν είναι απαραίτητες για να ληφθεί το αντίγραφο του δίσκου χωρίς αλλοίωση, καθότι στις περισσότερες των περιπτώσεων το ίδιο το λογισμικό το εξασφαλίζει αυτό, αλλά προσδίδουν επιπλέον αξιοπιστία στην έρευνα κατά την παρουσίασή της στο δικαστήριο και ελαχιστοποιεί τις πιθανότητες λάθους.



Εικόνα 6.1 : Σύνδεση συσκευής writeblocker για λήψη ακριβούς αντίγραφου μέσω τοπικού δικτύου.



Εικόνα 6.2:Σύνδεση συσκευής writeblocker για λήψη ακριβούς αντίγραφου απευθείας με το μέσο προς αντιγραφή.

6.2. Το εργαλείο EnCaseEnterprise

Το εργαλείο EnCaseEnterprise είναι προϊόν της εταιρείας GuidanceSoftware και μπορεί να θεωρηθεί ως μια πλήρης εργαλειοθήκη για την Ψηφιακή Δικανική [30]. Είναι πολύ διαδεδομένο στους κόλπους κυβερνητικών οργανισμών της ΕΕ και είναι ένα από τα κύρια εργαλεία που χρησιμοποιεί η Europol στην προσπάθειά της για την καταπολέμηση του ηλεκτρονικού εγκλήματος.

Με τον όρο πλήρης εργαλειοθήκη εννοούμε ότι παρέχεται από την εταιρεία λογισμικό καθώς και υλιστικό το οποίο έχει τη δυνατότητα να ολοκληρώσει την εξέταση και ανάλυση μιας υπόθεσης από την αρχή μέχρι και την παρουσίαση των στοιχείων στο δικαστήριο, χωρίς να είναι απαραίτητη η χρήση οτιδήποτε άλλου επιπλέον από το EnCase. Επίσης η εταιρεία πέραν από το εργαλείο προσφέρει και εκπαίδευση στο προσωπικό που θα το χρησιμοποιήσει, παρέχοντας πιστοποίηση ορθής γνώσης και χρήσης, η οποία είναι απαραίτητη για την αναγνώριση του αναλυτή από το δικαστήριο.

Πρακτικά το εν λόγω εργαλείο παρέχει όλα όσα θα μπορούσε να προσφέρει συνδυασμός πολλών εργαλείων ανοικτού κώδικα, συγκεντρωτικά, με πολύ αναλυτικό και καλά ταξινομημένο οδηγό χρήσης, υποστήριξη, και εκπαίδευση με την απαραίτητη πιστοποίηση. Η εκπαίδευση περιλαμβάνει τμήματα σε τάξη, αλλά και διαδικτυακά. Εκτός αυτών παρέχονται και αντικείμενα σε διαδικτυακά σεμινάρια. Όλα τα μαθήματα ταξινομούνται αναλόγως του επιπέδου γνώσεων του εκπαιδευομένου για καλύτερη και αποτελεσματικότερη κατανόηση.

Πιο αναλυτικά το EnCaseEnterprise V7 έχει πάρα πολλές δυνατότητες οι οποίες του επιτρέπουν να ξεχωρίζει από τα υπόλοιπα και να δικαιολογεί το υψηλό μερίδιό του στη συγκεκριμένη αγορά, η οποία εξ αιτίας της ραγδαίας αύξησης του ηλεκτρονικού εγκλήματος παρουσιάζει μεγάλη άνοδο [42]. Τα κύρια χαρακτηριστικά του αναφέρονται συνοπτικά παρακάτω.

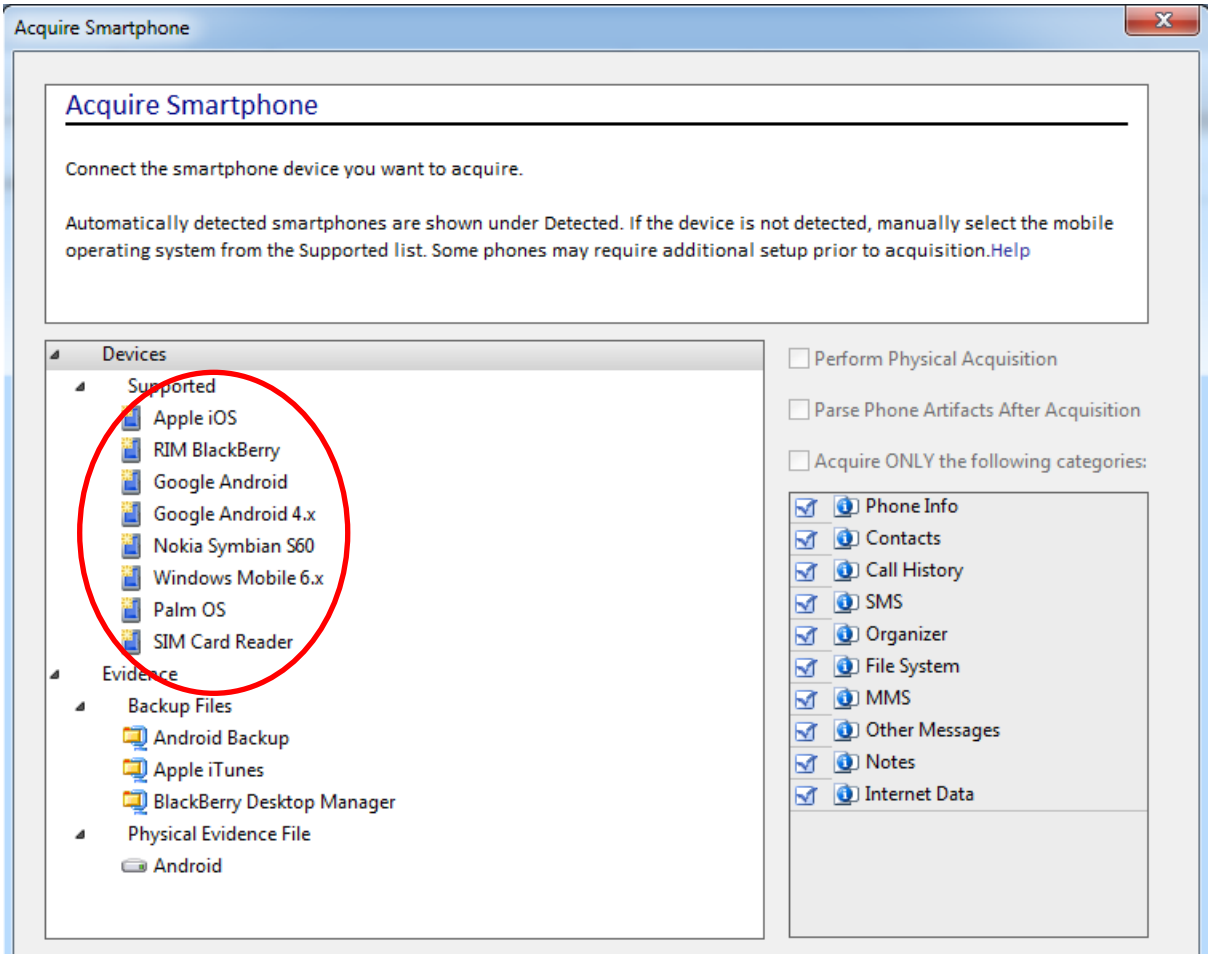
Δυνατότητα λήψης στοιχείων, όπως ακριβές αντίγραφο δίσκων, ή πτητικής μνήμης όχι μόνο με απευθείας σύνδεση με το μέσο, αλλά και απομακρυσμένα εντός του ιδίου τοπικού δικτύου (στο Enterpriserelease μόνο), η οποία επιτρέπει στον ερευνητή να εξετάσει στοιχεία αυτά άμεσα και διακριτικά [43]. Η συλλογή γίνεται με το EnCaseImager,το οποίο διατίθεται δωρεάν από την εταιρεία και εξετάστηκε πρακτικά, το οποίο όμως κατά τη διάρκεια της συλλογής των δεδομένων για τη δημιουργία του ακριβούς αντίγραφου, η οποία έγινε για σκοπούς εξέτασης του εν λόγω τμήματος του εργαλείου, δεν ενημερώνει τον ερευνητή σε ποιο στάδιο βρίσκεται η

διαδικασία με πιθανή συνέπεια την εκ παραδρομής διακοπή της διαδικασίας πριν την ολοκλήρωσή της, ή τη μη αξιοποίηση του πολύτιμου, για τον ερευνητή, χρόνου.

Επίσης σε περίπτωση που ο ύποπτος ηλεκτρονικός υπολογιστής είναι απενεργοποιημένος το εργαλείο διαθέτει live cd το οποίο χρησιμοποιείται για την ανάκτηση του ακριβούς αντίγραφου του δίσκου σε περίπτωση που δεν μπορεί να εφαρμοστεί άλλη μέθοδος, όπως η αφαίρεση του δίσκου.

Κατανομή εργασιών μεταξύ των πυρήνων καθώς και την ανάθεση προτεραιοτήτων εκτέλεσης της κάθε εργασίας.

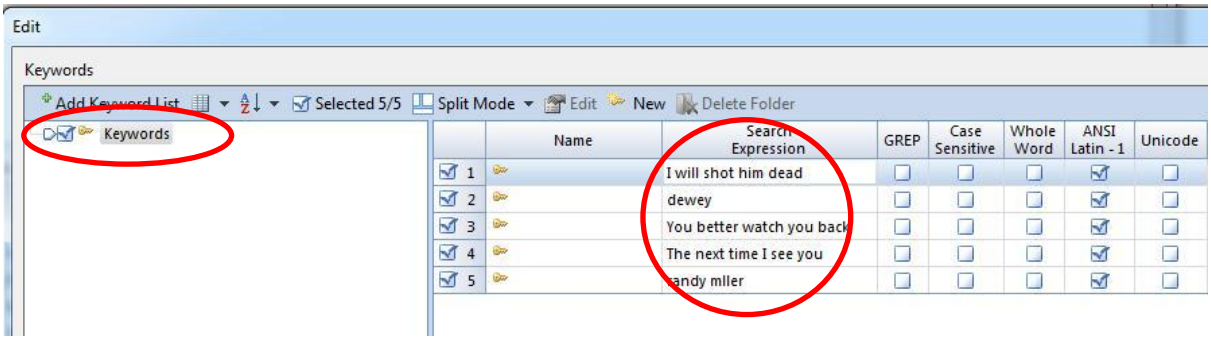
Εξέταση και ανάλυση συσκευών android ή iOS όπως κινητά τηλέφωνα ή ταμπλέτες. Περιλαμβάνονται και αρκετές εμπορικές εκδόσεις του android όπως το kindlefire καθώς επίσης και συσκευές blackberry. Πιο απλά φαίνεται ότι έχει την ικανότητα να εξετάζει οποιαδήποτε συσκευή έχει λειτουργικό σύστημα.



Εικόνα 6.3 :Κινητές συσκευές τις οποίες το εργαλείο EnCase μπορεί να εξετάσει

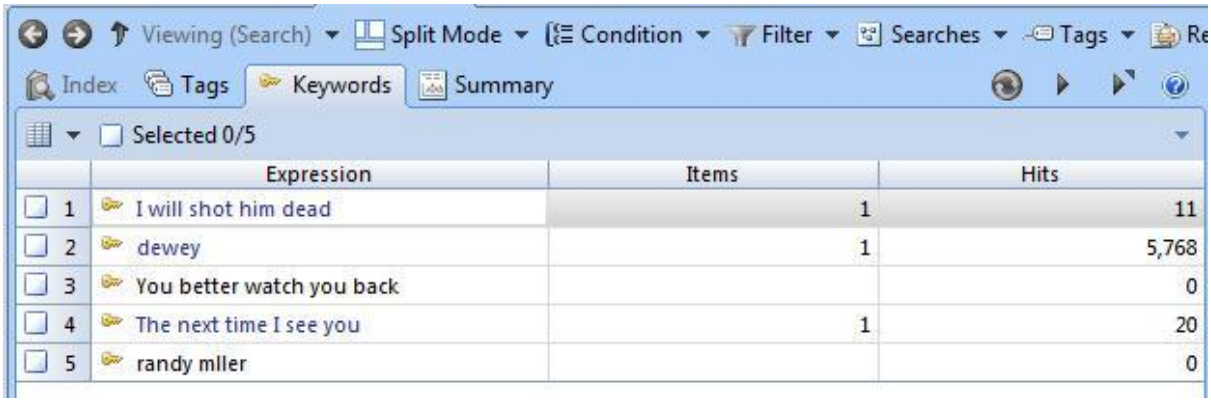
Δίνει τη δυνατότητα στους ερευνητές να μοιραστούν τα στοιχεία που έχουν με συνεργάτες, όπως άλλους ερευνητές, δικηγόρους ή άλλους ενδιαφερόμενους που δεν έχουν το εν λόγω εργαλείο, τα οποία όμως δεν μπορούν να επεξεργαστούν, αλλά μπορούν να προσθέσουν καθοδηγητικές περιγραφές οι οποίες να εισαχθούν στο EnCase.

Παρέχεται εξελιγμένη μέθοδος αναζήτησης η οποία περιλαμβάνει την αναζήτηση εντός ευρετηρίου, με τη χρήση ταμπέλας και με τη χρήση λέξης ή και φράσης κλειδί, όχι μόνο στα ονόματα των αρχείων αλλά και μέσα στο κείμενο τους σε όλες τις γνωστές μορφοποιήσεις. Η αναζήτηση αυτή μπορεί να γίνει ακόμα και στην πτητική μνήμη (RAM).



Εικόνα 6.4 : Αναζήτηση με λέξεις κλειδιά ή εκφράσεις

Που όπως φαίνεται στην πιο κάτω εικόνα επιστρέφει πολλά αποτελέσματα.

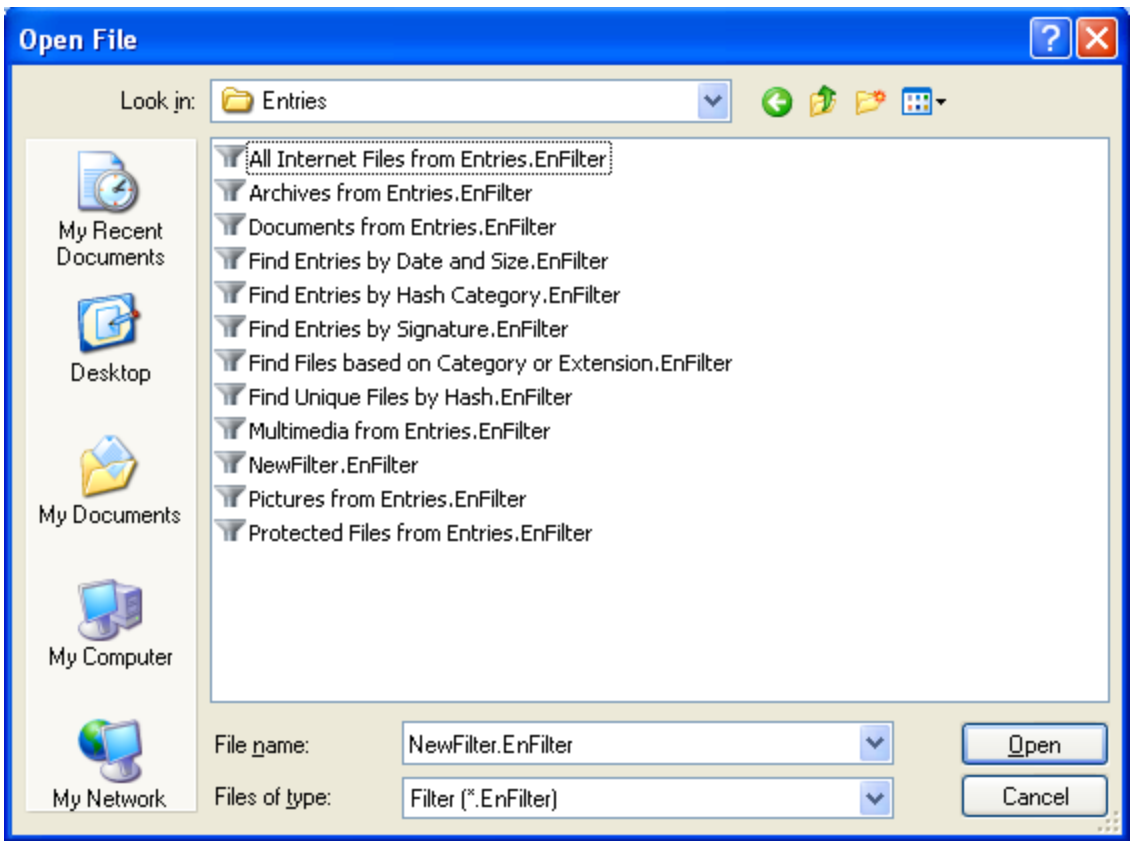


Εικόνα 6.5 : Παρουσίαση αποτελεσμάτων αναζήτησης.

Τα οποία μπορούν από μόνα τους να δώσουν ικανοποιητικά στοιχεία για τη στήριξη μιας υπόθεσης.

Εικόνα 6.6 : Μήνυμα που έστειλε ο ύποπτος μέσω facebook στο θύμα

Ο ερευνητής μπορεί να συνδυάσει τα φίλτρα, πάνω από 150 διαθέσιμα, και τις λέξεις-κλειδιά με τους λογικούς τελεστές για να δημιουργήσει μια σύνθετη αναζήτηση που θα του παράγει ακριβώς το αποτέλεσμα που επιθυμεί.



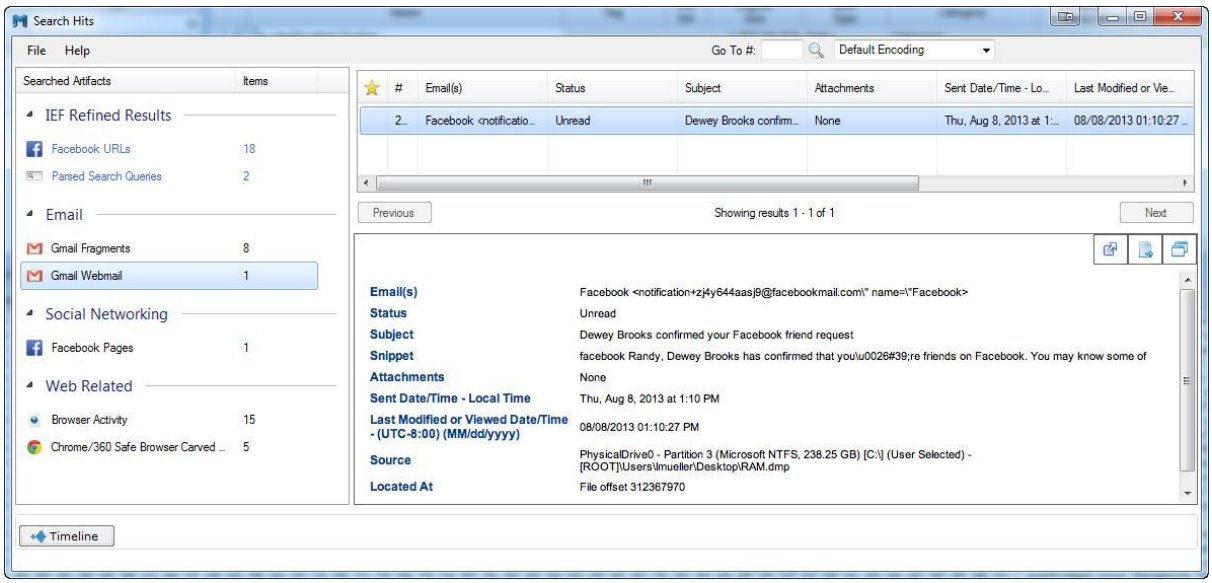
Εικόνα 6.7 : Είδη φίλτρων που παρέχει το EnCase

Πέραν αυτών υπάρχει και το EnScript το οποίο είναι μια αντικειμενοστραφής γλώσσα παρόμοια με τη C++ με την οποία ο ερευνητής μπορεί να δημιουργήσει δικά του σενάρια αναζήτησης πέραν των προϋπαρχόντων τα οποία καλύπτουν σχεδόν όλες τις πιθανές περιπτώσεις.

```
1  //EnCase V7 Code
2
3  class MyClass
4  {
5    DateClass Date;
6
7    MyClass(DateClass date = DateClass::Null) :
8      Date = date
9    {
10
11   }
12
13   String GetDate()
14   {
15     if (Date != DateClass::Null)
16     {
17       return String::Format("Date is {0}", Date.GetString());
18     }
19     else
20     {
21       return "<Invalid>";
22     }
23   }
24 }
25
26 class MainClass
27 {
28   void Main()
29   {
30     SystemClass::ClearConsole(1);
31     DateClass date;
32     date.Now();
33     MyClass mc(),
34             mc2(date);
35     Console.WriteLine(mc.GetDate());
36     Console.WriteLine(mc2.GetDate());
37   }
38 }
39
40
```

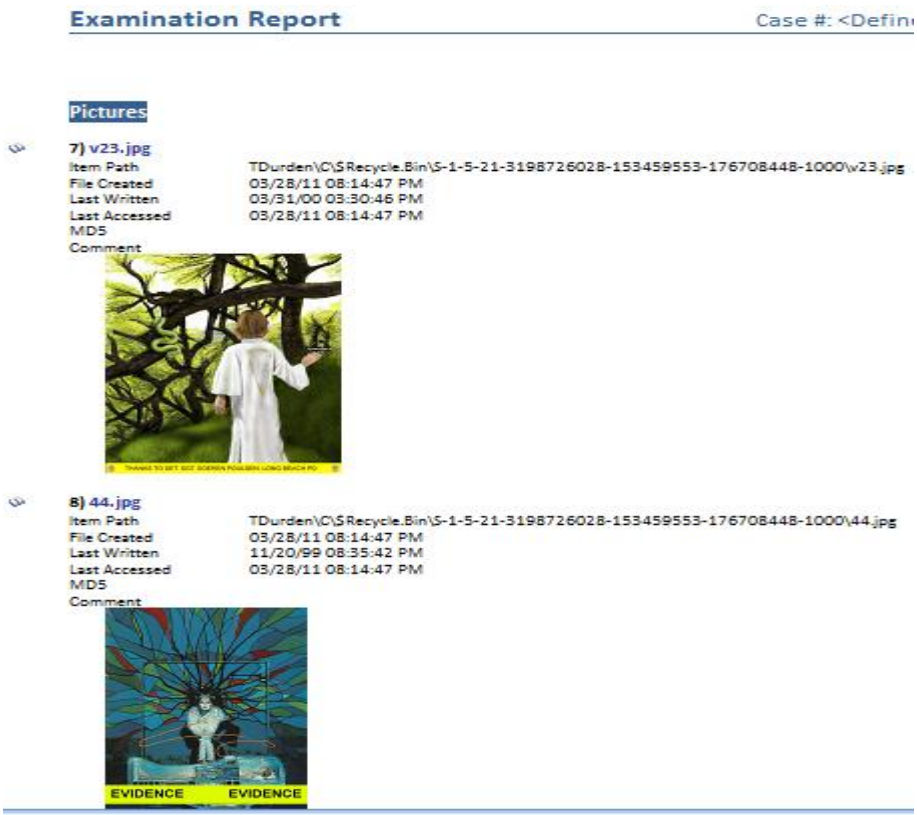
Εικόνα6.8 : Δείγμα τρόπου εγγραφής σεναρίου με το EnScript

Μεγάλη βοήθεια για τον ερευνητή είναι η δυνατότητα που του παρέχει για την αυτοματοποιημένη δημιουργία αναφορών οι οποίες με ένα μόνο κλικ παρέχουν όλη τη δραστηριότητα του υπόπτου, όπως το ιστορικό του φυλλομετρητή του, cookies, πληροφορίες logon κλπ κλπ.



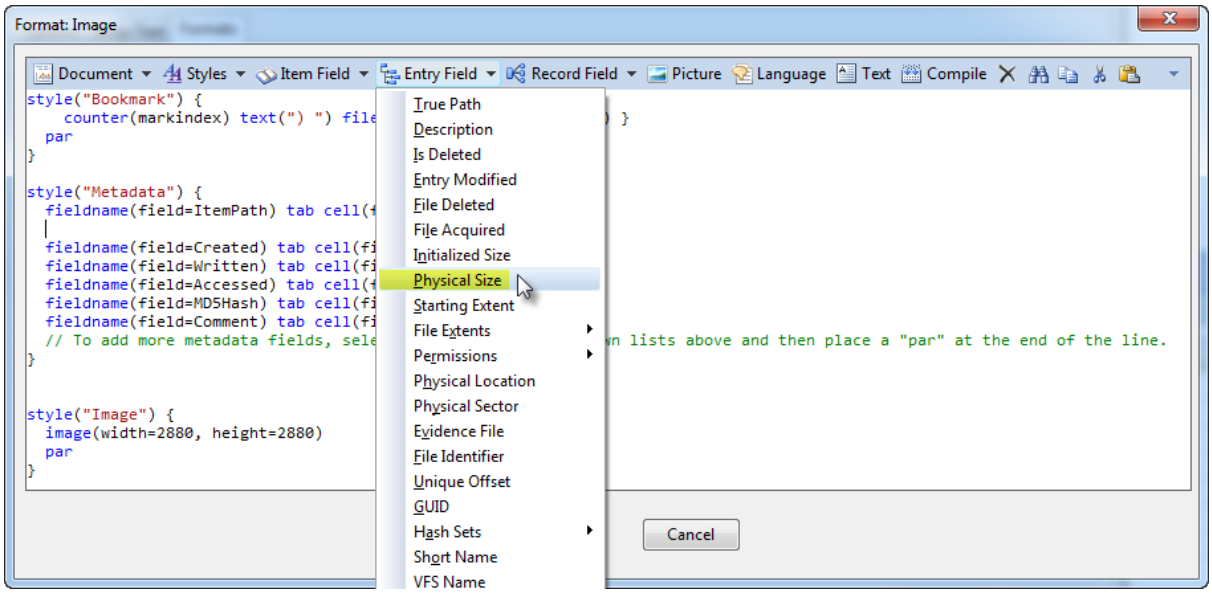
Εικόνα 6.9 : Αναζήτηση της Διαδικτυακής δραστηριότητας του υπόπτου

Για τη δημιουργία των αναφορών παρέχονται στον ερευνητή επιπρόσθετα πρότυπα τα οποία μπορεί να τα κατεβάσει από το κατάστημα εφαρμογών της εταιρείας χωρίς χρέωση και να τα χρησιμοποιήσει με ή χωρίς αλλαγές, αναλόγως της υπόθεσης που θα κληθεί να παρουσιάσει.



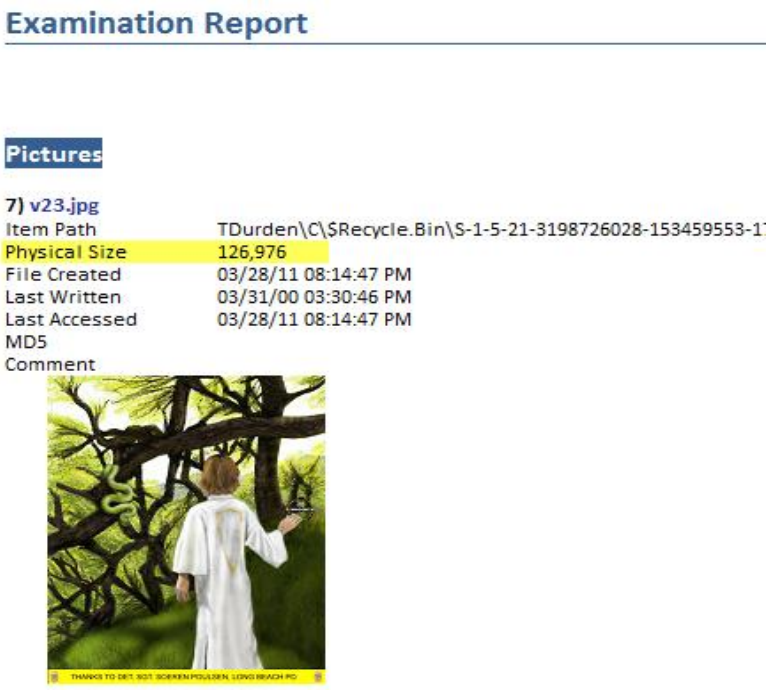
Εικόνα 6.10 :Τρόπος παρουσίασης εικόνων μαζί με τα μεταδεδομένα τους, μέσω της αυτόματης αναφοράς

Για παράδειγμα, το να προσθέσει κάποιος μεταδεδομένα σε κάποιο είδος αρχείου που θεωρεί απαραίτητα κατά την παρουσίασή του στο δικαστήριο δεν είναι απαραίτητο να ξέρει να χρησιμοποιεί κώδικα, το εργαλείο έχει φροντίσει να είναι μια απλή διαδικασία λίγων κλικ.



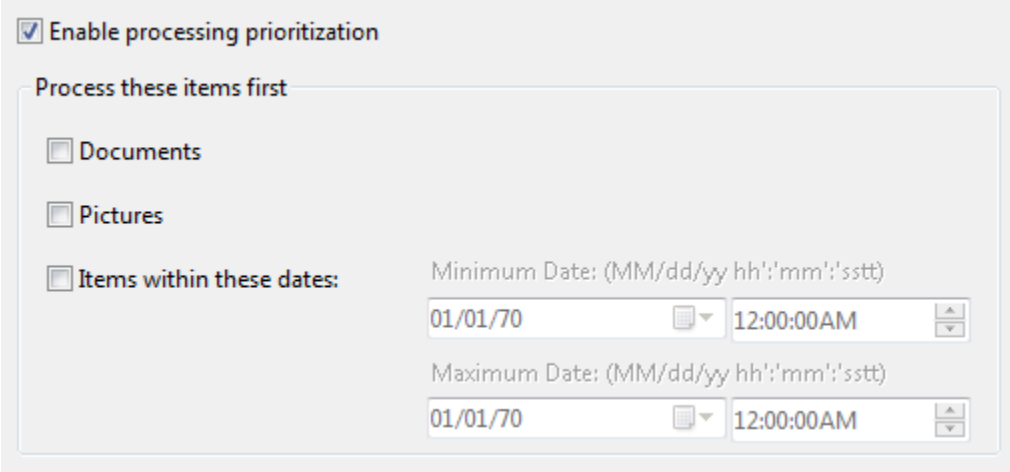
Εικόνα 6.11 : Προσθήκη μεταδεδομένων σε εικόνα χωρίς εγγραφή κώδικα μέσω του EnCase

Έτσι ώστε να μπορεί ο ερευνητής να παρουσιάσει όλα τα στοιχεία που θεωρεί υποστηρικτικά για το αρχείο στην αναφορά του στο λιγότερο δυνατό χρόνο.



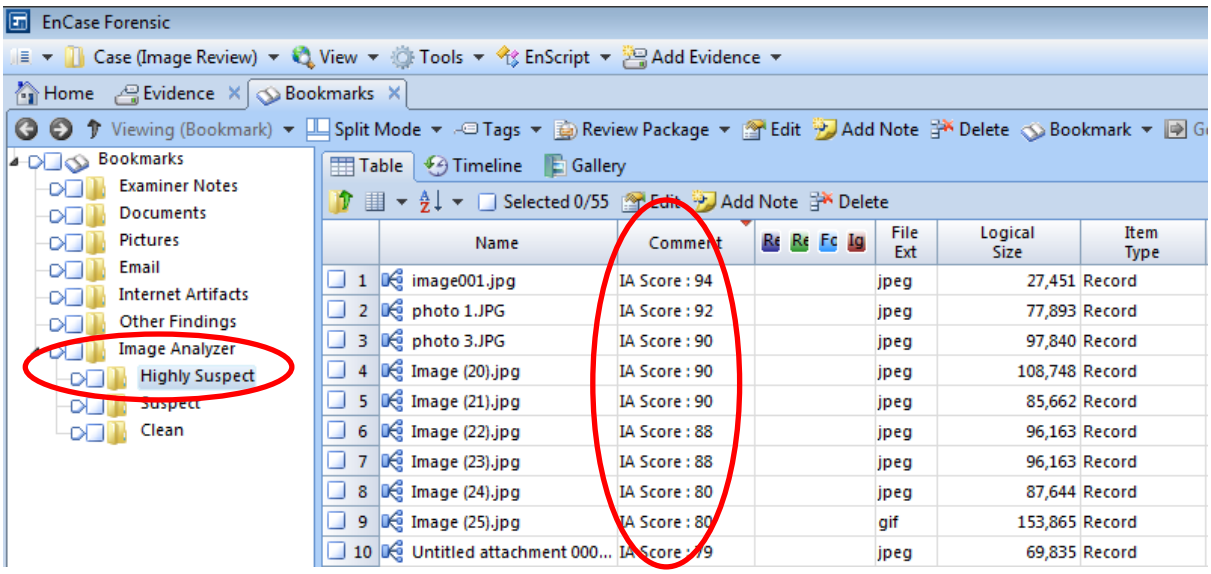
Εικόνα 6.12 :Επιτυχής προσθήκης επιπλέον στοιχείων σε αυτόματη αναφορά

Καθορισμός προτεραιοτήτων που αφορά στο ποια αρχεία θα τύχουν επεξεργασίας πρώτα και ποια αργότερα, με αυτή τη δυνατότητα αρχεία τα οποία ο ερευνητής πιστεύει ότι είναι κρίσιμα θα επεξεργαστούν πρώτα, χαρακτηριστικό το οποίο μεταφράζεται σε τεράστιο κέρδος χρόνου αν λάβουμε υπόψη το χρονοβόρο της διαδικασίας σε περιπτώσεις μεγάλου όγκου δεδομένων οι οποίες είναι πλέον οι πιο συνηθισμένες.



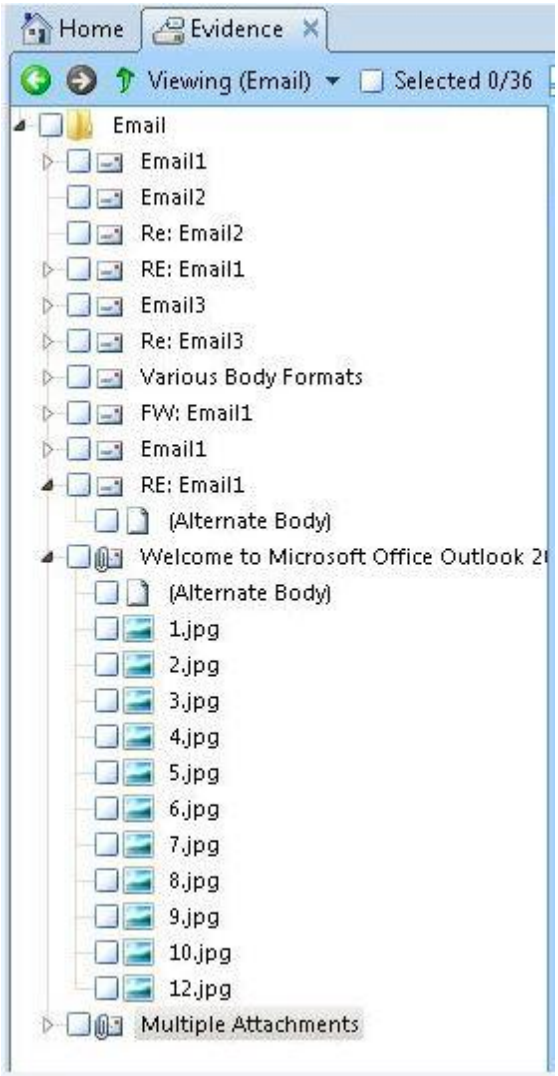
Εικόνα 6.13 : Καθορισμός προτεραιότητας επεξεργασίας από τον ερευνητή

Λαμβάνοντας υπόψη το γεγονός ότι ο όγκος δεδομένων που εξετάζεται πλέον για κάθε υπόθεση είναι πολύ μεγάλος και απαιτεί πολύ περισσότερο χρόνο σε σχέση με μια δεκαετία πριν, έχουν δημιουργηθεί και εργαλεία τα οποία μπορούν να μειώσουν την αναζήτηση στο ελάχιστο, όπως για παράδειγμα το ImageAnalyzer το οποίο μπορεί να εντοπίσει εικόνες με πορνογραφικό υλικό και να τις παρουσιάσει στον ερευνητή μειώνοντας κατά πολύ το χρόνο που θα απαιτούνταν για να τις εντοπίσει μόνος του. Τα εργαλεία αυτά σε καμία περίπτωση δεν αντικαθιστούν τον αναλυτή, απλά τον κάνουν πιο αποτελεσματικό.



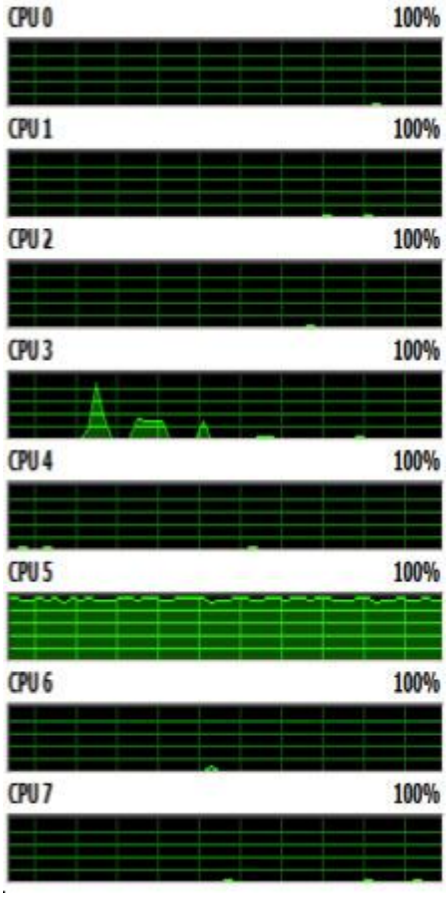
Εικόνα 6.14 : Χρήση πρόσθετου για εντοπισμό εικόνων ύποπτων για πορνογραφικό περιεχόμενο

Ένα από τα σημαντικότερα χαρακτηριστικά του εργαλείου είναι η δυνατότητα που παρέχει στον ερευνητή για την επισκόπηση της ηλεκτρονικής αλληλογραφίας του υπόπτου. Έχει τη δυνατότητα να αναπαράγει όχι μόνο την αλληλογραφία σε περιβάλλον που προσομοιάζει με αυτό των προγραμμάτων διαχείρισης ηλεκτρονικής αλληλογραφίας όπως αυτό του MS Outlook, αλλά μπορεί και να αναπαράγει επ' ακριβώς και το νήμα της επικοινωνίας με αποτέλεσμα μηνύματα που είτε δε θα είχαν κανένα νόημα από μόνα τους, είτε θα έπρεπε να θυσιαστεί πολύτιμος χρόνος για να συνδεθούν, να παρουσιάζονται στον ερευνητή συνδεδεμένα και να του παρέχουν πλήρη άποψη για τις ηλεκτρονικές συνομιλίες του υπόπτου.



Εικόνα 6.15 :Παρουσίαση ηλεκτρονική αλληλογραφίας με ολοκληρωμένο νήμα

Τέλος με την αύξηση των εργαλείων που παρέχουν στους απλούς χρήστες τη δυνατότητα κρυπτογράφησης είτε ολόκληρων δίσκων, είτε συγκεκριμένων φακέλων, παρέχεται μια περιορισμένη δυνατότητα αποκρυπτογράφησης με τη χρήση του EnCaseDecryptionSuite (EDS). Σε περίπτωση αποκρυπτογράφησης όμως χωρίς κανένα στοιχείο από τον ερευνητή, με τη μέθοδο εξαντλητικών δοκιμών δεν έχει να προσφέρει κάτι καλύτερο από οποιοδήποτε δωρεάν λογισμικό καθότι δεν εκμεταλλεύεται τον επεξεργαστή της κάρτας γραφικών και περιορίζεται σε έναν επεξεργαστή της CPU.



Εικόνα 6.16 : Χρήση επεξεργαστή κατά τη διάρκεια προσπάθειας αποκρυπτογράφησης

Τα προϊόντα κρυπτογράφησης που υποστηρίζει μέχρι τη στιγμή που γράφεται αυτό το κείμενο είναι του παρακάτω πίνακα :

Vendor	**Product**	**Supported Versions**	**64-bit Support**
Check Point	Check Point Full Disk Encryption (formerly Pointsec PC)	6.3.1 up to 7.4, 8.0 (for Windows and Macintosh computers)	Yes
Credant	Mobile Guardian	5.2.1, 5.3, 5.4.1, 5.4.2, 6.1 through 6.8, 7.3	Yes
GuardianEdge	Encryption Plus/Anywhere	7 and 8	No
GuardianEdge	Hard Disk Encryption	9.1.5, 9.2.2 , 9.3.0, 9.4.0, 9.5.0, 9.5.1	Yes
McAfee	EndPoint Encryption (formerly SafeBoot)	4, 5, 6, 7 (for Windows and Macintosh	Yes (for Versions 4 and

		computers)	5)
Microsoft	BitLocker and BitLocker To Go	Windows Vista, 7, and 8, Server 2008	Yes
Sophos	SafeGuard Easy and Enterprise (formerly Utimaco)	4.5, 5.5, 5.6, 6.0	Yes (only for SafeGuard Easy, not for Enterprise)
Symantec	PGP Whole Disk Encryption	9.8, 9.9, 10, 10.1, 10.2	Yes
Symantec	Endpoint Encryption	7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.0.7, 7.0.8, 8.0, 8.2	Yes
WinMagic	SecureDoc Full Disk Encryption	4.5, 4.6, 5.x, 6.x	Yes

6.3. Εργαλείο FTK (Forensic Toolkit 5)

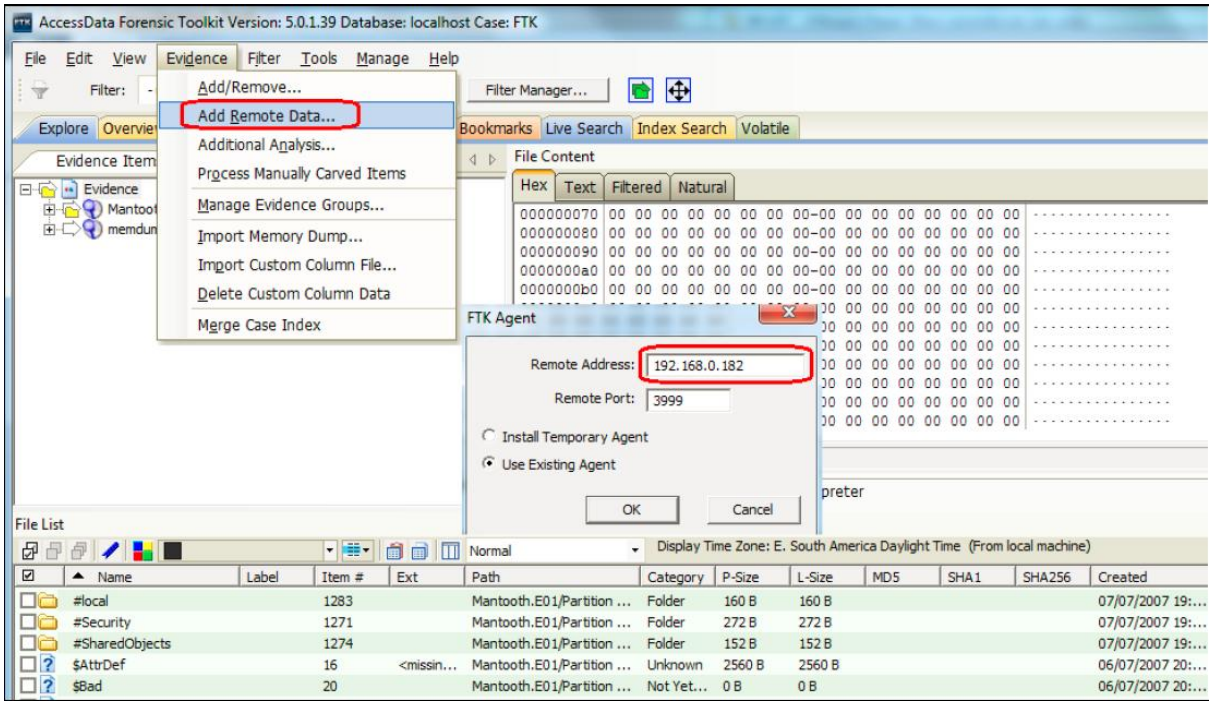
Το FTK είναι ένα εμπορικό εργαλείο λήψης και ανάλυσης ψηφιακών πειστηρίων της εταιρείας AccessData το οποίο περιλαμβάνει ένα εργαλείο λήψης εικόνας (FTK imager), ένα ανάλυσης δεδομένων (FTK &RegistryViewer), και 2 εργαλεία αποκρυπτογράφησης (PRTK & DNA) [29].

Το συγκεκριμένο εργαλείο είναι αυτό που χρησιμοποιεί η Αστυνομία Κύπρου και το οποίο της έχει επιτρέψει να έχει μεγάλες επιτυχίες, σε σχέση με το μέγεθός της σε προσωπικό και πόρους, έναντι στο ηλεκτρονικό έγκλημα οποιασδήποτε μορφής, παρά τους περιορισμούς από τη νομοθεσία.

Η εταιρεία παρέχει εκπαίδευση είτε με Διαδικτυακά σεμινάρια, είτε με μαθήματα σε τάξη σε όλα τα επίπεδα δίνοντας και την απαραίτητη πιστοποίηση στον υποψήφιο ερευνητή – αναλυτή. Τα προγράμματα εκπαίδευσης δεν αφορούν μόνο στη χρήση του εργαλείου αλλά και σε όλα τα θέματα της Ψηφιακής Δικανικής, όπως διαδικασίες και ανάλυση των πιο γνωστών λειτουργικών συστημάτων. Η υποστήριξη εκτός από το εγχειρίδιο χρήσης, το οποίο είναι πάρα πολύ καλό για έναν αρχάριο αλλά δεν εμβαθύνει ίσως όσο θα έπρεπε στα πιο πολύπλοκα χαρακτηριστικά του εργαλείου, περιλαμβάνει πέραν του φόρουμ και επίλυση προβλημάτων μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου.

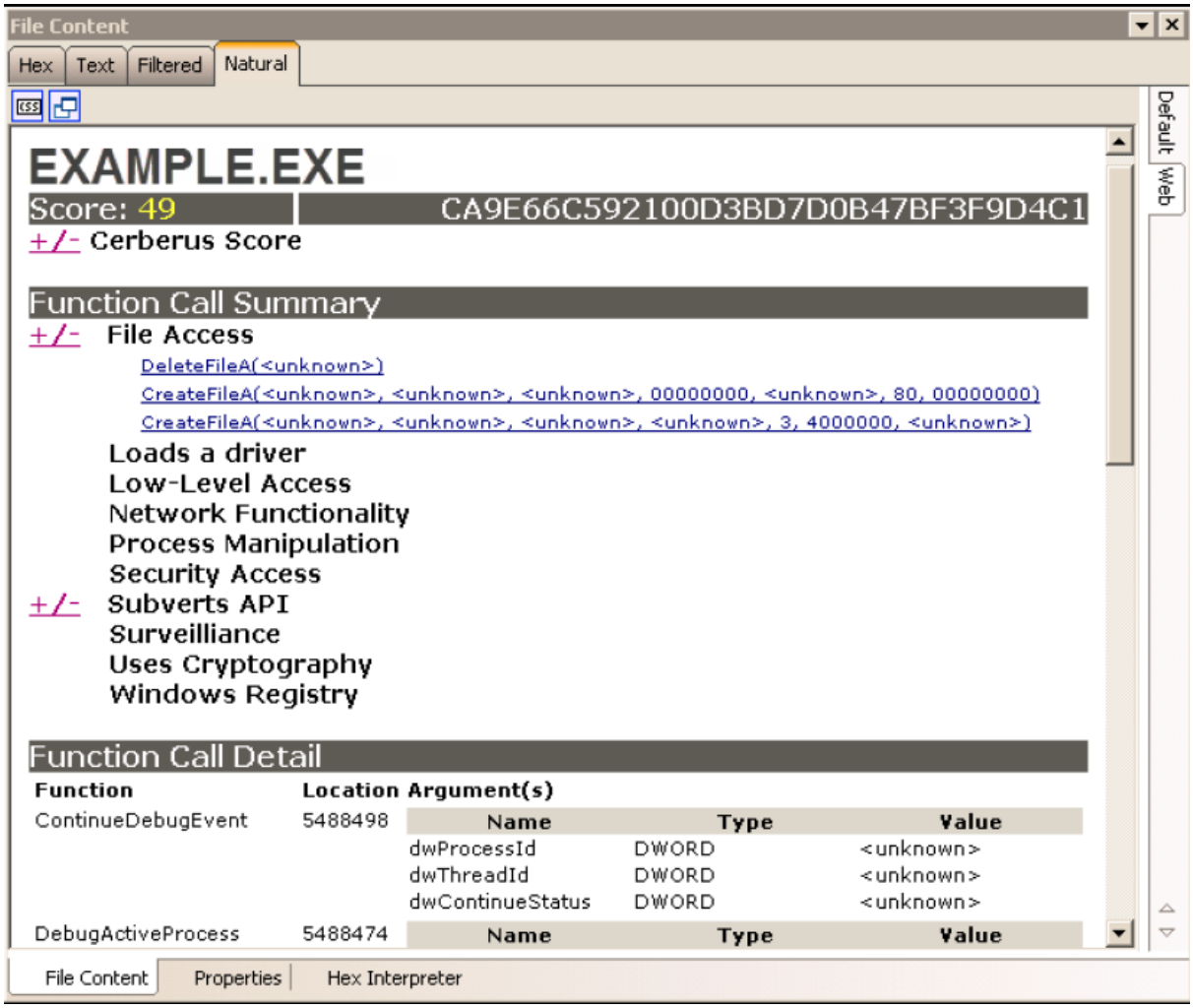
Έχει υψηλές απαιτήσεις σε υπολογιστικούς πόρους και για τη λειτουργία του απαιτείται και η χρήση βάσης δεδομένων η οποία μπορεί να είναι η PostgreSQL 9.1.13 η οποία παρέχεται δωρεάν από την Access Data, είτε η Oracle 10, είτε η Microsoft SQL Server 2008 R2 [27]. Λόγω της χρήσης της βάσης δεδομένων δεν παρουσιάζεται το φαινόμενο της απώλειας έργου του αναλυτή λόγω κατάρρευσης του συστήματος όπως παρουσιάζεται σε εργαλεία που βασίζονται στη χρήση της μνήμης. Τα τμήματα μεταξύ τους είναι διαμερισματοποιημένα και λειτουργούν ανεξάρτητα. Για παράδειγμα αν καταρρεύσει το γραφικό τμήμα, η επεξεργασία των δεδομένων συνεχίζει αδιάλειπτα.

Στην τελευταία αναβάθμισή του προστέθηκε και η δυνατότητα απομακρυσμένης ανάλυσης ή συλλογής δεδομένων από υπολογιστές που βρίσκονται στο ίδιο εσωτερικό δίκτυο, ένα χαρακτηριστικό το οποίο μπορεί να χρησιμοποιηθεί για συγκαλυμμένη διαδικασία λήψης ψηφιακών πειστηρίων.



Εικόνα 6.17 : Επιλογή απομακρυσμένης συλλογής και ανάλυσης ψηφιακών πειστηρίων με το εργαλείο FTK

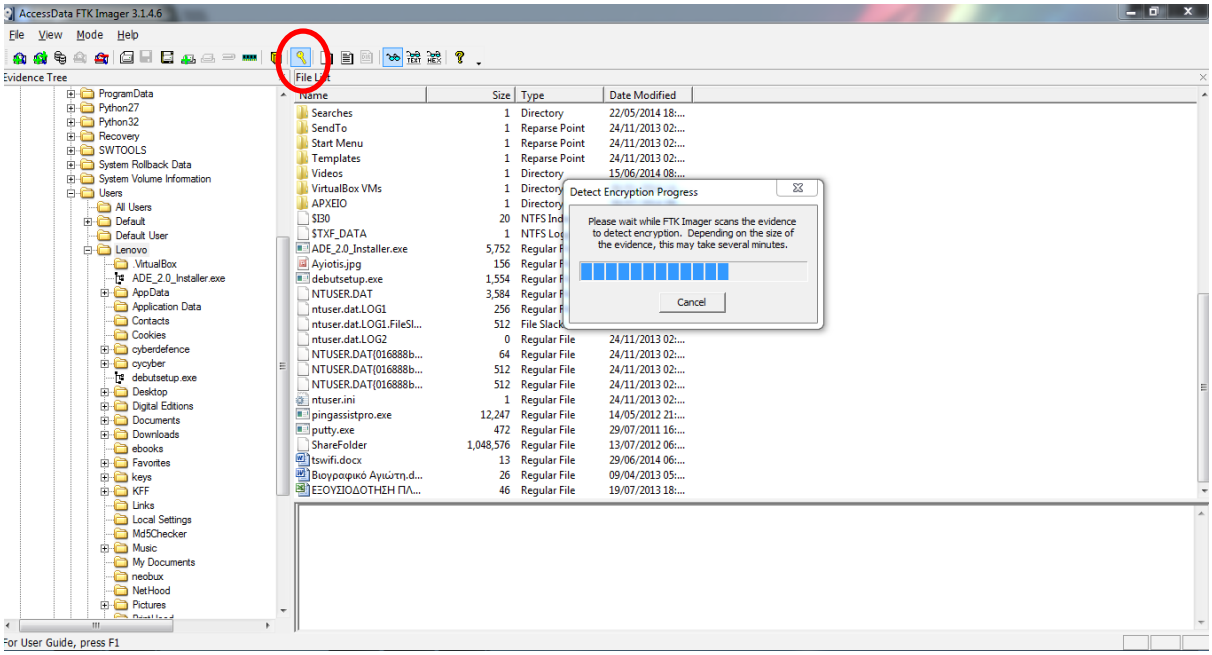
Ακόμα έχει προστεθεί η δυνατότητα διαλογής και ανάλυσης κακόβουλου λογισμικού με το εργαλείο CerberusAnalysis όπου αναλύσει όλα τα εκτελέσιμα αρχεία, τα συγκρίνει με τη βάση δεδομένων του και δίνει βαθμολογία στην απειλή που θεωρεί ότι υπάρχει [40].



Εικόνα 6.18 : Βαθμολογία επικινδυνότητας κακόβουλου λογισμικού από το CerberusAnalysis

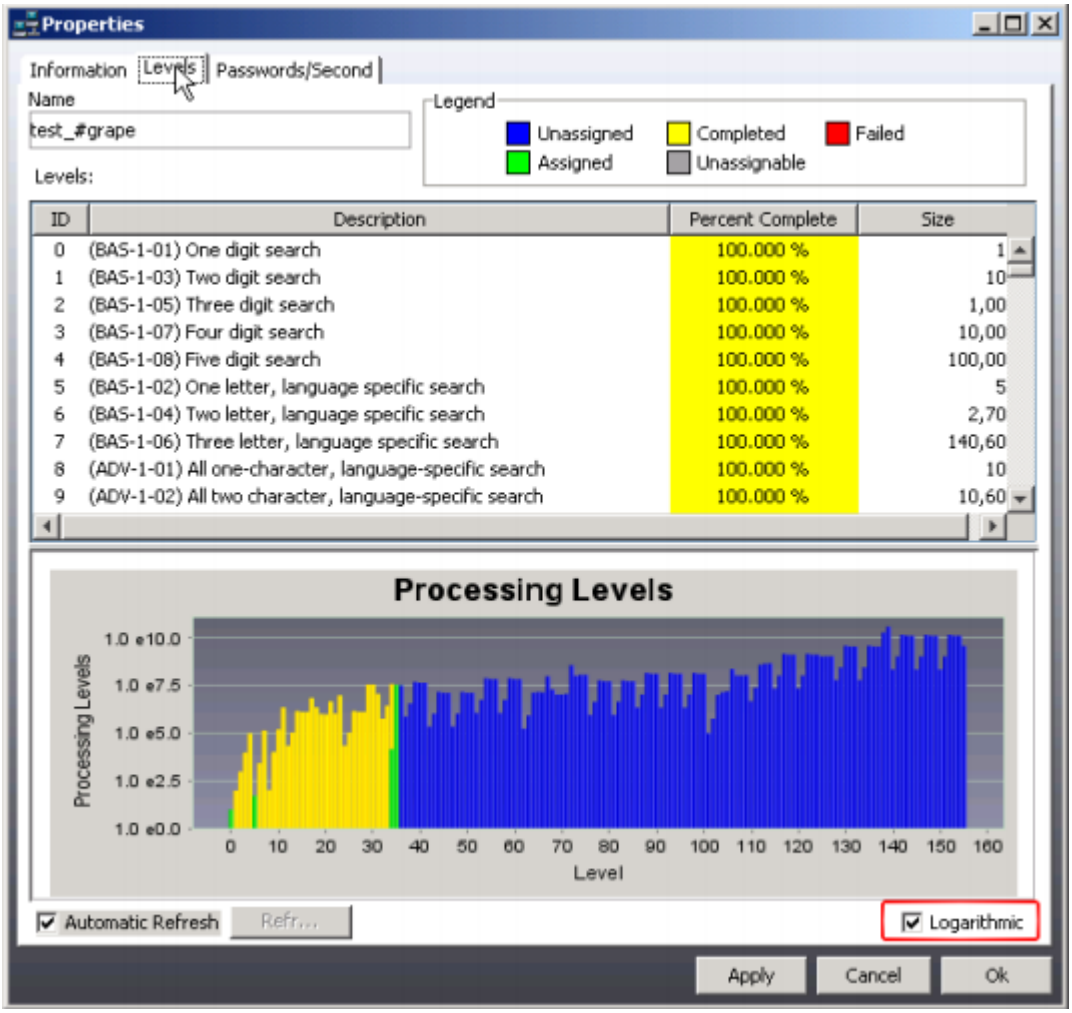
Έχει πολλές δυνατότητες σε αποκρυπτογράφηση με τη χρήση του PasswordRecoveryToolKit όπου μπορεί να αποκρυπτογραφήσει, ανάλογα πάντα με την επεξεργαστική ισχύ των μηχανημάτων και την ποιότητα του κωδικού που έχει χρησιμοποιηθεί, κρυπτογραφημένα αρχεία ή φακέλους από περισσότερες από 200 εφαρμογές κρυπτογράφησης. Το συγκεκριμένο εργαλείο έχει και τη δυνατότητα να εκμεταλλευτεί τις GPU των καρτών γραφικών που τυχόν να υπάρχουν και να πολλαπλασιάσει την ταχύτητα δοκιμών ανάλογα με το είδος της κάρτας. Στο εν λόγω χαρακτηριστικό έγινε επίδειξη στο δικανικό εργαστήριο της αστυνομίας όπου διαπιστώθηκε να γίνεται η δοκιμή των κωδικών με ρυθμό λίγο περισσότερο από δεκαπλάσιο σε σχέση με τη χρήση μόνο της CPU. Υποστηρίζει αποκρυπτογράφηση των Credant, SafeBoot, Utimaco, SafeGuardEnterpriseandEasy, EFS, PGP, GuardianEdge, Pointsec, S/MIMEOpenOffice, TrueCrypt, FileVault (Apple), FileVault 2 (Apple), DMGfiles (Apple), RAR, ZIP, includingWinZipadvancedencryption, 7-Zip, passwordprotectediOSbackupfiles, PGPpasswordfiles, BCArchive, BCTextEncoder, ABICoder, AdvancedFileLock, AShampoo, CryptoForge, Cypherus και άλλων λιγότερο διαδεδομένων προγραμμάτων. Πρέπει να τονιστεί

ότι είναι το μόνο εργαλείο που μπορεί να εντοπίσει τα κρυπτογραφημένα pdf αρχεία, τα οποία τα παρουσιάζει στον ερευνητή για να τους δώσει την ανάλογη προσοχή [27].



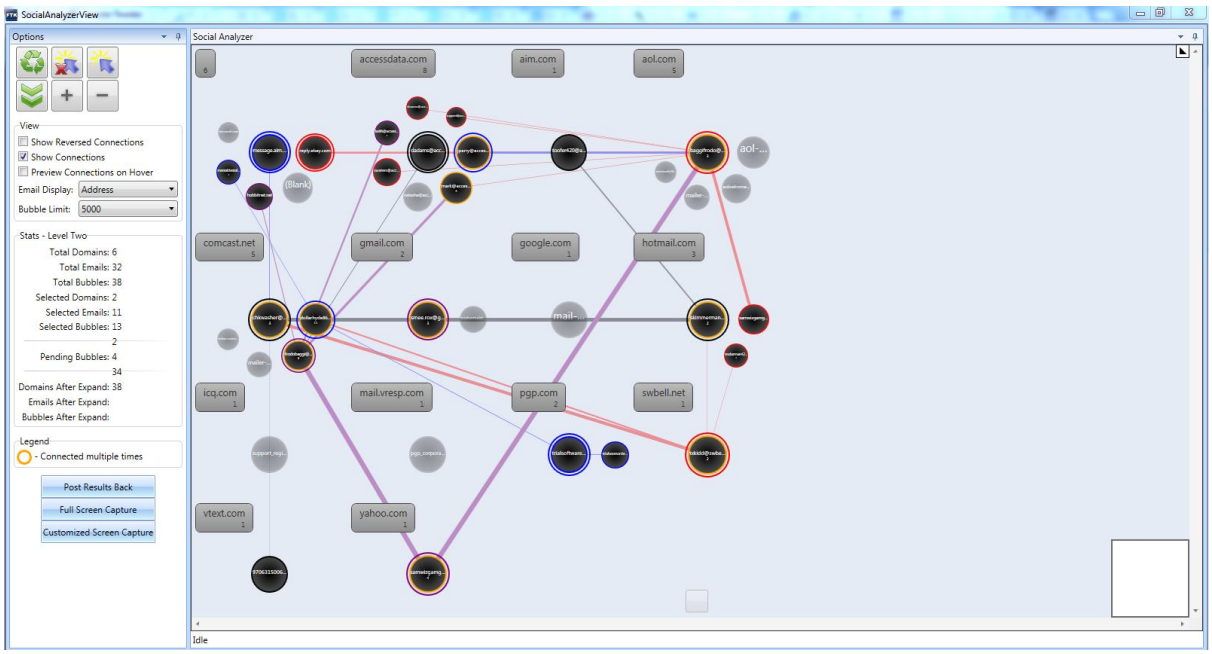
Εικόνα 6.19 : Εντοπισμός κρυπτογραφημένων αρχείων με σκοπό να τα προσέξει ο αναλυτής

Τα οποία μπορεί να γίνει προσπάθεια προσπέλασής τους με τη χρήση του εργαλείου PRTK 7.6 το οποίο προσφέρεται μαζί με το εν λόγω εργαλείο.

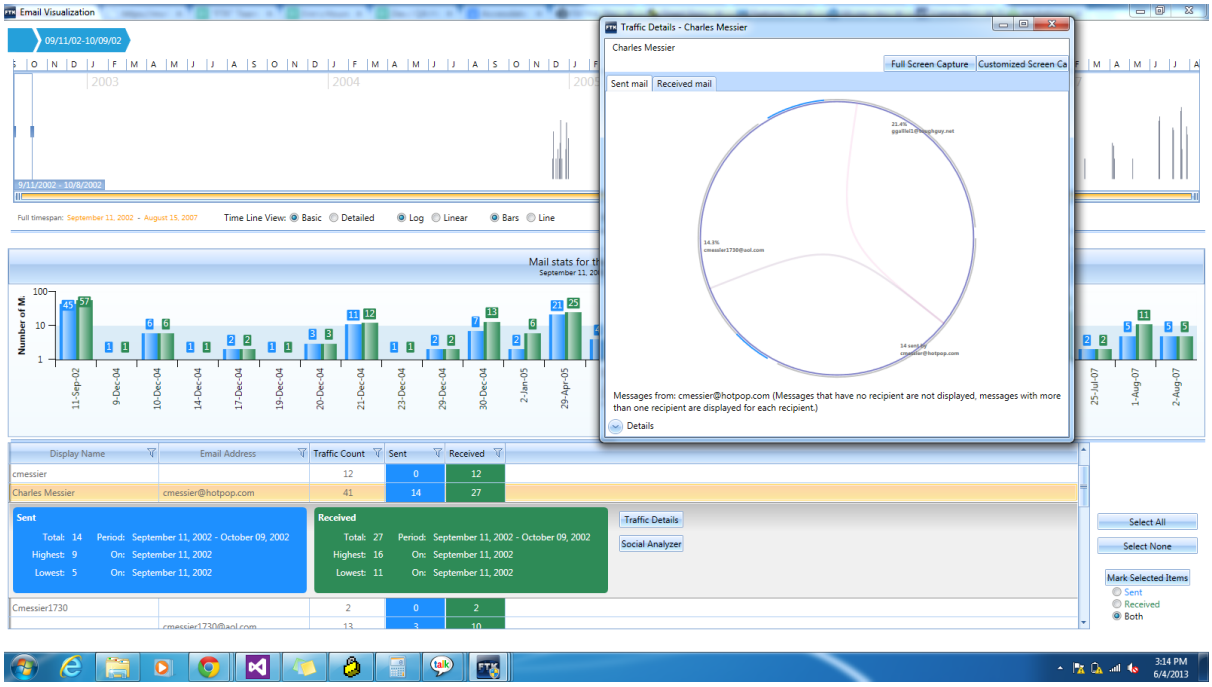


Εικόνα 6.20 : Προσπάθεια προσπέλασης κρυπτογραφημένων αρχείων με το PRTK 7.6

Επιτρέπει τον έλεγχο των δεδομένων με χρονική ταξινόμηση και παρουσιάζει με γραφικό τρόπο διακίνηση αλληλογραφίας, κοινωνικές συσχετίσεις όπως και την ποσότητα ανταλλαγής μηνυμάτων ή επαφών με αντίστοιχα δίκτυα που έλαβε χώρα στην υπό εξέταση συσκευή. Εξάγει στατιστικά που περιλαμβάνουν την αποστολή – λήψη ηλεκτρονικών μηνυμάτων ανάλογα με την περίοδο ενδιαφέροντος και μπορεί να παρουσιάζει αυτά τα στοιχεία με εικόνες στην τελική αναφορά του αναλυτή.

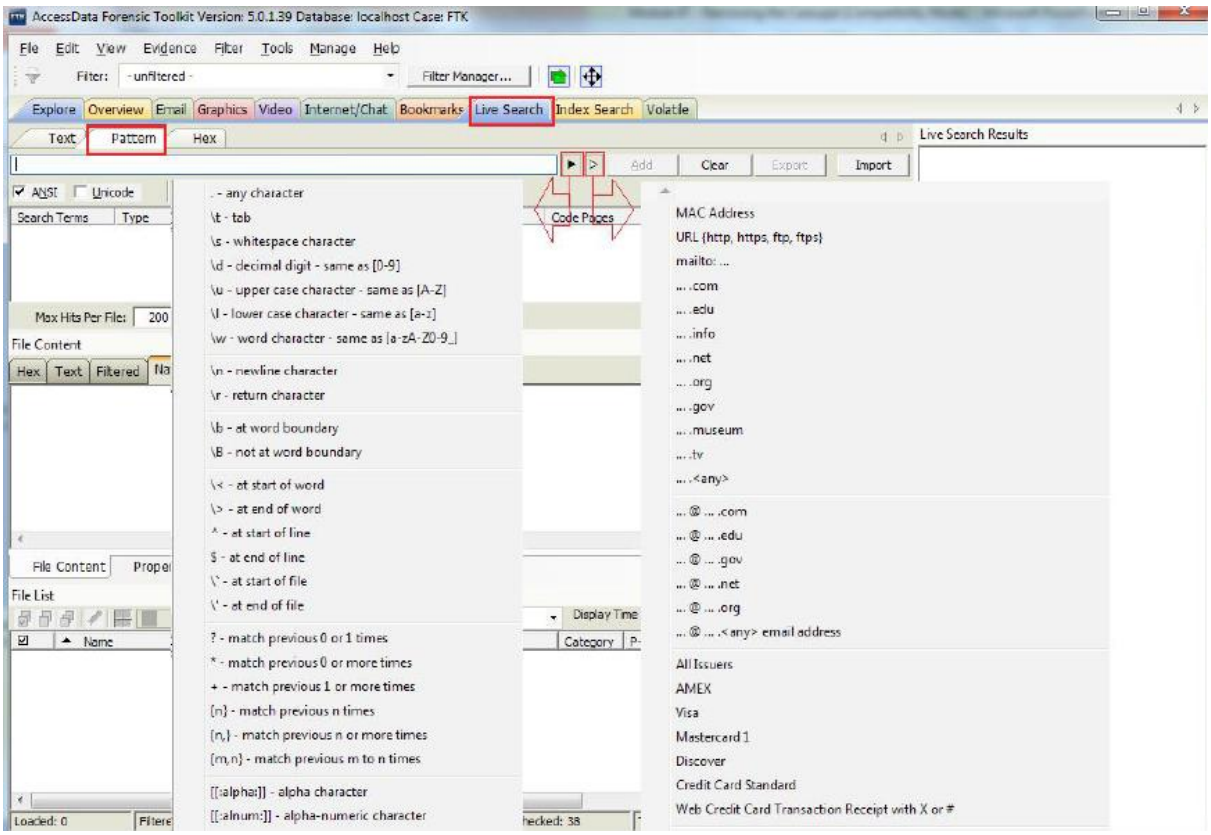


Εικόνα 6.21 : Ανάλυση κοινωνικών συσχετίσεων από τον εξεταζόμενο υπολογιστή.



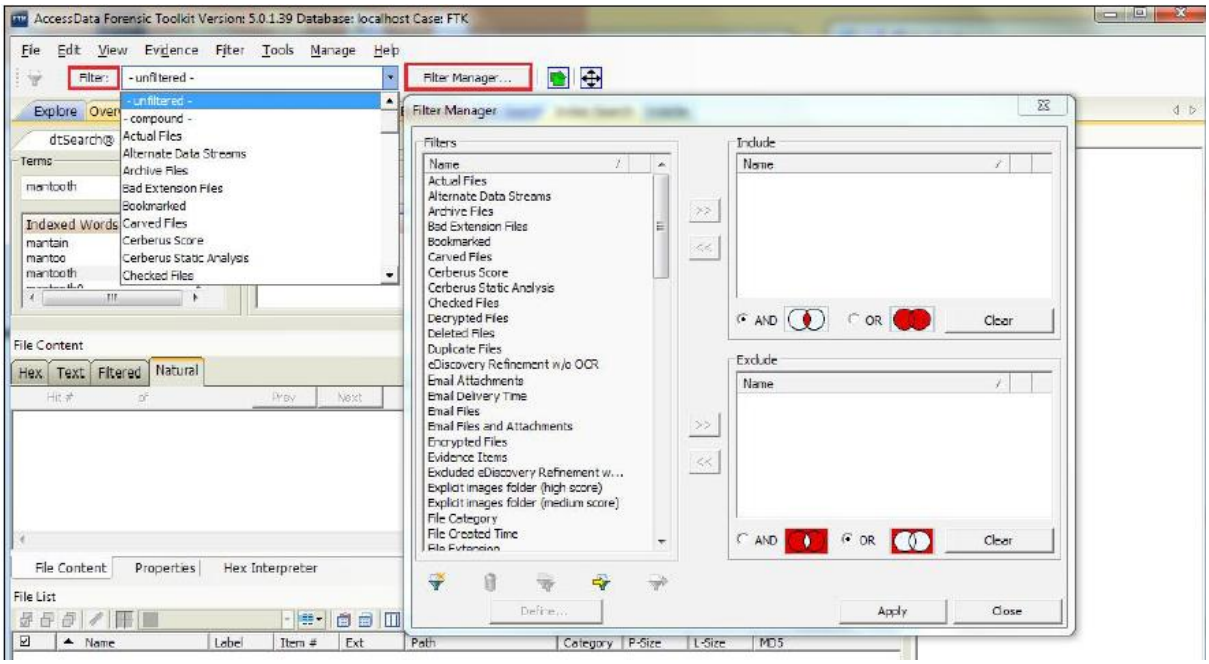
Εικόνα 6.22 : Αναλυτική κίνηση δικτύου με στατιστικά στοιχεία τα οποία διαμορφώνει ο ερευνητής

Η υποστήριξη των λογικών εκφράσεων κατά την αναζήτηση εντός του δημιουργημένου ευρετηρίου επιτρέπει τον εντοπισμό εξειδικευμένων συνδυασμών χαρακτήρων εντός όλων των εγγράφων κατά την αναζήτηση.



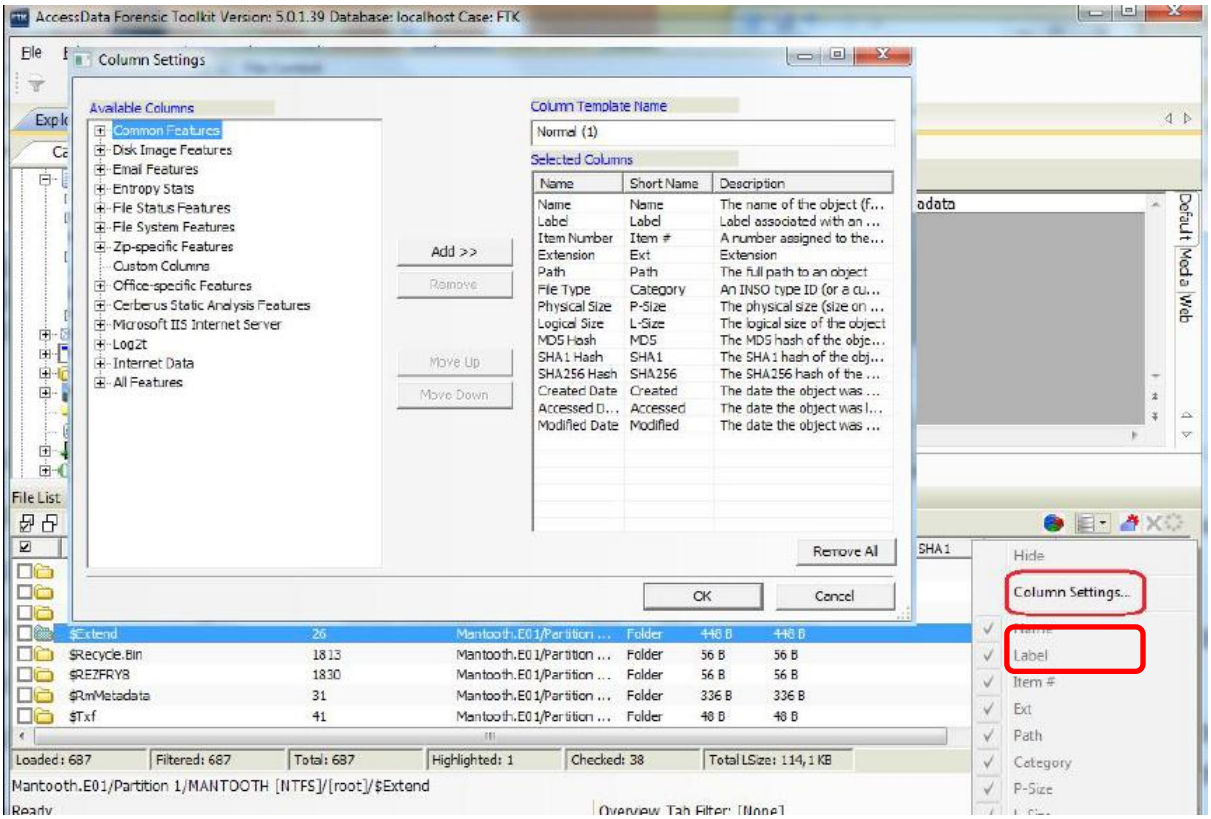
Εικόνα 6.23 : Αναζήτηση εντός του κειμένου των εγγράφων με χρήση λογικών τελεστών

Η χρήση των φίλτρων στην αναζήτηση ισχύει και σε αυτό το εργαλείο με την ύπαρξη πολλών προκαθορισμένων, αλλά και με τη δυνατότητα να δημιουργήσει δικά του ο ερευνητής.



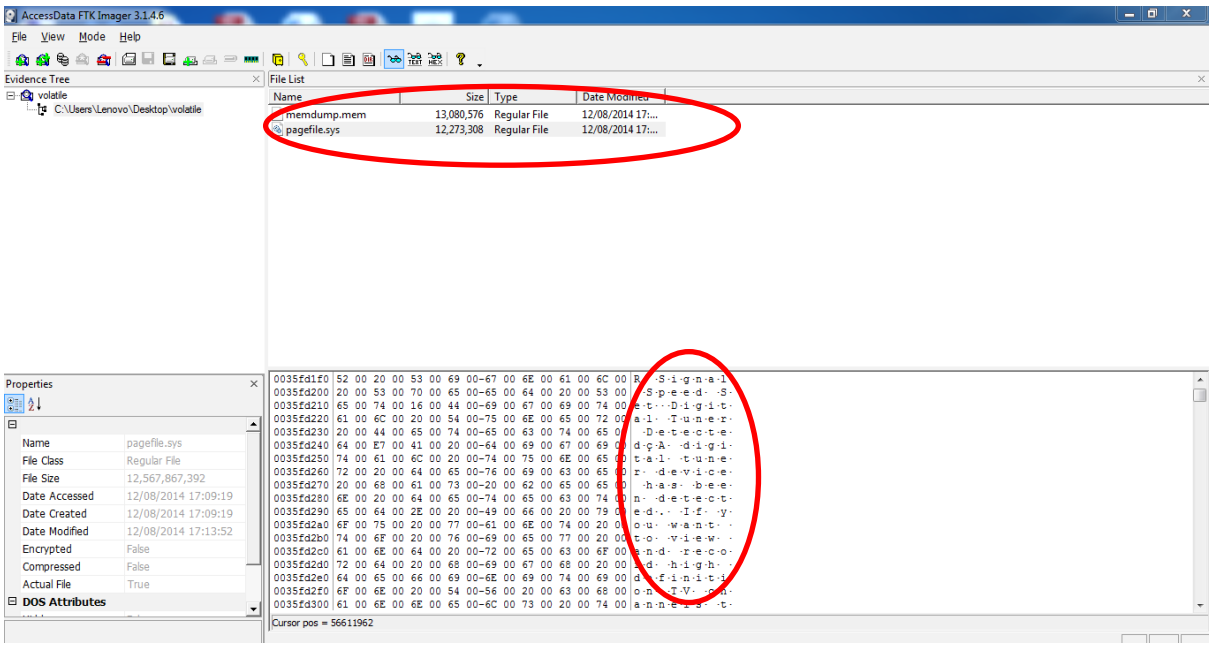
Εικόνα 6.24 : Χρήση φίλτρων για αναζήτηση εντός ευρετηρίου

Η παρουσίαση των μεταδεδομένων στο FTK γίνεται μέσω στηλών όπου η πρόσθεση ή η αφαίρεση των πληροφοριών που θέλει ο ερευνητής να φαίνονται για κάθε αρχείο γίνεται μέσα από το γραφικό του προγράμματος με την επιλογή τους με ένα κλικ.



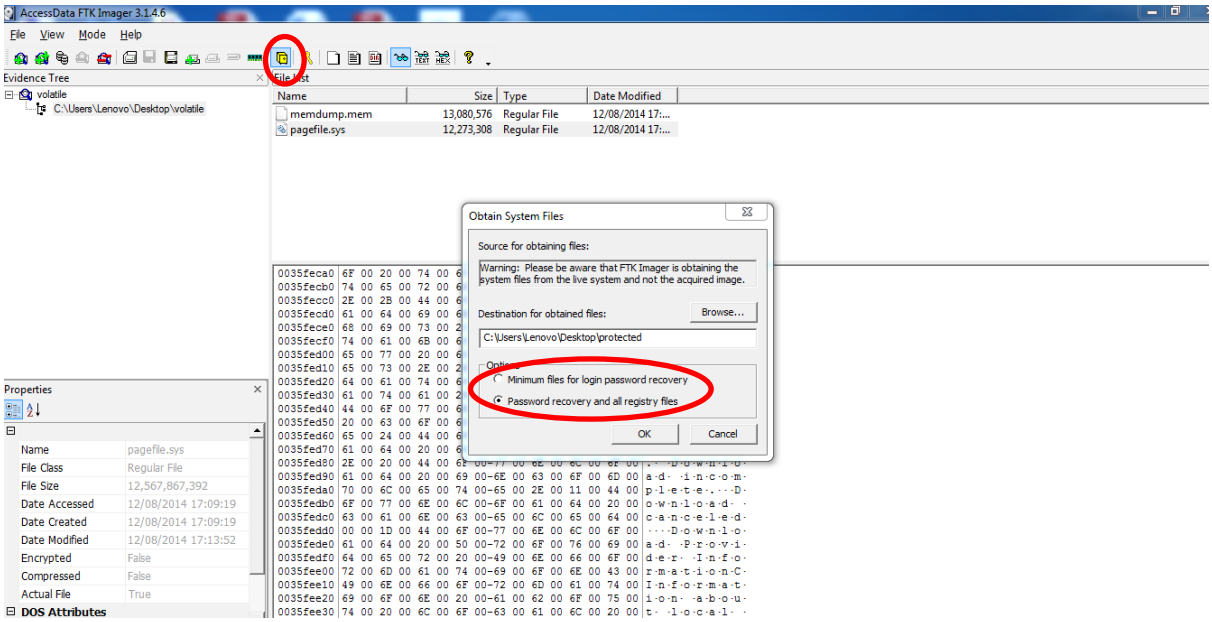
Εικόνα 6.25 : Προσθήκη ή αφαίρεση μεταδεδομένων αρχείων με χρήση στηλών

Η συλλογή των στοιχείων της πτητικής μνήμης όπως τρέχουσες διεργασίες, έγγραφα που χρησιμοποιούνται, ιστοσελίδες που προσπελάστηκαν, ονόματα χρήστη και κωδικούς γίνονται με το εργαλείο FTKimager [44].



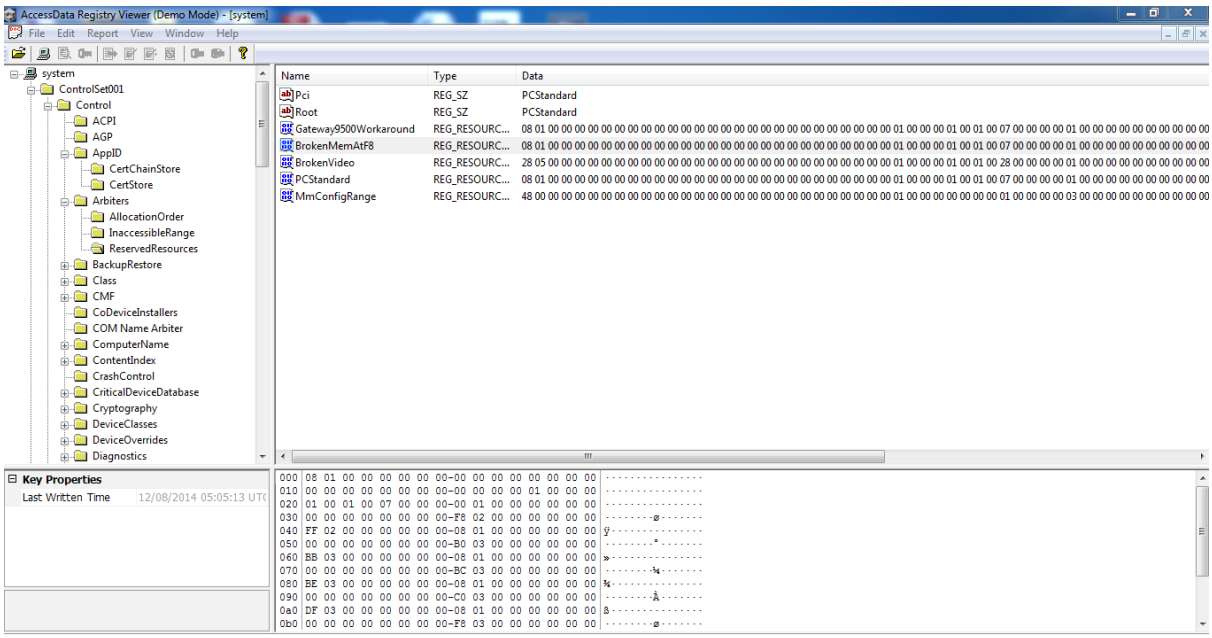
Εικόνα 6.26 : Συλλογή δεδομένων μνήμης RAM με toFTKimager (Πρακτική Δοκιμή)

Επίσης μπορεί να συλλέξει προστατευόμενα αρχεία, όπως τα αρχεία της Registry των windows.



Εικόνα 6.27 : Συλλογή δεδομένων προστατευόμενων αρχείων της registry με toFTKimager (Πρακτική Δοκιμή)

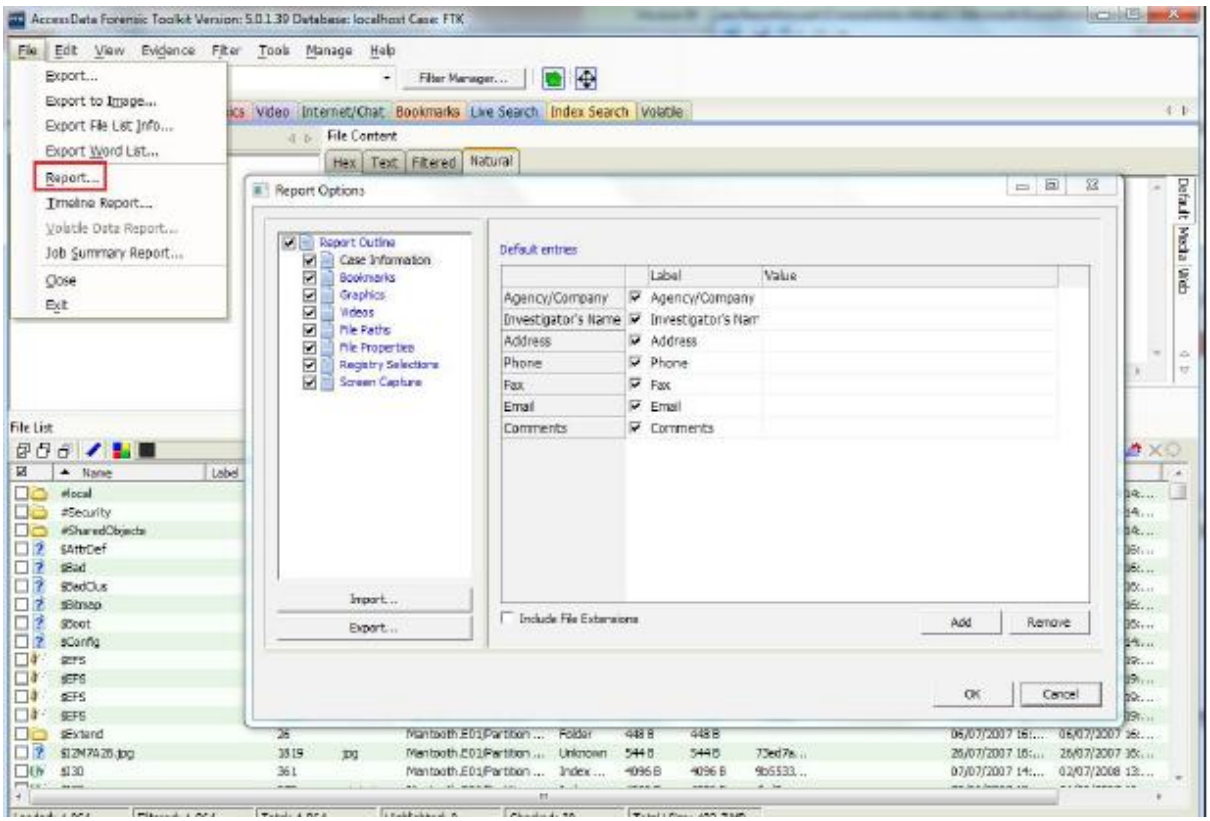
Τα οποία μπορούν να αναλυθούν με τη χρήση του εργαλείου RegistryViewer το οποίο περιλαμβάνεται στο πακέτο του FTK και διατίθεται δωρεάν από την ιστοσελίδα της εταιρείας μαζί με το FTKImager.



Εικόνα 6.28 : Ανάλυση δεδομένων της registry με toRegistryViewer (Πρακτική Δοκιμή)

Πέραν της συλλογής των στοιχείων και της δημιουργίας του ακριβούς αντίγραφου το εργαλείο έχει και τη δυνατότητα υποστήριξης συστήματος RAID. Η δυνατότητα αυτή εξετάστηκε, σε πραγματικές συνθήκες, στο εργαστήριο της Κυπριακής Αστυνομίας σε σύστημα RAID 5, πέντε δίσκων 1TB έκαστος, με τους δύο από τους πέντε μη λειτουργήσιμους. Αν και η διαδικασία ήταν αρκετά χρονοβόρα το αποτέλεσμα ήταν η πλήρης ανάκτηση των δεδομένων και η επαναφορά του συστήματος ως αρχική μορφή, μετά την αντικατάσταση των δίσκων.

Τέλος αφού ολοκληρωθεί η έρευνα κι έχουν βρεθεί τα απαραίτητα πειστήρια που ο ερευνητής αναζητούσε τότε μπορεί να γίνει η παρουσίαση των αποτελεσμάτων με τρόπο ώστε να μπορεί να γίνει αποδεκτός στο δικαστήριο. Η αυτόματη αναφορά περιλαμβάνει όλα όσα ο ερευνητής θεώρησε αναγκαία να παρουσιαστούν και έχει αποθηκεύσει σε όλη τη διάρκεια της έρευνας [27].



Εικόνα 6.29 : Δημιουργία αυτόματης αναφοράς

6.3 Το Εργαλείο X-WaysForensics

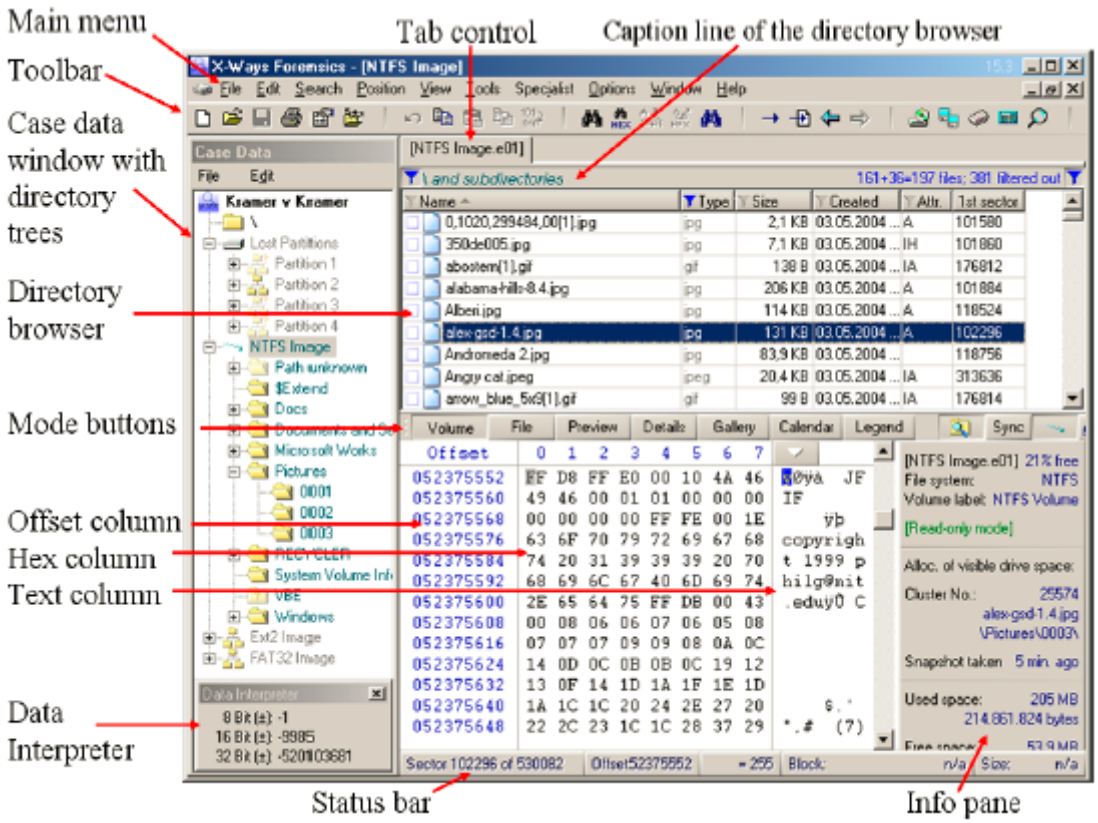
Το εργαλείο αυτό είναι η ολοκληρωμένη λύση στη ψηφιακή δικανική της εταιρίας X-WaysSoftwareTechnologyAGto οποίο όπως και τα προηγούμενα συνδυάζει τις δυνατότητες των επιμέρους εργαλείων της εταιρείας με τρόπο που να επιτρέπει τη διενέργεια μιας πλήρους έρευνας χωρίς την ανάγκη απόκτησης άλλου λογισμικού για σκοπούς ολοκλήρωσής της [31].

Η υποστήριξη που παρέχεται από την κατασκευάστρια εταιρεία αφορά σε εκπαίδευση σε τμήματα σε όλον τον κόσμο, με την επιτυχή ολοκλήρωση των οποίων παρέχεται η ανάλογη πιστοποίηση και υπάρχει και το αντίστοιχο εγχειρίδιο χρήσης και ανάλογα βίντεο τα οποία επιτρέπουν σε κάποιο αρχάριο να ανακαλύψει γρήγορα και εύκολα τις δυνατότητές του. Σε περίπτωση που χρειαστεί τεχνική υποστήριξη, παρέχεται μέσω ηλεκτρονικού ταχυδρομείου και μέσω φόρουμ.

Σύμφωνα με την εταιρεία οι απαιτήσεις σε υπολογιστικούς πόρους είναι πολύ περιορισμένες σε σχέση με τον ανταγωνισμό και μπορεί να τρέξει σε υπολογιστές καθημερινής χρήσης, με την

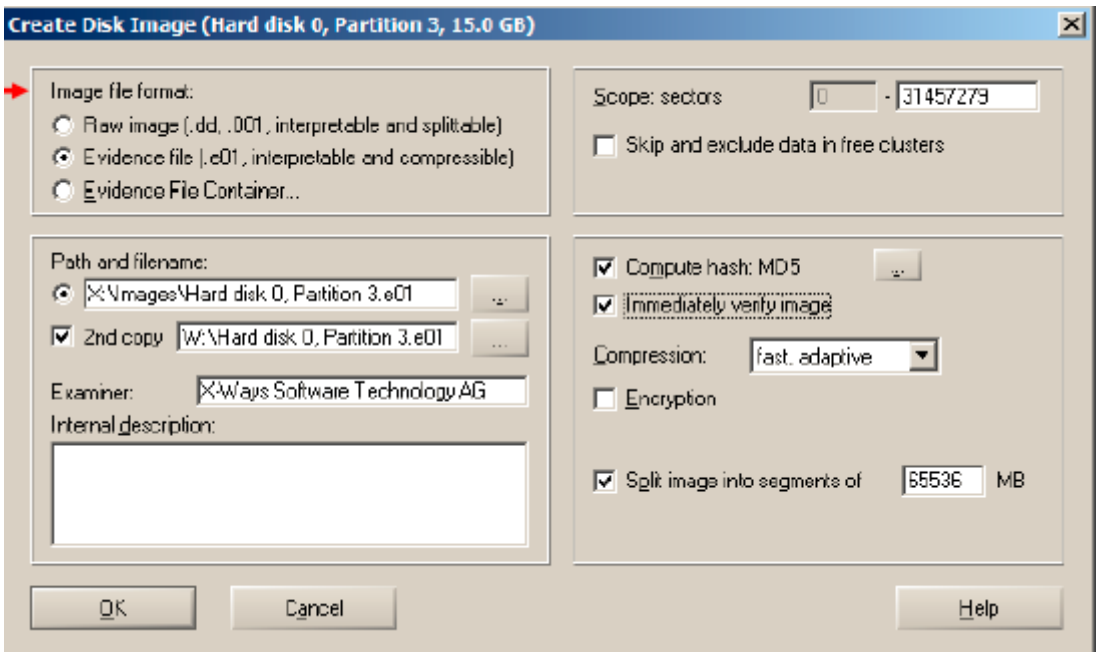
ανάλογη βέβαια καθυστέρηση στη συλλογή και ανάλυση, η οποία εξαρτάται άμεσα από τον όγκο δεδομένων που θα τύχει επεξεργασίας.

Η διεπαφή με τον ερευνητή είναι του ίδιου επιπέδου με τα προηγούμενα εργαλεία και βασίζεται στη χρήση ενός καλά δομημένου γραφικού περιβάλλοντος, γεγονός που κάνει σχετικά απλή τη χρήση του.



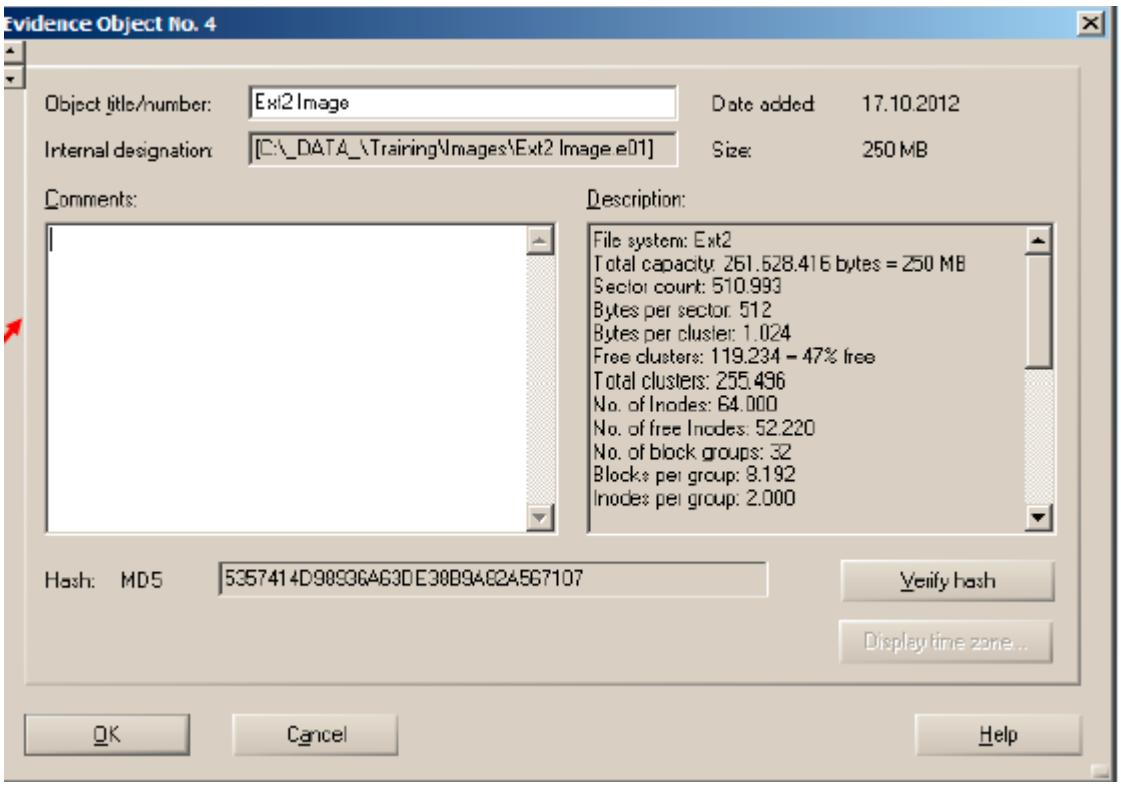
Εικόνα 6.30 : Γραφικό περιβάλλον του εργαλείου X-WaysForensics

Η δημιουργία του ακριβούς αντίγραφου γίνεται με λίγα μόνο κλικ και επιτρέπει την ταυτόχρονη παραγωγή 2 αντιγράφων τα οποία μπορούν να είναι και κρυπτογραφημένα καθώς και μοιρασμένα για να μπορούν να τοποθετηθούν με τη λήξη της υπόθεσης σε μαγνητικά μέσα μικρότερης χωρητικότητας για να αποθηκευτούν. Η λήψη των ψηφιακών πειστηρίων από απομακρυσμένο υπολογιστή είναι δυνατή μόνο με την προμήθεια του λογισμικού F-Responseτο οποίο δεν είναι της ίδιας εταιρείας και απαιτεί ξεχωριστή άδεια χρήσης [45].



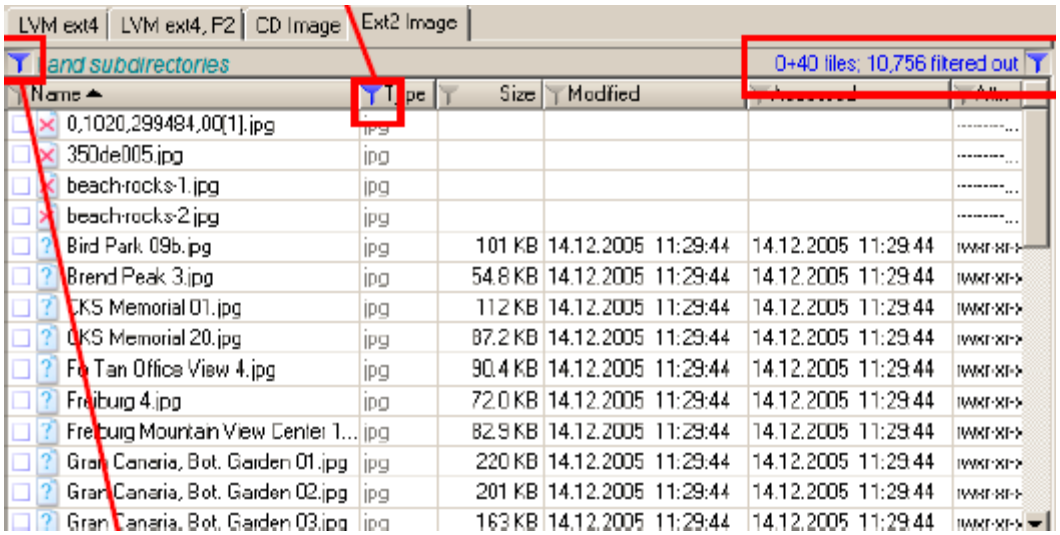
Εικόνα 6.31 : Δημιουργία ακριβούς αντιγράφου ψηφιακού μέσου αποθήκευσης

Ο ερευνητής για κάθε υπόθεση μπορεί να δημιουργεί πίνακες όπου θα αποθηκεύει έγγραφα, εικόνες ή αρχεία τα οποία κατά τη διάρκεια της έρευνας θεωρεί πως μπορεί να τα χρησιμοποιήσει και να τα παρουσιάσει στην τελική του αναφορά.



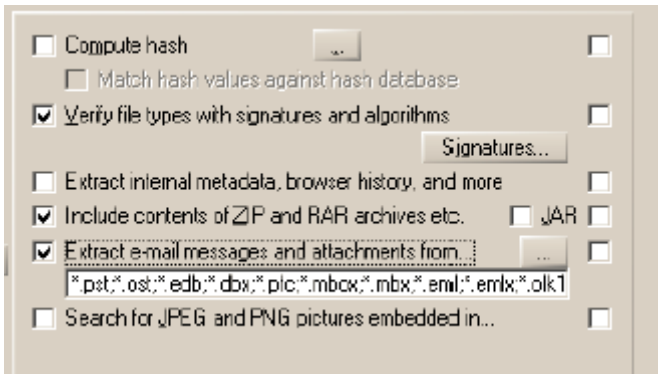
Εικόνα 6.32 : Δημιουργία πίνακα αποθήκευσης εγγράφων ή αρχείων για μελλοντική χρήση

Η αναζήτηση στα αρχεία του υπόπτου υπολογιστή γίνεται με τη χρήση φίλτρων τα οποία επιτρέπουν με το συνδυασμό τους να γίνει επιλογή οποιουδήποτε είδους αρχείου.



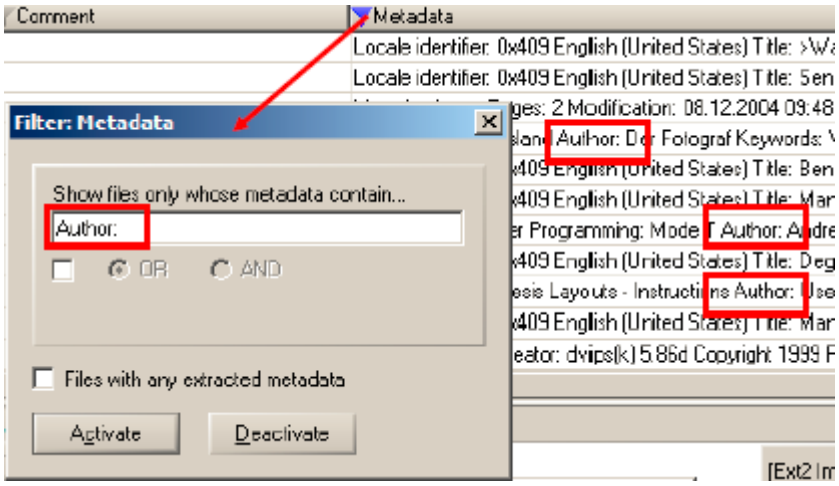
Εικόνα 6.33 : Έρευνα στο ευρετήριο αρχείων με χρήση προεγκατεστημένων φίλτρων

Η αναζήτηση ηλεκτρονικής αλληλογραφίας μπορεί να γίνει με δυνατότητα διαχωρισμού των μηνυμάτων από τα υπόλοιπα αρχεία, αλλά δεν υπάρχει η δυνατότητα δημιουργίας του νήματος μιας συζήτησης. Παρέχεται μόνο η ημερομηνία και η ώρα που αποθηκεύτηκε το αρχείο και η χρονοβόρα εργασία της δημιουργίας του νήματος πρέπει να γίνει από τον ίδιο τον ερευνητή.



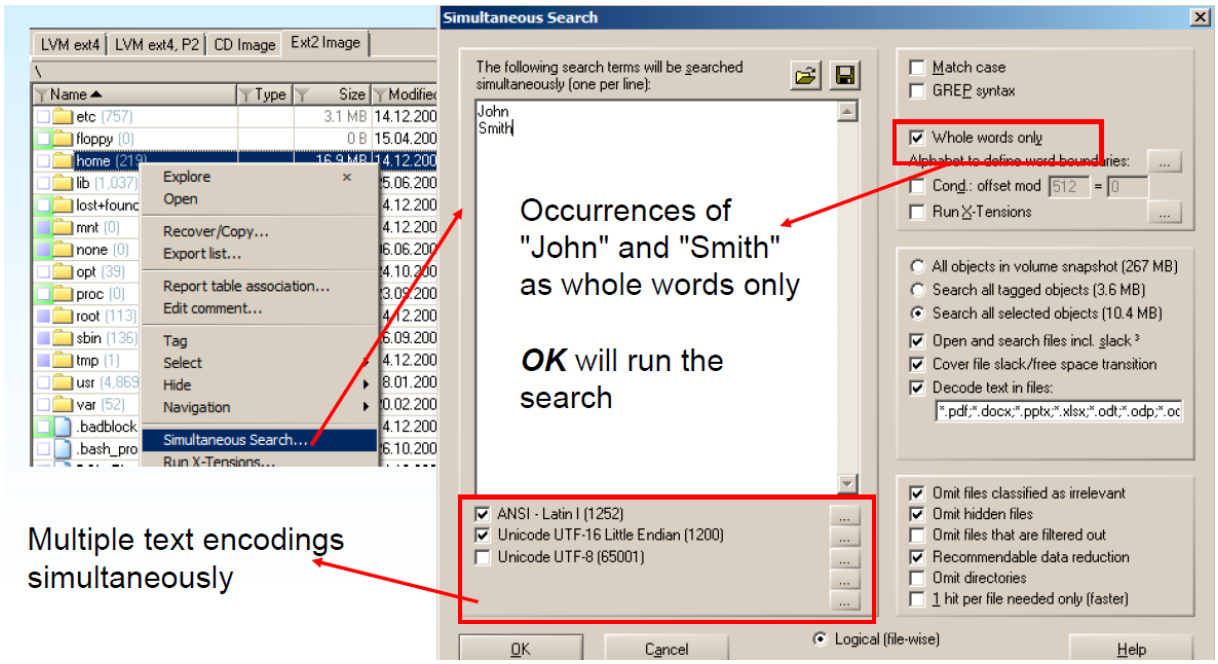
Εικόνα 6.34 : Συλλογή μηνυμάτων ηλεκτρονικής αλληλογραφίας χωρίς τη δυνατότητα αναδημιουργίας του νήματος της συζήτησης μεταξύ των αποστολέων.

Η λήψη των μεταδεδομένων των αρχείων καθώς και αρχείων, καθώς και η ιστορία των φυλλομετρητών μπορεί να γίνει με τον ίδιο τρόπο που γίνεται και η λήψη της ηλεκτρονικής αλληλογραφίας και το εργαλείο δίνει τη δυνατότητα στον ερευνητή να εκτελέσει αναζήτηση με φίλτρα που αφορούν στα μεταδεδομένα.



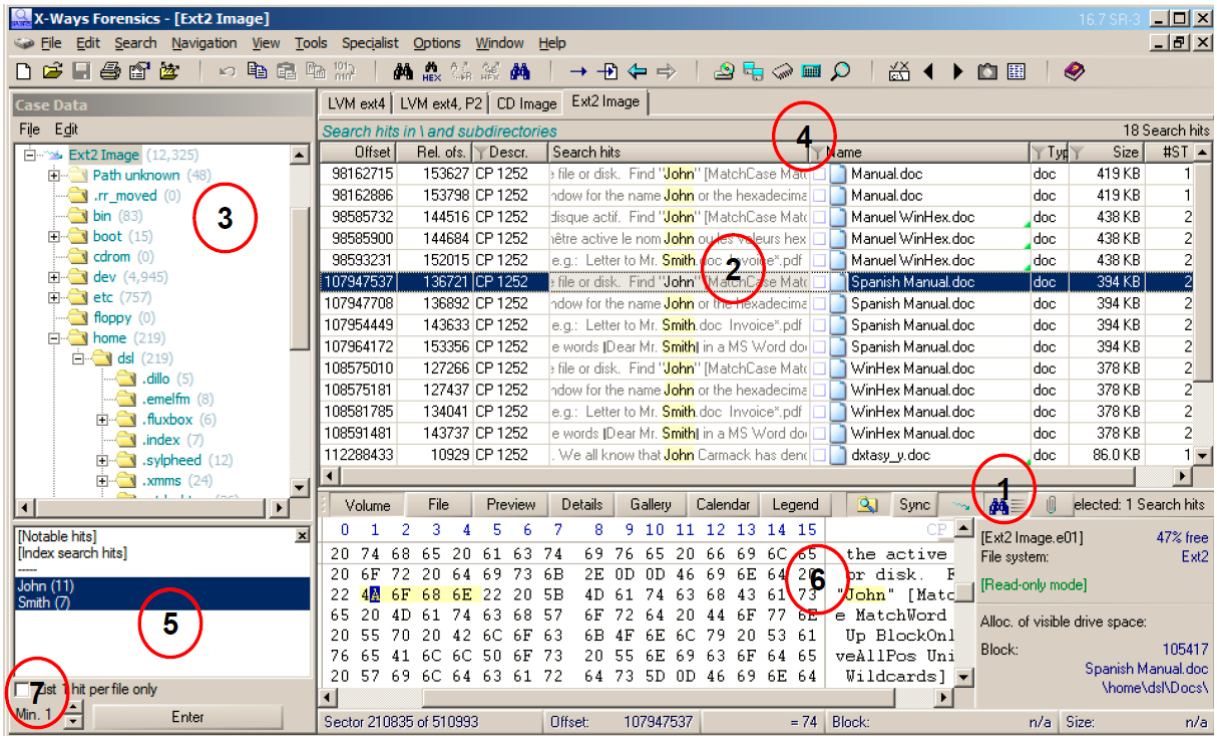
Εικόνα 6.35 : Αναζήτηση αρχείων με τη χρήση μεταδεδομένων για φίλτρο.

Η αναζήτηση κειμένου μέσα στα έγγραφα γίνεται όπως και στα προηγούμενα εργαλεία με τη χρήση λογικών εκφράσεων ταυτόχρονα σε πολλαπλή κωδικοποίηση το οποίο επιτρέπει την αναζήτηση ακόμα και σε έγγραφα που έχει τροποποιηθεί η επέκτασή τους για να μην εντοπίζονται.



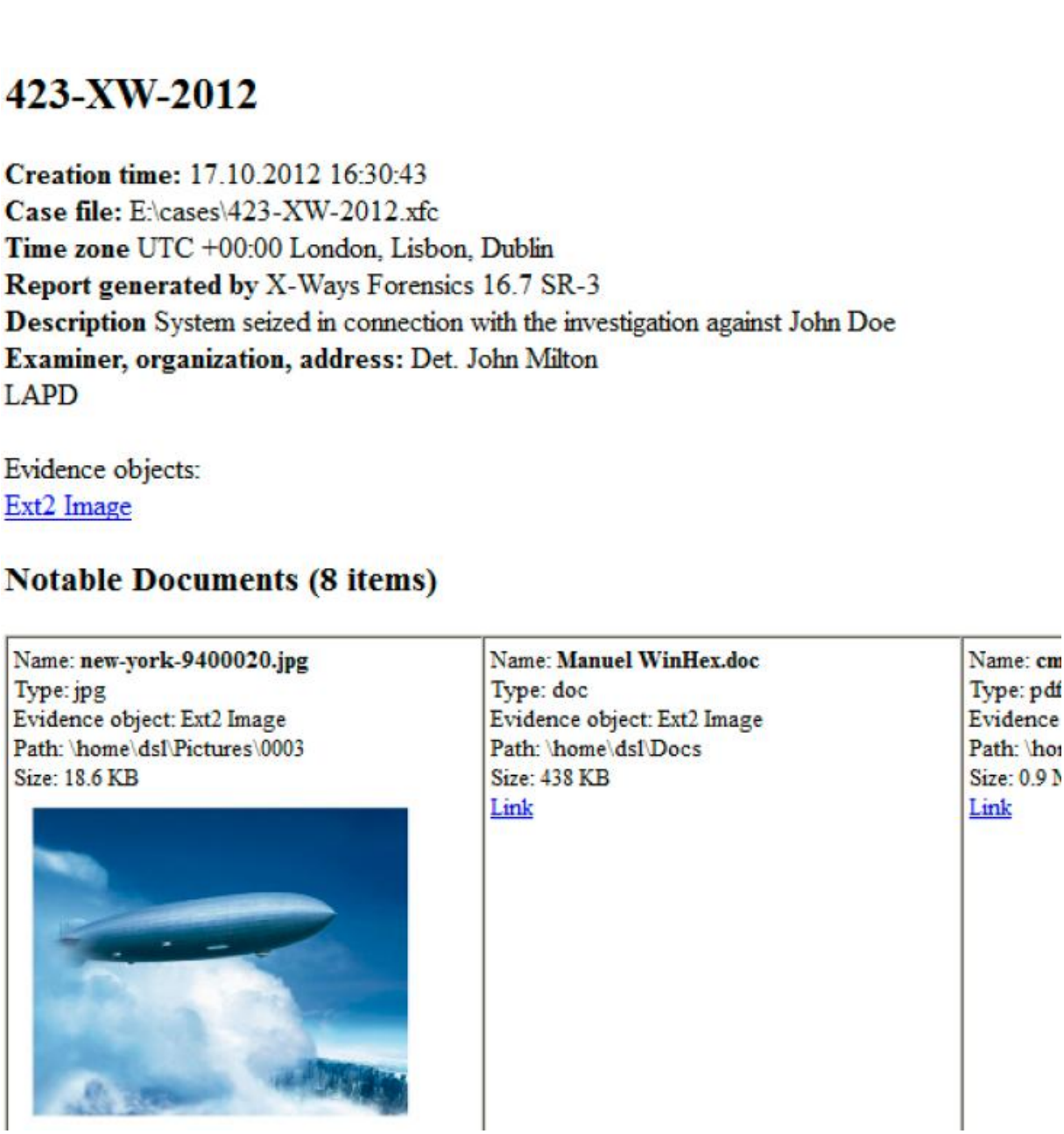
Εικόνα 6.36 : Αναζήτηση κειμένου εντός των εγγράφων με χρήση λογικών τελεστών.

Η οποία αναζήτηση θα φέρει όλα τα αποτελέσματα, αναλόγως κωδικοποίησης, στον ερευνητή για αξιολόγηση και αποθήκευση των αρχείων που τον ενδιαφέρουν.



Εικόνα 6.37 : Τρόπος εμφάνισης αποτελεσμάτων αναζήτησης κειμένου εντός των εγγράφων

Όταν συλλεχθούν και αναλυθούν όλα τα στοιχεία από τον ερευνητή, τότε μπορεί να ετοιμάσει την αναφορά που θα παρουσιάσει με τα ευρήματά του με τη χρήση του εργαλείου, όπου σε μορφή htmlπαρουσιάζονται όλα όσα είχε αποθηκεύσει για παρουσίαση. Στην παρουσίαση για όλα τα αρχεία που δεν είναι εικόνες περιλαμβάνονται σύνδεσμοι, ενώ οι εικόνες ενσωματώνονται απευθείας.



423-XW-2012

Creation time: 17.10.2012 16:30:43
Case file: E:\cases\423-XW-2012.xfc
Time zone UTC +00:00 London, Lisbon, Dublin
Report generated by X-Ways Forensics 16.7 SR-3
Description System seized in connection with the investigation against John Doe
Examiner, organization, address: Det. John Milton
LAPD

Evidence objects:
Ext2 Image

Notable Documents (8 items)

Name: **new-york-9400020.jpg**
Type: jpg
Evidence object: Ext2 Image
Path: \home\dsl\Pictures\0003
Size: 18.6 KB

Name: **Manuel WinHex.doc**
Type: doc
Evidence object: Ext2 Image
Path: \home\dsl\Docs
Size: 438 KB
Link

Name: **cm**
Type: pdf
Evidence
Path: \ho
Size: 0.9 M
Link

Εικόνα 6.38 : Δημιουργία αυτόματης αναφοράς σύμφωνα που περιλαμβάνει όσα θεωρεί ο ερευνητής πως πρέπει να παρουσιαστούν σε μορφή μόνο HTML.

6.4 Το Εργαλείο ADFTriage-G2

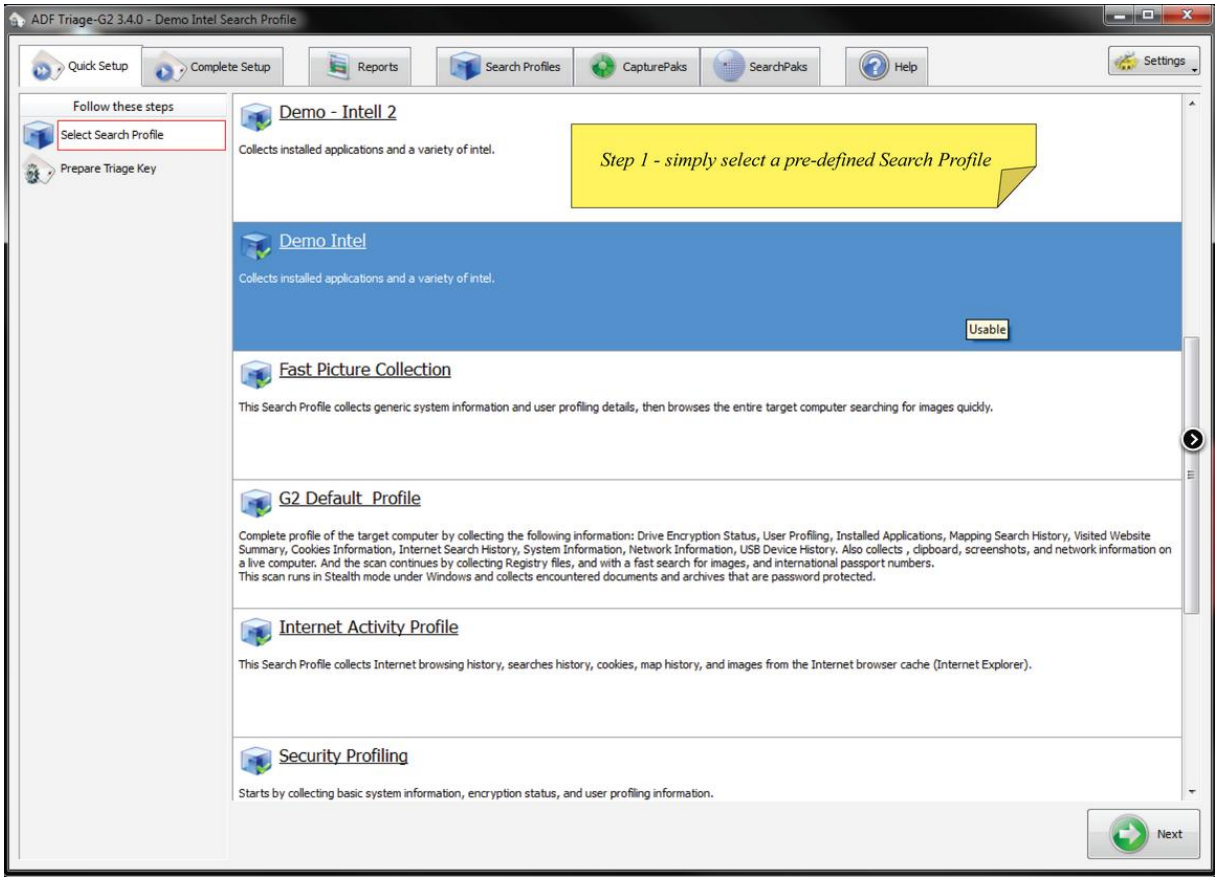
Είναι εργαλείο της εταιρείας ADFSolutionsto οποίο προορίζεται κυρίως για χρήση από οργανισμούς που ασχολούνται περισσότερο με την ασφάλεια, όπως στρατός, μυστικές υπηρεσίες και παρόμοιους κρατικούς οργανισμούς [33]. Λόγω της φύσεως της αποστολής του σαν εργαλείο έχει πολύ περιορισμένες δυνατότητες σε σχέση με τα προαναφερθέντα σε θέματα όπως λήψη ακριβούς αντίγραφου δίσκου και γενικά στον όγκο δεδομένων τον οποίο μπορεί να διαχειριστεί.

Ο ερευνητής μπορεί να χρησιμοποιήσει το εργαλείο ενώ ο υπολογιστής είναι ενεργοποιημένος ή να χρησιμοποιήσει τοcdεκκίνησης για μια εκκίνηση που δε θα αφήσει ίχνη και θα είναι δικανικά αποδεκτή. Το εργαλείο έρχεται σε μικρή φορητή συσκευασία μαζί με παρελκόμενα τα οποία μπορούν να χρησιμοποιηθούν για το άνοιγμα της υποδοχής του cd χωρίς την εκκίνηση του υπολογιστή ή να διευκολύνουν τον ερευνητή στην προσπάθειά του για ανάκτηση των πληροφοριών που αναζητεί.

Εικόνα 6.39 : Σετ εργαλείων που παραλαμβάνει από τον ερευνητή κάποιος που θα πάει να συλλέξει τις πληροφορίες από τον προς εξέταση υπολογιστή.

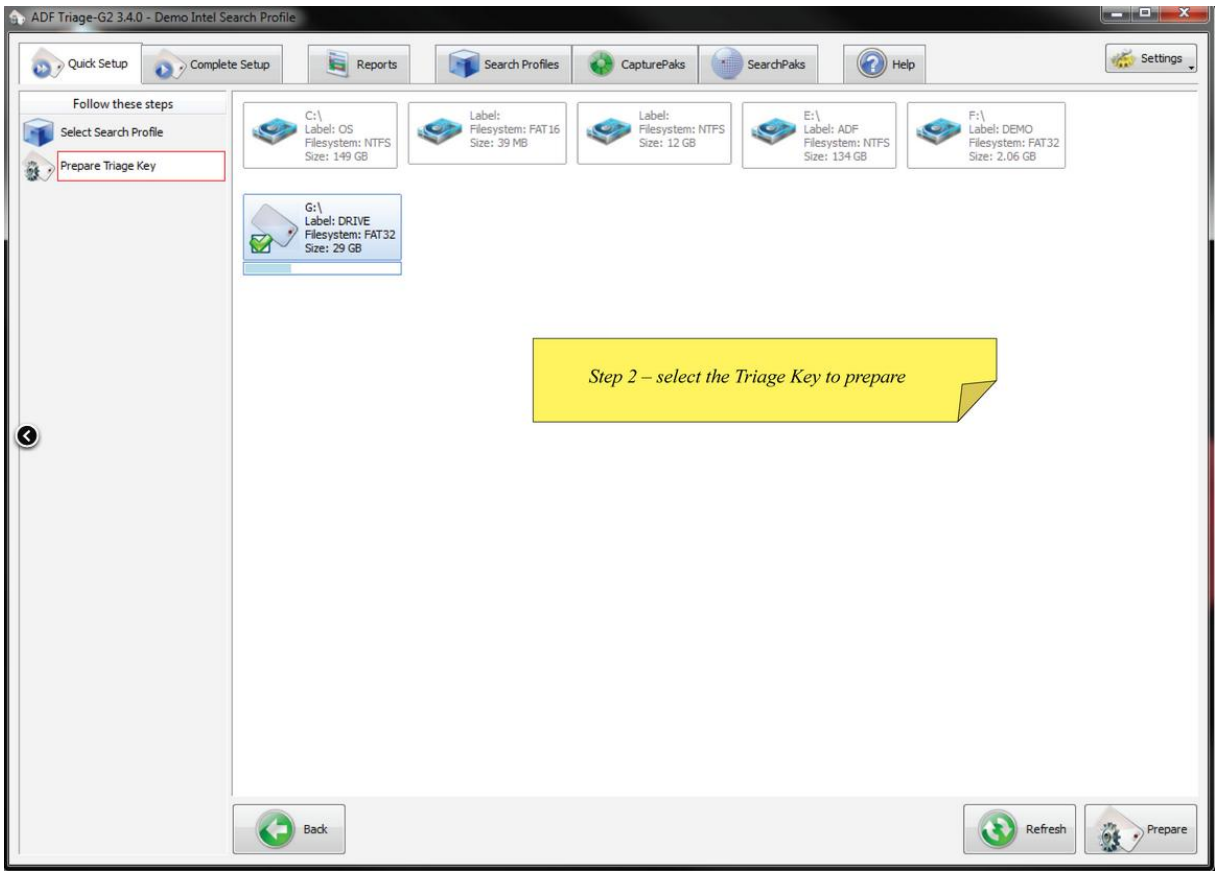
Η διαδικασία συλλογής και ανάλυσης των δεδομένων είναι πολύ διαφορετική και πολύ απλή σε σχέση με των υπολοίπων [41]. Λόγω του ότι είναι σχεδιασμένο για να χρησιμοποιείται από μη εξειδικευμένο προσωπικό, το μόνο που χρειάζεται να κάνει ο χειριστής είναι να κάνει χρήση του USBkey, το οποίο έχει προετοιμαστεί κατάλληλα με την επιλογή των παραμέτρων αναζήτησης σύμφωνα με την αποστολή.

Για ευκολία χρήσης το Triage-G2 έχει προεγκατεστημένα προφίλ αναζήτησης, με αποτέλεσμα να μπορεί ο χειριστής να ελέγξει και να αναλύσει τους ύποπτους υπολογιστές με 2 κινήσεις. Η πρώτη είναι η επιλογή του προφίλ που θα χρησιμοποιηθεί.



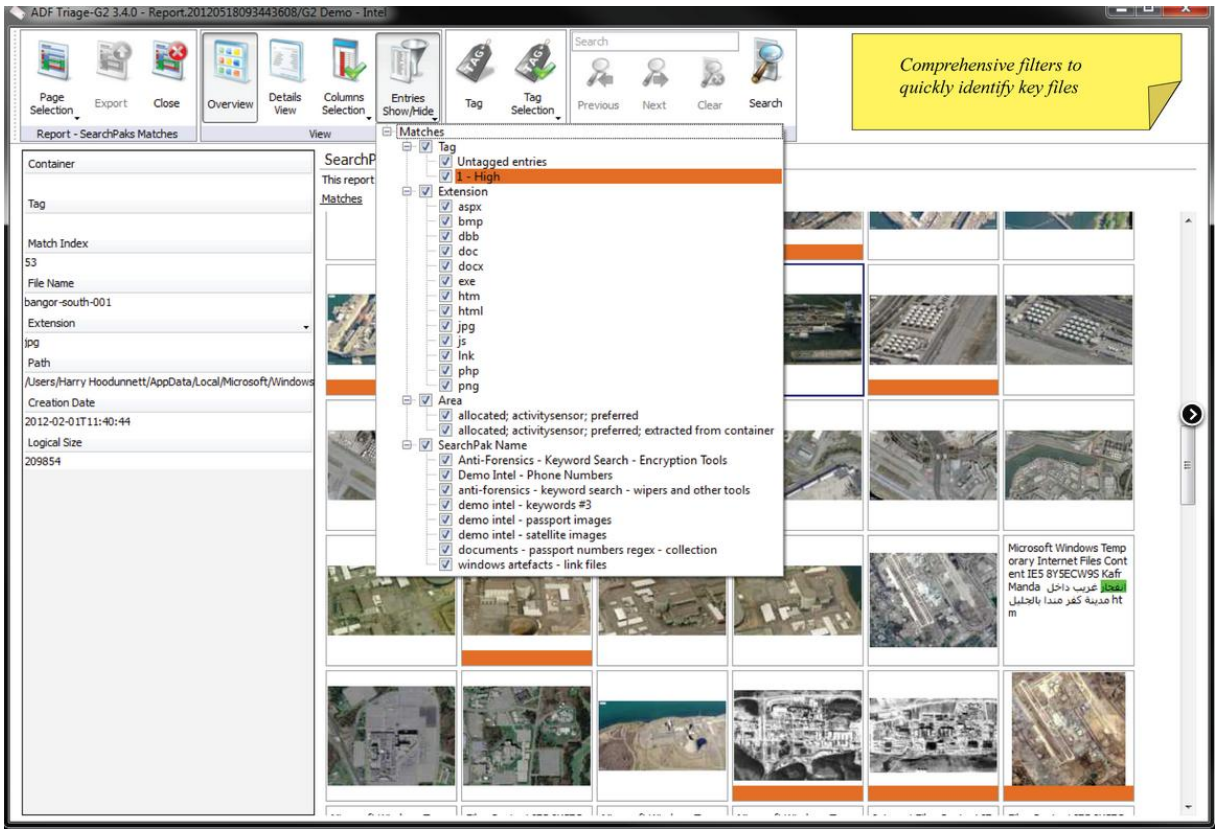
Εικόνα 6.40 : 1ο Βήμα. Επιλογή από προεγκατεστημένα προφίλ αναζήτησης που θα φορτωθούν στο USBkey.

Και η δεύτερη η επιλογή του USBkeyπου θα προετοιμαστεί για τη χρήση σύμφωνα με το προεπιλεγμένο προφίλ.



Εικόνα 6.40 : 2ο Βήμα. Επιλογή σε ποιο από τα διαθέσιμα USBkeys θα φορτωθούν τα προεγκατεστημένα προφίλ αναζήτησης της εικόνας 6.39

Με την εισαγωγή του USBkeyστον υπό εξέταση υπολογιστή ο χρήστης μπορεί είτε να δει επιτόπου τα αρχεία τα οποία καθορίστηκαν ως σημαντικά από το προφίλ που επιλέχτηκε αρχικά,είτε μπορεί να τα συλλέξει για λεπτομερέστερη ανάλυση στο εργαστήριο.

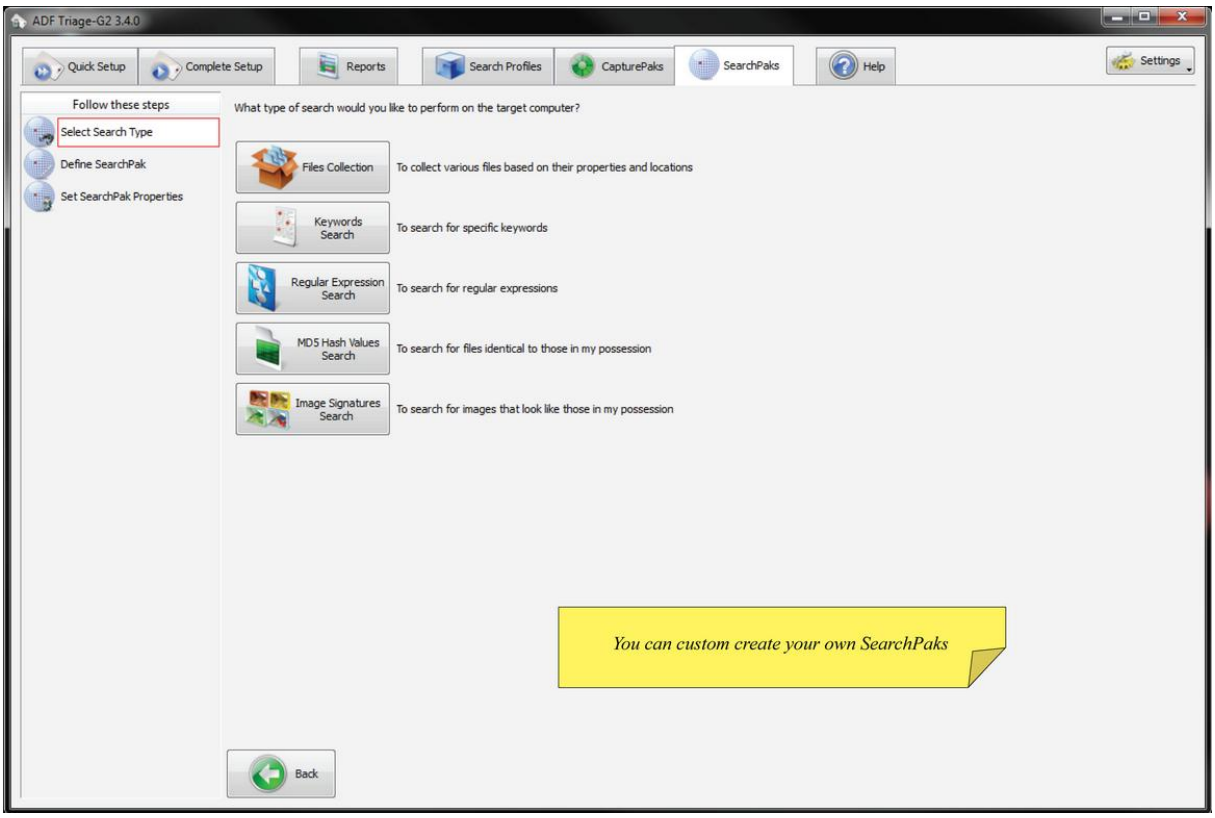


Εικόνα 6.41 : Άμεση εμφάνιση των αναζητήσεων που φορτώθηκαν στον υπολογιστή προς έρευνα. Αν υπάρχει ο χρόνος φορτώνονται και στο USBkeyγια ανάλυση στη βάση.

Η προεπιλογή των κριτηρίων αναζήτησης αρχείων μπορεί πολύ εύκολα να διαμορφωθεί από τον ερευνητή σύμφωνα με το τι πληροφορίες επιθυμεί να λάβει από τον προς εξέταση υπολογιστή. Η διαδικασία είναι τέτοια που δεν απαιτείται κάποια εξειδίκευση, απλά γνώση για το τι ακριβώς πρέπει να αναζητηθεί. Το είδος του λειτουργικού που θα έχει ο υπολογιστής δεν έχει σημασία καθώς με το ίδιο USBkeyμπορεί να γίνει η συλλογή των πληροφοριών από τα τρία γνωστότερα λειτουργικά συστήματα, Windows, Linuxκαι Macintosh.

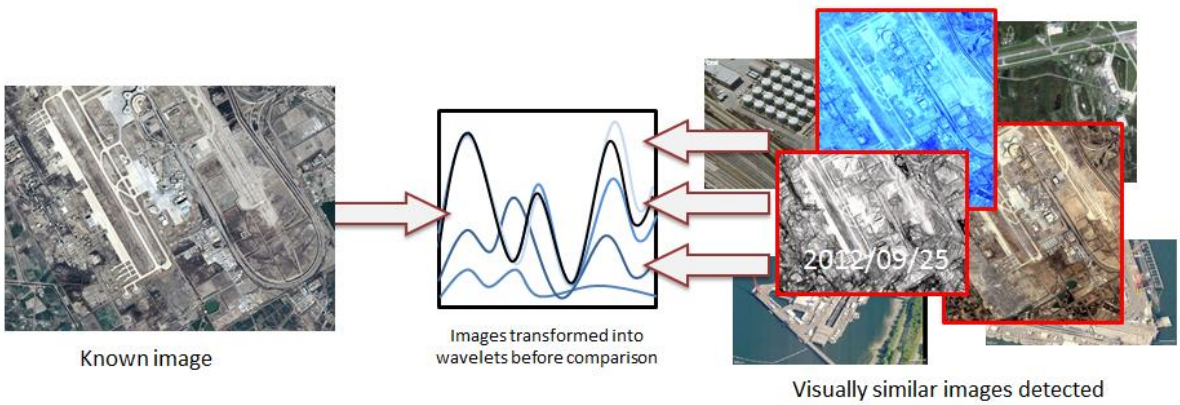
Υπάρχουν γι αυτό το σκοπό πολλά προρυθμισμένα πακέτα αναζήτησης τα οποία μπορεί ο ερευνητής να τα επιλέξει για κέρδος χρόνου, όπως για λήψη συζητήσεων από Chatδιαφόρων υπηρεσιών, αρχείων από εφαρμογές γραφείου, ηλεκτρονικό ταχυδρομείο, επαφές και φωτογραφίες.

Μπορεί επίσης να συλλέξει δεδομένα από την ιστορία όλων των γνωστών φυλλομετρητών καθώς επίσης και τους όρους αναζήτησης που έκανε ο χρήστης στις μηχανές αναζήτησης. Επιπλέον επιτρέπει τη συλλογή όλων χαρτών κατευθύνσεων που αναζητήθηκαν στο GoogleMapsσε συστήματα Windows.



Εικόνα 6.42 :Διαμόρφωση των κριτηρίων αναζήτησης που θα φορτωθούν στο USBkeyόταν τα προεγκατεστημένα δεν είναι ικανοποιητικά για την αποστολή.

Κατά τη διάρκεια της ανάλυσης των συλλεχθέντων αρχείων το εργαλείο παρέχει στον ερευνητή τη δυνατότητα να διαμορφώσει την επιλογή των αρχείων βάσει των επικεφαλίδων τους για κέρδος χρόνου και για σίγουρα σωστή διαλογή. Επίσης έχει αυξημένες δυνατότητες σύγκρισης - ταυτοποίησης εικόνας οι οποίες ξεφεύγουν από τη συνηθισμένη ανάλυση με τη συνάρτηση κατακερματισμού(MD5, SHA1) και επιτρέπουν το γρήγορο εντοπισμό παρόμοιων εικόνων, ακόμα και διαγραμμένες, οι οποίες μπορούν να προσφέρουν πολύ σημαντικές πληροφορίες σε περίοδο επιχειρήσεων.



Εικόνα 6.42 :Σύγκριση εικόνων που λήφθηκαν, με υπάρχουσες με τη μέθοδο της κυματοποίησης για εντοπισμό αυτών που ενδιαφέρουν τον ερευνητή.

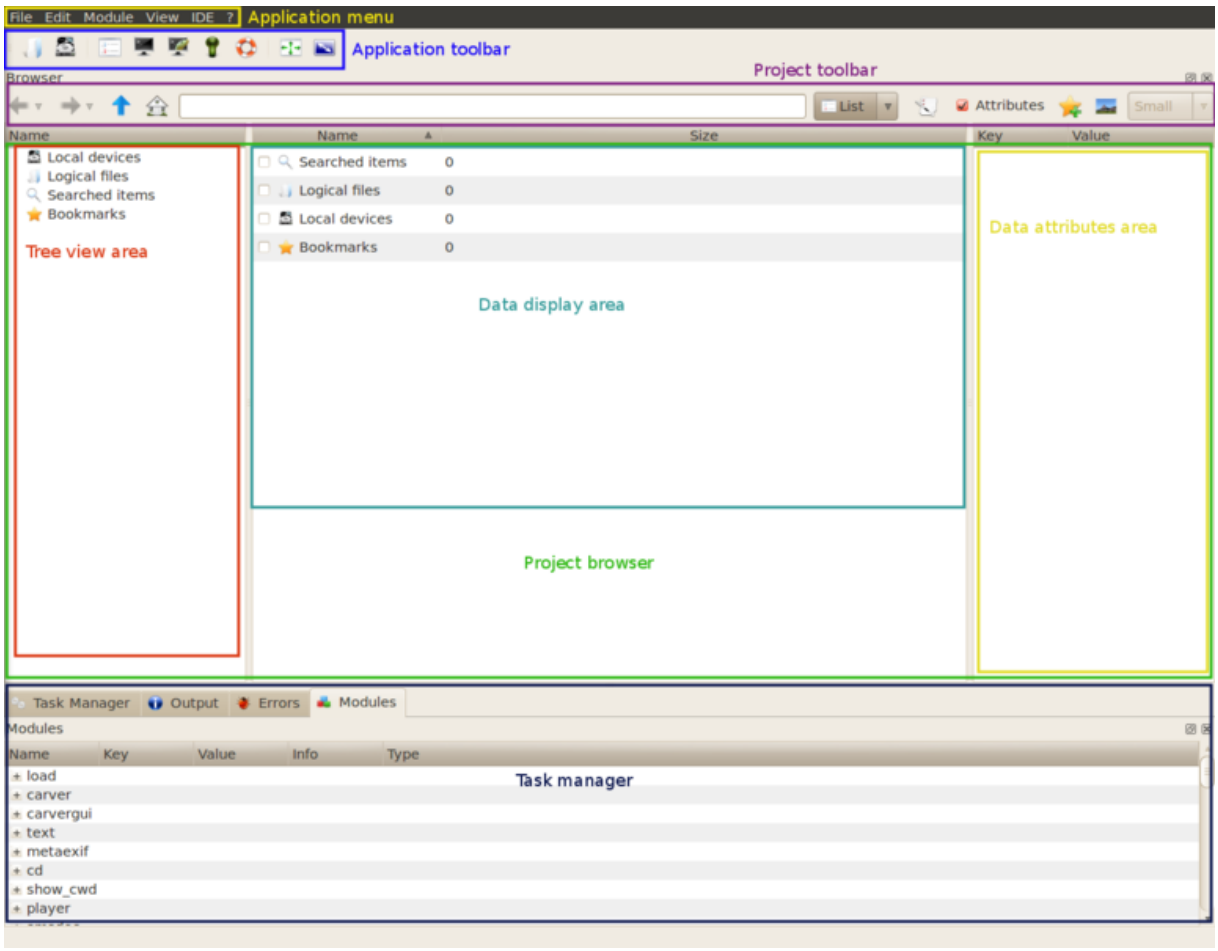
6.5 Εργαλεία Ανοικτού Κώδικα

Τα εργαλεία ανοικτού κώδικα είναι εργαλεία τα οποία έχουν τη δυνατότητα να προσφέρουν συγκεκριμένες εργασίες ψηφιακής δικανικής, εστιάζοντας το κάθε ένα ξεχωριστά σε μια από τις 4 φάσεις. Το κοινό τους χαρακτηριστικό είναι ότι ο κώδικάς τους είναι ανοικτός και μπορεί όποιος επιθυμεί να μελετήσει ακριβώς τη διαδικασία που ακολουθούν και να εντοπίσει πιθανά τρωτά τους σημεία [08]. Το συγκεκριμένο χαρακτηριστικό μπορεί να θεωρηθεί ως πλεονέκτημα σε σχέση με τα εμπορικά κλειστού κώδικα τα οποία όμως υπερτερούν σε άλλες κατηγορίες, όπως η παροχή εκπαίδευσης και πιστοποίησης τα οποία εκτιμούνται υπέρ του δέοντος στις δικαστικές αίθουσες, παρά το ότι το παραγόμενο αποτέλεσμα ακολουθώντας την ίδια δικανική διαδικασία μπορεί να είναι ακριβώς το ίδιο. Γενικά το αν θα γίνει αποδεκτό ή όχι στο δικαστήριο ένα ψηφιακό πειστήριο εξαρτάται άμεσα από το πόσο αποδεκτός είναι ο ερευνητής που το παρουσιάζει από τους αντίδικους και από το πόσο αποδεκτά είναι στο χώρο η διαδικασία και τα εργαλεία που χρησιμοποίησε για τη συλλογή και ανάλυση του.

Θα επιχειρηθεί να γίνει μια σύντομη παρουσίασή κάποιων εξ αυτών παρακάτω :

1. Digital Forensics Framework

   Είναι μια συλλογή εργαλείων η οποία μπορεί να αναλάβει από την αρχή μέχρι το τέλος μια δικανική έρευνα. Έχει την ικανότητα να διατηρήσει την απαιτούμενη αλυσίδα φύλαξης των πειστηρίων με το ενσωματωμένο λογισμικό writeblocker και μπορεί να συλλέξει αρχεία από όλων των ειδών ψηφιακά μέσα αποθήκευσης και από την πτητική μνήμη από λειτουργικά περιβάλλοντα Windowsκαι Linux. Έχει γραφικό περιβάλλον, αλλά και γραμμή εντολών αλλά δεν μπορεί να θεωρηθεί πολύ εύκολο στη χρήση. Παρέχει οδηγό χρήσης στο διαδίκτυο και επιτρέπει τη συλλογή, διαλογή και ανάκτηση των δεδομένων όπως και τα προηγούμενα εμπορικά εργαλεία που παρουσιάστηκαν [36].



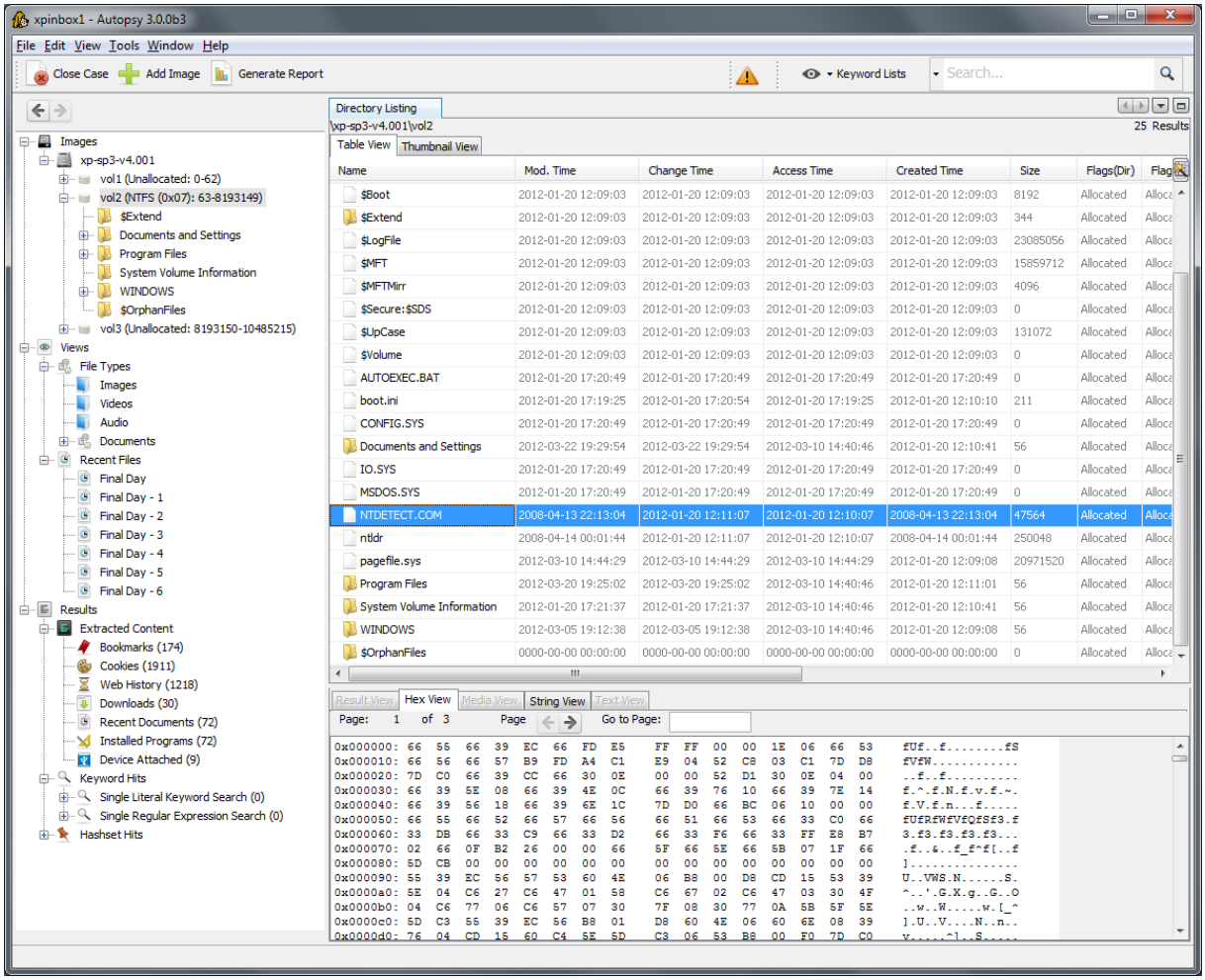
Εικόνα 6.43 : Κεντρικό παράθυρο του εργαλείου ανοικτού κώδικα DFF.

2. Autopsy - SleuthKit

Είναι ένα γραφικό εργαλείο το οποίο μαζί με το SleuthKit, το οποίο είναι μια βιβλιοθήκη εργαλείων σε γραμμή εντολών, επιτρέπουν την ανάλυση αντιγράφων δίσκων σε βάθος. Έχει τη δυνατότητα να κάνει χρονολογική ανάλυση για σκοπούς ανάλυσης δραστηριότητας του υπολογιστή, να πραγματοποιεί έρευνα με λέξεις κλειδιά, να ερευνά τη Διαδικτυακή δραστηριότητα του χρήστη, έλεγχο ηλεκτρονικής αλληλογραφίας, να διαχωρίζει γνωστού τύπου αρχεία από αγνώστου ή από γνωστού κακόβουλου και μπορεί να παράγει αναφορά σε HTML,ή XLS [34].

Οι δυνατότητές του σε ανάλυση δεν περιορίζονται μόνο σε απενεργοποιημένες συσκευές αλλά μπορεί να αναλύσει και ενεργοποιημένες με τη χρήση cd. Επίσης έχει τη δυνατότητα να οργανώνει την έρευνα σε υποθέσεις οι οποίες να περιέχουν περισσότερα από ένα ύποπτα συστήματα και σε όλη τη διάρκεια της έρευνας να διατηρεί και να

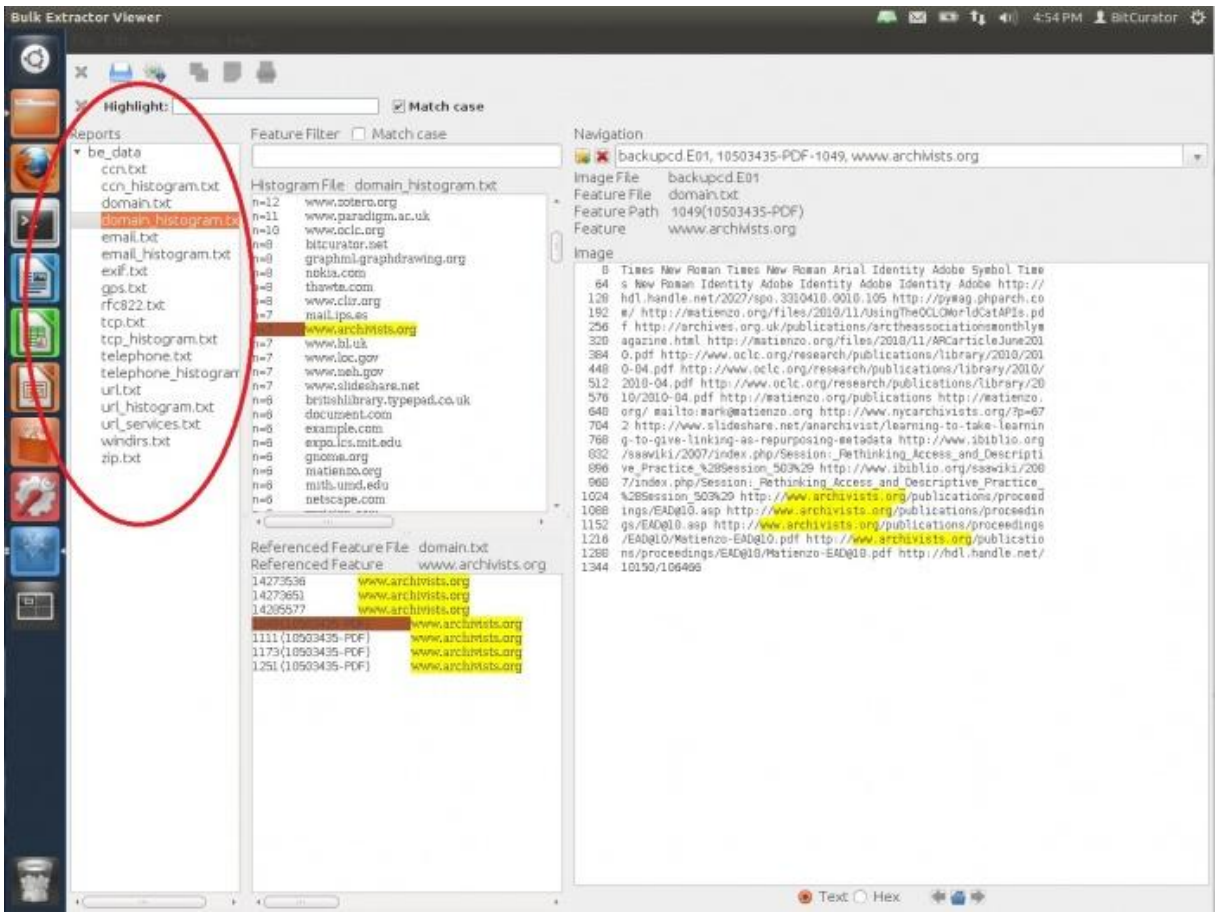
μπορεί να αποδείξει την ακεραιότητα των πειστηρίων με την εξαγωγή των hashvaluetων αρχείων που έχει ερευνήσει.



Εικόνα 6.44 : Ανάλυση μέσου αποθήκευσης με το εργαλείο ανοικτού κώδικα Autopsy.

3. Bulk Extractor

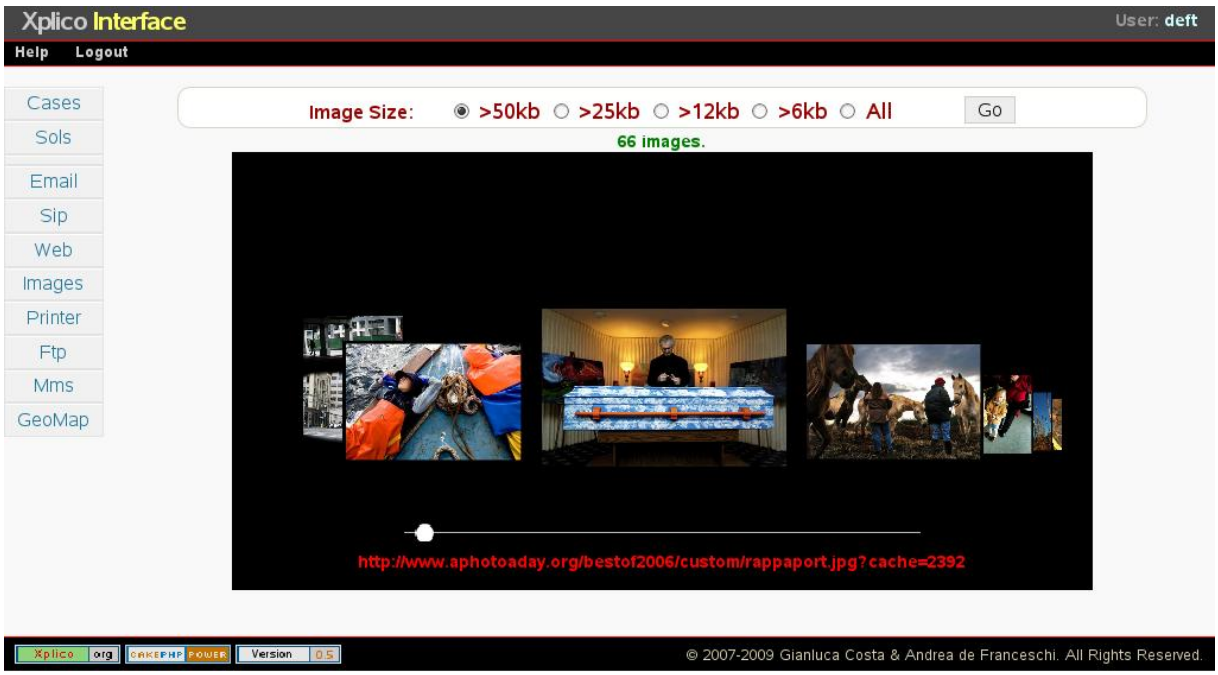
Είναι ένα εργαλείο ψηφιακής δικανικής το οποίο ερευνά ένα αντίγραφο δίσκου, ή ένα αρχείο και εξάγει πληροφορίες όπως αριθμούς πιστωτικών καρτών, διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις ιστοσελίδων και αρχεία zip. Όλα τα στοιχεία τα τοποθετεί σε αρχεία κειμένου txtγια να μπορούν να διαβαστούν ή να αναλυθούν με τη χρήση άλλων εργαλείων ψηφιακής δικανικής [37].



Εικόνα 6.45 : Παρουσίαση αποτελεσμάτων με αυτόματη δημιουργία αναφοράς από το εργαλείο ανοικτού κώδικα BulkExtractor.

4. Xplico

Είναι ένα εργαλείο το οποίο επικεντρώνεται στην κατηγορία της δικανικής δικτύων και επιτρέπει στον ερευνητή να συλλέξει στοιχεία από όλη τη διακίνηση δεδομένων που γίνεται στο εσωτερικό δίκτυο αλλά και από προς και από το Διαδίκτυο. Υποστηρίζει πολλαπλά πρωτόκολλα ηλεκτρονικού ταχυδρομείου, HTTP, TCP, UDP, IMAPκαι μπορεί να εξάγει όλα τα δεδομένα σε βάση δεδομένων MySQLή SQLite [35].Με τη χρήση του είναι δυνατή η συνεχής και συγκαλυμμένη παρακολούθηση ενός εσωτερικού δικτύου (LAN), είτε μεμονωμένων χρηστών με τη μέθοδο του arppoisoning. Έχει δοκιμαστεί πρακτικά σε δίκτυο με περισσότερους από 20 χρήστες ταυτόχρονα χωρίς να προκαλεί σοβαρά προβλήματα, ή καθυστερήσεις στη διακίνηση των δεδομένων που να προκαλέσουν υποψίες σε κάποιον που δεν γνώριζε την ύπαρξή του.



Εικόνα 6.46 : Συλλογή εικόνων που έχουν διακινηθεί μέσα από το εσωτερικό δίκτυο που ελέγχεται από το εργαλείο ανοικτού κώδικα xplico.

6.6. Συγκριτικός Πίνακας Χαρακτηριστικών Εργαλείων Ψηφιακής Δικανικής

Χαρακτηριστικό	**FTK**	**EnCase**	**X-Ways**	**ADF**
Απαιτήσεις Συστήματος	υψηλές	κανονικές	χαμηλές	χαμηλές
Επιπλέον Απαιτήσεις	Β.Δ.	---	---	---
Εκπαίδευση - Υποστήριξη				
Εκπαίδευση σε τάξη	✓	✓	✓	✓
Δικτυακή Εκπαίδευση	✓	✓	×	×
Αυτόνομη Διδασκαλία	✓	✓	✓	×
Φόρουμ	✓	✓	✓	×
Τηλεφωνική Υποστήριξη	✓	✓	×	×
Υποστήριξη με Ηλ. Ταχ.	✓	✓	✓	✓
Υποστήριξη Συστημάτων Αρχείων				
FAT 12/16/32	✓	✓	✓	✓
NTFS	✓	✓	✓	✓
Ext 2	✓	✓	✓	✓
Ext 3	✓	✓	✓	✓
Solaris	✓	✓	✓	×
BSD FFS	✓	×	×	×
JFS	✓	✓	×	×
LV2M	✓	✓	✓	×
CD/DVD	✓	✓	✓	×
RAIDS	✓	×	✓	×

Χαρακτηριστικό	**FTK**	**EnCase**	**X-Ways**	**ADF**
Αναζήτηση – Ανάλυση Αρχείων				
Χρήση Λογικών εκφράσεων	✓	✓	✓	✓
Χρήση Φίλτρων	✓	✓	✓	✓
Εντοπισμός Κακόβουλου Λογισμικού	✓	✓	×	×
Εντοπισμός Κειμένου	✓	✓	×	×
Αναζήτηση Πτητικής Μνήμης	✓	✓	✓	✓
Αναζήτηση σε Προστατευμένα Αρχεία	✓	✓	✓	×
Ηλεκτρονική Αλληλογραφία	✓	✓	✓	✓
Αναπαραγωγή Νήματος Ηλεκτρονικής Αλληλογραφίας	✓	✓	×	×
Εντοπισμός Πορνογραφικού Περιεχομένου σε Εικόνες	✓	✓	×	×
Χρονική Κατανομή Γεγονότων	✓	✓	✓	×
Αυτόματος Εντοπισμός Κρυπτογραφημένων Αρχείων	✓	✓	✓	×
Εντοπισμός HPA και DCO	✓	✓	✓	×
Δικανική Ανάλυση				
Φυλλομέτρηση Φυσικού Δίσκου και Ακριβούς Αντίγραφου	✓	✓	✓	✓
Φυλλομέτρηση μη Κατανεμημένου Χώρου στον Δίσκο	✓	✓	✓	×
Αποκάλυψη Σειριακού Αριθμού Δίσκου	✓	✓	×	×
Ανάκτηση Διαγραμμένων Αρχείων	✓	✓	✓	✓
Κατάταξη Αρχείων Βάσει Υπογραφής	✓	✓	✓	✓
Υπολογισμός της συνάρτησης κατακερματισμού – Σύγκριση	✓	✓	✓	✓
Εντοπισμός Λανθασμένων Επεκτάσεων Αρχείων	✓	✓	✓	✓
Ανάλυση Πτητικής Μνήμης	✓	✓	✓	✓
Ανάλυση Κινητών Συσκευών	✓	✓	✓	×
Μεμακρυσμένη Λήψη – Ανάλυση	✓	✓	×	×
Αποκρυπτογράφηση	✓	✓	×	×
Συσχετίσεις Επικοινωνίας	✓	✓	×	×
Προστασία Εγγραφής(Write Blocker)	✓	✓	✓	✓
Ανάλυση Φυλλομετρητών				
Ολοκληρωμένη Ανάλυση Όλων των Φυλλομετρητών	✓	×	×	×
Χρονική Ανάλυση Δραστηριότητας Υπόπτου στους Φυλλομετρητές	✓	✓	✓	✓
Συλλογή Δεδομένων Αναζήτησης και Δραστηριότητας	✓	✓	✓	✓
Εξαγωγή – παρουσίαση				
Αναφορά XML	✓	✓	×	×
Αναφορά HTML	✓	✓	✓	✓

Χαρακτηριστικό	FTK	EnCase	X-Ways	ADF
Αναφορά CSV	✓	✓	×	✓
Αναφορά MS Word	×	×	×	✓
Αναφορά text file	✓	✓	×	×
Εξαγωγή Αρχείων και Φακέλων	✓	✓	✓	✓

Πίνακας 6.1. : Ο εν λόγω πίνακας έχει ως βάση πίνακα της εταιρείας paraben[39],αλλά είναι προσαρμοσμένος κατάλληλα για τις ανάγκες της παρούσας μεταπτυχιακής διατριβής.

Κεφάλαιο 7
Προβλήματα – Δυσχέρειες

7.1. Τεχνικά θέματα

7.1.1. Κρυπτογράφηση

Κρυπτογραφημένα αρχεία ή ολόκληρα αποθηκευτικά μέσα είναι σχεδόν αδύνατο για τους ερευνητές να τα δουν χωρίς να έχουν το κλειδί, ή τον κωδικό. Τα σύγχρονα λειτουργικά συστήματα προσφέρουν τη δυνατότητα στους ιδιοκτήτες τους να κρυπτογραφήσουν ολόκληρο το σύστημα από την αρχή περιορίζοντας τη δυνατότητα των ερευνητών για έλεγχο ακόμα και στα βασικά αρχεία μιας συσκευής. Πολλά προγράμματα επίσης προσφέρουν τη δυνατότητα ισχυρής κρυπτογράφησης αρχείων ή και ολόκληρων αποθηκευτικών μέσων με ελάχιστο ή και με μηδαμινό κόστος. Επίσης η κρυπτογράφηση δεν περιορίζεται μόνο στα αρχεία των υπολογιστών αλλά επεκτείνεται και στην επικοινωνία, είτε αυτή είναι μέσω ηλεκτρονικού ταχυδρομείου ή chat, είτε είναι μέσω τηλεφωνικής επικοινωνίας μέσω διαδικτύου [46].

Οι ερευνητές σε περίπτωση που συναντήσουν κρυπτογραφημένα αρχεία θα πρέπει να ζητήσουν αρχικά τη συνεργασία του διαχειριστή του συστήματος, η οποία όμως δεν πρέπει να θεωρείται δεδομένη ακόμα και αν δεν είναι ο ίδιος ο ύποπτος που ελέγχεται. Σε περίπτωση που συναντήσουν άρνηση για συνεργασία τότε θα πρέπει να αναζητήσουν τρόπους αποκρυπτογράφησης. Προγράμματα αποκρυπτογράφησης προσφέρονται μαζί με πολλά από τα εργαλεία δικανικής που υπάρχουν, αλλά υπάρχουν και αυτόνομα. Η αποκρυπτογράφηση ενός αρχείου μπορεί να είναι πάρα πολύ χρονοβόρα ακόμα και σε ένα πολύ εξειδικευμένο εργαστήριο άσχετα με το πρόγραμμα κρυπτογράφησης που χρησιμοποιήθηκε. Οι τεχνικές που παρέχονται στον ερευνητή από τα προγράμματα είναι πολλές και η συνήθης τακτική είναι η δημιουργία αντιγράφων του κρυπτογραφημένου αρχείου και η χρήση πολλών τεχνικών ταυτόχρονα σε διαφορετικά συστήματα για κέρδος χρόνου.

Την ίδια ώρα ο ερευνητής με τη χρήση των εργαλείων του αναλύει τον αδιάθετο χώρο των μέσων αποθήκευσης και τα πρόσθετα δεδομένα σε κάθε αρχείο με σκοπό τον εντοπισμό στοιχείων που θα βοηθήσουν στην αποκάλυψη του ή και σε αυτούσιο τον κωδικό. Αν είχε καταφέρει να πάρει και ακριβές αντίγραφο της πτητικής μνήμης του υπολογιστή θα τον αναζητήσει και εκεί [02].

Από αυτό το πρόβλημα αναδεικνύεται και η σημασία της λήψης των αντιγράφων της συσκευής όταν είναι ενεργοποιημένη, όπου υπάρχει μεγάλη πιθανότητα τα αρχεία αυτά να είναι ανοιχτά από τον χρήστη και να ληφθούν στο αντίγραφο μη κρυπτογραφημένα για να γίνει η ανάλυσή τους από τον αναλυτή.

7.1.2. Αύξηση Αποθηκευτικού Χώρου

Κάθε χρόνο ο χώρος των αποθηκευτικών μέσων που είναι διαθέσιμα στην αγορά αυξάνεται συνεχώς, γεγονός που για τον εξεταστή σημαίνει πως οι υπολογιστές που θα χρησιμοποιούν για την ανάλυση θα πρέπει να έχουν επαρκή υπολογιστική δύναμη και διαθέσιμο αποθηκευτικό χώρο για να μπορούν να διαχειριστούν και να αναλύσουν αποτελεσματικά τεράστιους όγκους δεδομένων. Ακόμα μια συνέπεια της αύξησης του όγκου των δεδομένων είναι ότι το έργο των ερευνητών να γίνεται όλο και πιο χρονοβόρο. Δεν είναι μόνο ο χρόνος που απαιτείται για να ληφθεί η εικόνα ενός μέσου, αλλά και ο χρόνος για να γίνει η ανάλυσή του. Στην πραγματικότητα όσο καλό και να είναι το εργαλείο, η ανθρώπινη εφυία εξακολουθεί να είναι απαραίτητη [02], τα εργαλεία απλά μειώνουν την άσκοπη εργασία του ερευνητή για να μπορεί να συγκεντρωθεί σε ουσιώδη θέματα που αφορούν την υπόθεση [06,46].

7.1.3. Νέες Τεχνολογίες

Η τεχνολογία της πληροφορικής εξελίσσεται ραγδαία, νέες μηχανές, νέα προγράμματα και λειτουργικά εμφανίζονται συνεχώς με αποτέλεσμα κανένας ερευνητής να μην μπορεί να είναι ειδικευμένος σε όλους τους τομείς, παρόλο που αναμένεται από αυτούς να αναλύσουν κάτι που δεν έχουν ξαναδεί προηγουμένως. Για να καταφέρει ένας ερευνητής να το αντιμετωπίσει πρέπει να είναι προετοιμασμένος και να μπορεί να δοκιμάσει και να πειραματιστεί με τη συμπεριφορά νέων τεχνολογιών.

Τα σύγχρονα εργαλεία τα τελευταία χρόνια άρχισαν να έχουν τη δυνατότητα να ερευνούν συσκευές πέραν των υπολογιστών και των εξυπηρετητών, όπως έξυπνα τηλέφωνα και ταμπλέτες οι οποίες είναι πολύ εύχρηστες και έχουν πλέον τις ίδιες δυνατότητες με τους υπολογιστές για τη διενέργεια ενός εγκλήματος. Αυτό είναι μια μεγάλη πρόκληση για τους ερευνητές καθώς δεν είναι σίγουροι για την ικανότητα των εργαλείων τους με τις συγκεκριμένες συσκευές επειδή δεν έχουν δοκιμαστεί πλήρως και επειδή και ο κώδικάς των εργαλείων δεν είναι ανοικτός είναι σχεδόν αδύνατο να εντοπίσουν τυχόν προβλήματα γι αυτό και η αμφισβήτηση μεγαλώνει [06].

7.1.4. Αντίμετρα Δικανικής

Είναι η διαδικασία παρεμπόδισης της ψηφιακής ανάλυσης ενός υπολογιστή. Αυτή μπορεί να περιλαμβάνει κρυπτογράφηση, εγγραφή μεγάλων αρχείων για να μην μπορούν να ανακτηθούν τα διαγραμμένα, αλλαγή των metadata αρχείων με σκοπό τη «μεταμφίεση» των αρχείων. Ακόμα και χρήση AlternativeDataStreams (ADS) όπου ένας ύποπτος που κατέχει τη συγκεκριμένη γνώση μπορεί να κρύψει κάτι πολύ αποτελεσματικά. Για τη χρήση αυτών των μεθόδων παλαιότερα ήταν αναγκαία η πολύ καλή γνώση υπολογιστών και συγκεκριμένα η καλή χρήση της γραμμής εντολών των λειτουργικών συστημάτων. Τώρα έχουν εμφανιστεί και προγράμματα με εύκολο σχετικά γραφικό περιβάλλον που μπορούν να αλλάξουν και τη μορφή ακόμα και βίντεο και να το κρύψουν σε αρχεία του λειτουργικού που ούτε τα λογισμικά ασφαλείας δεν ελέγχουν [46].

7.1.5. Κόστος Εργαλείων

Τα εξειδικευμένα εργαλεία που χρησιμοποιεί ένας ερευνητής θεωρούνται πολύ ακριβά από τις διοικήσεις των οργανισμών και σαν αποτέλεσμα επιλέγουν πολύ απλά στο να μην επενδύσουν

οποιοδήποτε ποσό για τη ψηφιακή δικανική και γενικά για την ασφάλεια των πληροφοριακών συστημάτων. Αυτή η νοοτροπία αυξάνει τα περιστατικά κυβερνοεγκλήματος επειδή αφήνει τους οργανισμούς απροετοίμαστους για να αντιμετωπίσουν οποιοδήποτε περιστατικό ασφαλείας έχει να κάνει με τα πληροφοριακά συστήματά τους [02]. Παρόλο που υπάρχουν οικονομικότερα ή και δωρεάν ακόμα εργαλεία των οποίων συνδυασμένη χρήση από εξειδικευμένο προσωπικό μπορεί να αποδώσει το ίδιο τελικό αποτέλεσμα που θα έδινε ένα εμπορικό εργαλείο, εντούτοις δεν γίνονται εύκολα αποδεκτά από ένα δικαστήριο τα εξαγόμενα τεκμήρια και υπάρχει και η πιθανότητα λάθους χειρισμού από το προσωπικό η οποία να οδηγήσει και σε απώλεια αυτών.

7.1.6. Έλλειψη Σχετικής Γνώσης

Πέραν αυτών οι εξειδικευμένοι ερευνητές έχουν να αντιμετωπίσουν τη γενική έλλειψη σχετικής γνώσης η οποία μπορεί να υπάρξει εντός των δικαστηρίων με αποτέλεσμα όλη η προσπάθειά του να πηγαίνει άκαρπη λόγω του ότι δεν μπόρεσε να μεταφέρει τα ευρήματά του στους δικαστές και τους δικηγόρους με επαρκή τρόπο. Άρα πέραν από την απαραίτητη γνώση σε λογισμικό και υλιστικό ένας ερευνητής θα πρέπει να έχει και την ικανότητα να παρουσιάζει ξεκάθαρα τα ευρήματά του στο δικαστήριο [02,14].

7.1.7. Εκπαίδευση - Εμπειρία

Σοβαρό πρόβλημα προκύπτει και με την εκπαίδευση των ερευνητών για την οποία οι οργανισμοί που ασχολούνται με την ψηφιακή δικανική αναφέρουν πως για να μπορέσει ένας νέος ερευνητής να διεξάγει μόνος του μια έρευνα θα πρέπει να έχει πλέον της πιστοποίησης και ένα έως δυο χρόνια εκπαίδευση επί τω έργο [06].

7.1.8. Πληθώρα φυλλομετρητών

Η πληθώρα φυλλομετρητών που υπάρχει σήμερα δίνει τη δυνατότητα στον ύποπτο να εκτελεί αναζητήσεις και να δραστηριοποιείται με πολλούς διαφορετικούς ταυτόχρονα. Λόγω του ότι ο κάθε ένας έχει τα δικά του χαρακτηριστικά δεν είναι δυνατόν για τα εργαλεία δικανικής να τους αναλύουν όλους και ταυτόχρονα. Τα περισσότερα εργαλεία περιορίζονται στους πιο διαδεδομένους και η ανάλυση που κάνουν είναι για τον καθένα ξεχωριστά με αποτέλεσμα το χρονικό διάγραμμα Διαδικτυακής αναζήτησης και δραστηριότητας του υπόπτου να πρέπει να

γίνεται από τον ερευνητή καθιστώντας την εργασία πολύπλοκη, χρονοβόρα και επιρρεπή σε λάθη [12].

7.2. Αποφυγή Κοινοποίησης Περιστατικών

Σε πολλούς οργανισμούς περιστατικά δεν αναφέρονται λόγω νομικής ευθύνης. Υπάρχουν νόμοι οι οποίοι καθιστούν υπεύθυνο τον οργανισμό υπεύθυνο για την προστασία των δεδομένων και ο οργανισμός θα πρέπει να αποδείξει πως είχε λάβει όλα τα απαραίτητα λογικά μέτρα για την εξασφάλισή τους από κάποια επίθεση ή διαρροή. Οι Διοικήσεις των οργανισμών φοβούνται για τη δημοσιότητα που μπορεί να λάβει μια τέτοια ανακοίνωση και για την απώλεια μελλοντικών ή υφιστάμενων πελατών εξ' αιτίας της. Επίσης οποιαδήποτε τέτοια αναφορά ενέχει τον κίνδυνο τα δεδομένα της εταιρείας να εκτεθούν στους αστυνομικούς ερευνητές, όπως επίσης να διαταραχθεί το κλίμα και να αναστατωθεί το πρόγραμμα λόγω της διαδικασίας των ερευνών [02].

Κεφάλαιο 8
Επίλογος

Επικρατεί η άποψη ότι με τη χρήση των εξειδικευμένων εργαλείων από εξειδικευμένους ερευνητές μπορούν να εξαχθεί οποιαδήποτε πληροφορία από οποιαδήποτε συσκευή. Όμως όλο και περισσότεροι οργανισμοί έρχονται αντιμέτωποι με δεδομένα τα οποία δεν αναλύονται με τα σημερινά εργαλεία είτε λόγω μη συμβατότητας, κρυπτογράφησης ή απλά λόγω έλλειψης εκπαίδευσης.

8.1 Το μέλλον της Ψηφιακής Δικανικής

Η συνεχής αύξηση των δυνατοτήτων των συσκευών αποθήκευσης δεδομένων, ο πολλαπλασιασμός των διαμορφώσεων των αρχείων και των λειτουργικών συστημάτων, η διαβρωτική κρυπτογράφηση, η χρήση του νέφους (cloud), το κακόβουλο λογισμικό το οποίο πλέον δεν κρύβεται στη μόνιμη μνήμη, αλλά στην πτητική καθώς και οι νομικές προκλήσεις – κωλύματα καθιστούν όλο και πιο δύσκολη, απαιτητική και με αυξητική τάση κατανάλωσης πόρων τη λήψη των ψηφιακών πειστηρίων.

Η παρουσία κινητών συσκευών με πανσπερμία λειτουργικών και με υψηλές δυνατότητες εφάμιλλες ενός καλού ηλεκτρονικού υπολογιστή επιτρέπουν πλέον τη διεξαγωγή εγκλημάτων μέσω αυτών και υποχρεώνουν τους ερευνητές στην κατοχή εργαλείων για την ανάλυσή τους.

Επίσης η αδυναμία μέχρι σήμερα για συλλογή δεδομένων από συσκευές όπως μνήμες γραφικών καρτών, χειριστές RAID, διεπαφές δικτύου και διαχειριστές ισχύος καταδεικνύει πως ο πλήρης έλεγχος είναι σχεδόν αδύνατος ειδικά όταν πρόκειται για περιπτώσεις τύπου κυβερνοπολέμου όπου όλα είναι πιθανά να συμβούν και αφορούν περισσότερο σε χρήση κακόβουλου λογισμικού.

Τα σημερινά εργαλεία είναι σχεδιασμένα για να βρίσκουν συγκεκριμένα αποδεικτικά στοιχεία και όχι για να βοηθούν στην έρευνα και επίσης έχουν δημιουργηθεί για να επιλύουν εγκλήματα εναντίον ανθρώπων όπου τα στοιχεία βρίσκονται σε έναν ηλεκτρονικό υπολογιστή και όχι για να βοηθούν στη διαλεύκανση εγκλημάτων που έγιναν με ηλεκτρονικό υπολογιστή, ή εναντίον ηλεκτρονικού υπολογιστή. Πιο απλά δημιουργήθηκαν για να βρίσκουν στοιχεία των οποίων η κατοχή είναι έγκλημα από μόνη της, όπως η παιδική πορνογραφία. Στην προσπάθειά τους για να μη χάσουν κάποιο πιθανό στοιχείο έχουν θυσιάσει την ταχύτητα η οποία σε πολλές περιπτώσεις μπορεί να είναι πολύ πιο σημαντική από την παρουσίαση ενός μεγαλύτερου αριθμού ενοχοποιητικών στοιχείων.

8.2. Συμπεράσματα

Πολλοί επαγγελματίες του χώρου θεωρούν ότι η καλύτερη λύση για την αντιμετώπιση του πολλαπλασιασμού των μέσων, των λειτουργικών και της διαμόρφωσης αρχείων, είναι η κατοχή ειδικού εργαλείου για το κάθε ένα ξεχωριστά [06]. Στο χώρο του στρατού, όπου η ψηφιακή δικανική δεν αφορά τόσο στην προσαγωγή ενόχων στο δικαστήριο, όσο για αντιμετώπιση συμβάντων έγκαιρα και αποτελεσματικά οι επαγγελματίες προτείνουν και την εξειδίκευση του προσωπικού σε λειτουργικά συστήματα και όχι μόνο στους τρεις κλάδους της ψηφιακής δικανικής.

Η ανάλυσή της πτητικής μνήμης έχει ιδιαίτερη σημασία για περιπτώσεις που αφορούν σε θέματα κυβερνοπολέμου όπου η εστίαση γίνεται κυρίως σε εντοπισμό και ανάλυση κακόβουλου λογισμικού που έχει καταφέρει να παρακάμψει το όποιο λογισμικό ασφαλείας υπάρχει στα δίκτυα και στους υπολογιστές. Όσο η επιτήδευση του κακόβουλου λογισμικού αυξάνεται, ο μόνος τρόπος που μπορεί να εντοπιστεί και αποκατασταθεί η απειλή είναι μόνο μέσω της

ανάλυσης της πτητικής μνήμης. Αυτό δε μπορεί να επιτευχθεί μόνο με μια σύντομη ανασκόπηση των περιεχομένων της, αλλά είναι απαραίτητη η απαρίθμηση και εξαγωγή των κακόβουλων ευρημάτων [09]. Λαμβάνοντας υπόψη το συνεχές αυξανόμενο μέγεθος της πτητικής μνήμης εξαιτίας των αυξανόμενων αναγκών από τις εφαρμογές, η ανάλυση και ο εντοπισμός δεν είναι κάτι που μπορεί να γίνει από έναν ερευνητή σε εύλογο χρονικό διάστημα και κρίνεται απαραίτητη η προσθήκη αυτής της ικανότητας στα εργαλεία δικανικής.

Η διαδικασία της απενεργοποίησης των υπολογιστών αν δεν ληφθεί πρώτα το στιγμιότυπο της πτητικής μνήμης δεν πρέπει να είναι αποδεκτή από τη διαδικασία. Πολύτιμα δεδομένα που θα μπορούσαν να στοιχειοθετήσουν την υπόθεση καταστρέφονται πλήρως. Από τη στιγμή που οι ερευνητές καλούνται να παρέχουν ψηφιακά πειστήρια τα οποία μπορούν να επηρεάσουν άμεσα τα αποτελέσματα μιας έρευνας οφείλουν να τα παρέχουν. Βάσει των παραπάνω η διαδικασία των ερευνητών καθίσταται ολοένα και πιο πολύπλοκη και απαιτεί εργαλεία τα οποία θα έχουν πλούσια χαρακτηριστικά και θα ανταποκρίνονται γρήγορα σε πολύπλοκες εργασίες, ενώ ταυτόχρονα θα είναι εύκολα στη χρήση. Τα σημερινά εργαλεία πρέπει να επανασχεδιαστούν για να διευκολύνουν την έρευνα. Ειδικότερα όταν πρόκειται για εργαλεία πέραν της χρήσης για παρουσίαση στο δικαστήριο, όπως για κυβερνοάμυνα και πληροφορίες όπου η ταχύτητα είναι εξίσου σημαντική με την ακρίβεια.

Βιβλιογραφία

[01] Rogers, M. K., &Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. Computers&Security, 23, 12e16.

[02] Bassett, R., Bass, L., & O'Brien, P. (2006). Computer forensics: an essential ingredient for cyber security. Journal of InformationScienceand Technology,3(1), 22-32.

[03] Pollitt, M. M. An Ad Hoc Review of Digital Forensic Models.

[04] Shosha, A. F., Tobin, L., &Gladyshev, P. (2013). Digital Forensic Reconstruction of A Program Actions.

[05] Agarwal, M. A., Gupta, M. M., Gupta, M. S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), 118.

[06] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. DigitalInvestigation, 7, S64-S73.

[07] Pasquale, L., Yu, Y., Salehie, M., Cavallaro, L., Tun, T. T., &Nuseibeh, B. Requirements-driven adaptive digital forensics.

[08] Brian Carrier, (2003) Open Source Digital Forensics Tools : The Legal Argument

[09] The Importance of Memory Search and Analysis

[10] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. InternationalJournal of ComputerScience&InformationTechnology (IJCSIT), 3(3), 17-31.

[11] Kaur, G., &Nagpal, B. (2012). Malware Analysis & its Application to Digital Forensic. InternationalJournalonComputerScienceandEngineering (IJCSE),4(04), 622-626.

[12] Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity 5. digital investigation, 8, S62.

[13] Lazetik, G. B., &Koshevaliska, O. (2014). Digital Evidence in Criminal Procedures. BalkanSocialScienceReview, 2, PP-63.

[14] Lessing, M., & Von Solms, B. (2008). Live forensic acquisition as alternative to traditional forensic processes.

[15] Guarino, A. Digital Forensics in a Cyber Warfare Context.

[16] Guidelines on digital forensic procedures for OLAF staff

[17] Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden disk areas: HPA and DCO. InternationalJournal of DigitalEvidence, 5(1), 1-8.

[18] Casey, E. (2011). Digital evidence and computer crime: forensic science, computers and the internet. Academicpress.

[19] Ayers, R., Brothers, S., & Jansen, W. (2013). Guidelines on Mobile Device Forensics. NIST SpecialPublication, 800, 101.

[20] Lessard, J., & Kessler, G. C. Android Forensics: Simplifying Cell Phone Examinations.

[21] Owen, P., & Thomas, P. (2011). An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. digital investigation, 8(2), 135-140.

[22] Good Practice Guide for Computer-Based Electronic Evidence (ΕγχειρίδιοΚΑ)

[23] Multinational Cooperation on Modular Cyber Situation Awareness Package for Eu Headquarters, EDA Documentation

[24] Σύνταγμα Κυπριακής Δημοκρατίας

[25] Ο περί της Σύμβασης κατά του Εγκλήματος μέσω του Διαδικτύου (Κυρωτικός)ΝόμοςΝ.22(ΙΙΙ)/2004

[26] Farwell, J. P., &Rohozinski, R. (2011). Stuxnet and the Future of Cyber War.Survival, 53(1), 23-40.

[27] Omar, I., Majid M., (2013, February). Forensics Analysis With FTK. eForensics, 1/2013, 42-54.

[28] Clarke, R. A., &Knake, R. K. (2011). *Cyber war*. HarperCollins.

ΔιαδικτυακοίΣύνδεσμοι

[29] ACCESDATA, «Digital forensics solutions, Forensic Toolkit (FTK)» URL: http://www.accessdata.com/solutions/digital-forensics/ftk

[30] Guidance Software, «Encase Enterprise v7, Product overview» URL: https://www.guidancesoftware.com/products/Pages/encase-enterprise/overview.aspx?cmpid=nav

[31] X-Ways Software Technology AG «X-Ways Forensics: Integrated Computer Forensics Software» URL: http://www.x-ways.net/forensics/index-m.html

[32] Pinpoint Labs, «Computer Forensics, Implement and Manage Enterprise Collections» URL:http://pinpointlabs.com/trialgraphics.html

[33] ADF Solutions « Quickly Discover Actionable Intelligence from Computers and Digital Devices in the Field » URL: http://www.adfsolutions.com/products/triage-g2

[34] Sleuthkit – Autopsy,«Open Source Digital Investigation Tools» URL: http://www.sleuthkit.org/autopsy/desc.php

[35] Xplico,«Open Source Network Forensic Analysis Tool (NFAT)» URL: http://www.xplico.org/

[36] Digital Forensics Framework,«Open Source Digital investigation software» URL: http://www.digital-forensic.org/

[37] BitCurator,«Suite Of Open Source Digital Forensics And Data Analysis Tools» URL: http://wiki.bitcurator.net/index.php?title=Using_Bulk_Extractor_Viewer_to_Find_Potentially_Sensitive_Information_on_a_Disk_Image

[38] Convention on Cybercrime « Convention Committee on Cybercrime (T-CY) website» URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[39] Paraben Corporation «Computer Forensic Tools Comparison Chart» URL: https://www.paraben.com/downloads/p2c-comparison.pdf

[40] SC MAGAZINE, «Product Information, AccessData Tool Suite»URL: http://www.scmagazine.com/accessdata-tool-suite/review/4175/

[41] SC MAGAZINE, «Product Information, ADF Triage-G2» URL:http://www.scmagazine.com/adf-triage-g2-responder-examiner/review/4213/

[42] SC MAGAZINE, «Product Information, EnCase Forensic» URL: http://www.scmagazine.com/encase-forensic/review/4179/

[43] Volatility Labs, «Sampling RAM Across the (EnCase) Enterprise» URL: http://volatility-labs.blogspot.com/2013/10/sampling-ram-across-encase-enterprise.html

[44] eForensics Magazine, «FTK Imager Step By Step» URL: https://eforensicsmag.com/forensic-toolkit-ftk-imager-preorder/

[45] F-Response, «software utility that enables an investigator to conduct live forensics over an IP network» URL: https://www.f-response.com/

[46] Forensic Control, «Introduction to computer forensics» URL: https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

Παράρτημα Α
Αντιστοίχηση Ελληνικών – Αγγλικών Όρων

Αδιάθετος Χώρος	Unallocated Space
Ακριβές Αντίγραφο Δίσκου	Disk Image
Αλυσίδα Φύλαξης	Chain of Custody
Ανάχωμα Ασφαλείας	Firewall
Αποδιοργάνωση	Disruption
Διεπαφή Χρήστη	User Interface
Δικανική Δικτύων	Network Forensics
Δικανική Κινητών Συσκευών	Mobile Forensics
Δικανική Υπολογιστών	Computer Fornesics
Δικαστήριο	Court
Δρομολογητής	Router

Εκμετάλλευση	Exploitation
Ενθυλάκωση	Encapsulation
Επικεφαλίδα	Header
Ηλεκτρονική Αλληλογραφία	Email
Κακόβουλο	Malware
Κυβερνοπόλεμος	Cyber war
Κυβερνοφυσικές Επιθέσεις	Cyber physical Attacks
Κυβερνοχώρος	Cyberspace
Λέξεις-Κλειδιά	Key-Words
Μεταγωγέας	Switch
Μεταδεδομένα	Meta-data
Μορφοποίηση	Format
Νήμα	Thread
Πληροφοριακές Επιχειρήσεις	Information Warfare
Πρόσθετα Δεδομένα	File Slack
Προσπέλαση	Access
Πτητική Μνήμη	Volatile Memory
Σενάρια	Scripts
Συνάρτηση Κατακερματισμού	Hash Value
Συνδεδεμένη Λίστα	Linked List
Τεκμήριο	Evidence
Τρέχουσες Διεργασίες	Process Listings
Φυλλομετρητής	Browser
Ψηφιακή Δικανική	Digital Forensics