ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάπτυξη πλαισίου αυτόματης ψηφιακής ανάλυσης (Windows Forensics Framework), ενός υπολογιστή με εγκατεστημένο το λειτουργικό σύστημα των Windows.** **Development of an automated Forensics Framework, for computers with Windows Operating System.**
Ονοματεπώνυμο Φοιτητή	**ΝΙΚΟΛΑΟΣ ΖΩΑΝΝΟΣ**
Πατρώνυμο	**ΜΙΛΤΙΑΔΗΣ**
Αριθμός Μητρώου	**ΜΠΣΠ 14027**
Επιβλέπων	**ΠΑΤΣΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ, Επίκουρος Καθηγητής**
Συνεπιβλέπων	**ΠΑΠΑΓΕΩΡΓΙΟΥ ΣΠΥΡΙΔΩΝ**

Ημερομηνία Παράδοσης **12 ΙΟΥΛΙΟΥ 2017**

Τριμελής Εξεταστική Επιτροπή

Κωνσταντίνος Πατσάκης Επίκουρος Καθηγητής	Παναγιώτης Κοτζανικολάου Επίκουρος Καθηγητής	Χρήστος Δουληγέρης Καθηγητής

Περίληψη: Το αντικείμενο της συγκεκριμένης μεταπτυχιακής εργασίας, είναι η εξέταση ενός ηλεκτρονικού υπολογιστή (ενεργοποιημένου ή απενεργοποιημένου), με εγκατεστημένο λειτουργικό σύστημα Windows 7 ή 8 ή 10, στον οποίο έχει πραγματοποιηθεί μία διαδικτυακή επίθεση. Κατά την εξέτασή του, συλλέγονται και αναλύονται σημαντικές πληροφορίες, ικανές να στοιχειοθετήσουν την αντικειμενική υπόσταση εκείνων των ποινικών άρθρων που σχετίζονται με τα εγκλήματα που πραγματοποιούνται μέσω του διαδικτύου.

Η μεταπτυχιακή εργασία, ξεκινάει με την περιγραφή της σημαντικότητας μιας εγκληματολογικής έρευνας, ενός ηλεκτρονικού υπολογιστή και συνεχίζει με την επεξήγηση, του τρόπου λειτουργίας του λογισμικού που αναπτύχθηκε προκειμένου τη συλλογή πληροφοριών από το υλικό, το μητρώο του λειτουργικού, τον σκληρό δίσκο, τη μνήμη του συστήματος, τους περιηγητές/φυλλομετρητές και τα τυχόν εξωτερικά μέσα αποθήκευσης, του υπό μελέτη συστήματος.

Εν συνεχεία, περιγράφεται η δυνατότητα του λογισμικού, σχετικά με την ανάλυση των ληφθέντων πληροφοριών, με σκοπό να δοθεί στον αναλυτή μια πληρέστερη εικόνα για τη χρονική στιγμή που πραγματοποιήθηκε η επίθεση, το μέγεθος αυτής και την τυχόν ζημιά που προκλήθηκε, είτε στο σύστημα, είτε στον κάτοχο του συστήματος. Με το πέρας δε αυτής της ανάλυσης, δημιουργείται, αυτόματα (από το λογισμικό), ένας πίνακας, που περιέχει εν συντομία όλες τις παραπάνω πληροφορίες και ο οποίος σε συνδυασμό με τα ληφθέντα αρχεία, θα αποτελεί τα αποδεικτικά στοιχεία της τέλεσης της εν λόγω αξιόποινης πράξης.

Λέξεις-κλειδιά: Εγκληματολογική Έρευνα Windows 7, Εγκληματολογική Έρευνα Windows 8, Εγκληματολογική Έρευνα Windows 10, Συλλογή & Ανάλυση Πληροφοριών Μνήμης, Συλλογή & Ανάλυση Πληροφοριών Σκληρού Δίσκου, Συλλογή & Ανάλυση Πληροφοριών Εξωτερικών Μέσων Αποθήκευσης, Συλλογή & Ανάλυση Πληροφοριών Μητρώου Λειτουργικού.

Περιεχόμενο: Κείμενο, εικόνες, λογισμικό σε γλώσσα προγραμματισμού ActiveX.

Abstract: The subject of this master's thesis is to examine a computer (activated or deactivated) in which has been installed the windows 7 or 8 or 10 and it has been traced, on it, a penetration, using the web. Throughout this examination the information which are been collected and analyzed, are able to constitute the evidence of a trial.

This master's thesis begins by describing the value of windows forensics and continues with the description of the software that has been created in order to collect the necessary information from system's hardware, registry, ram, web browsers, hard disk drives and usb flash disks.

Thereinafter follows the description of the software about the analysis of the information that has been collected. The purpose of this analysis is to give to the analysts farther more information regarding the chronology of events (timeline) and the exent of the damages. At the end of this analysis the software creates a table which contains important information that is able to constitute the evidence of a trial.

Keywords: Forensics, Windows 7 Forensics, Windows 8 Forensics, Windows 10 Forensics, RAM Forensics, HDD Forensics, USB Forensics, Registry Forensics, Timeline.

Content: Text, Images, Code in ActiveX.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1 – ΕΙΣΑΓΩΓΗ

1.1 Αντικείμενο της μεταπτυχιακής εργασίας

Το αντικείμενο της συγκεκριμένης μεταπτυχιακής εργασίας, είναι η δημιουργία ενός κατάλληλου λογισμικού, με το οποίο θα μπορεί, ένας αναλυτής συστημάτων, να συλλέξει πληροφορίες από έναν ηλεκτρονικό υπολογιστή (ενεργοποιημένος ή απενεργοποιημένος), στον οποίο έχει εγκατασταθεί το λειτουργικό σύστημα των Windows 7 ή 8 ή 10.

Οι πληροφορίες που θα συλλέγονται αρχικά, θα αφορούν το υλικό, του υπό μελέτη συστήματος. Δηλαδή, ο σειριακός αριθμός της κεντρικής πλακέτας (motherboard), το μοντέλο αυτής, η ημερομηνία του συστήματος, το όνομα και το είδος του εγκατεστημένου λογισμικού, το όνομα (username), τόσο των χρηστών του συστήματος, όσο και του συνδεδεμένου χρήστη κατά την χρονική στιγμή λήψης των δεδομένων, τα ονόματα των αρχείων που φορτώνονται κατά την εκκίνηση του λειτουργικού (windows startup), τα ονόματα των προγραμμάτων που διαβάζονται κατά την εκκίνηση του υπολογιστή (boot execute, winlogon entries κλπ) αλλά και πληροφορίες σχετικές με την κάρτα δικτύου του συστήματος (ip address, mac address, web provider, firewall κλπ).

Στη συνέχεια, θα συλλέγονται πληροφορίες σχετικά με τους εγκατεστημένους περιηγητές/ φυλλομετρητές του συστήματος (internet explorer, firefox mozilla, google chrome, safari) που αναφέρονται στις φωτογραφίες που φορτώθηκαν από το διαδίκτυο, στο ιστορικό επισκεψιμότητας ιστοσελίδων, αλλά και στις ιστοσελίδες που αποθήκευσε ο χρήστης του συστήματος, ως αγαπημένες. Ταυτόχρονα, σε περίπτωση που ο συνδεδεμένος χρήστης, του υπό μελέτη συστήματος, έχει ρυθμίσει το λογισμικό «outlook» ή «outlook express», που βρίσκεται στο πακέτο προγραμμάτων «Microsoft Office», για τη λήψη και την ανάγνωση των ηλεκτρονικών του μηνυμάτων, τότε, αυτόματα, λαμβάνονται πληροφορίες σχετικά με τα επισυναπτόμενα αρχεία των ηλεκτρονικών του μηνυμάτων (email) και των στοιχείων των συνομιλητών του, στο διαδίκτυο.

Με την ολοκλήρωση των παραπάνω δύο ενεργειών, η συλλογή των πληροφοριών συνεχίζεται λαμβάνοντας ένα πλήρες αντίγραφο των δεδομένων που είναι φορτωμένα στην μνήμη του συστήματος (σε περίπτωση που το υπό μελέτη σύστημα βρεθεί ενεργοποιημένο). Επειδή το σύστημα μπορεί να βρεθεί και απενεργοποιημένο, γι' αυτό επιβάλλεται στον χρήστη του λογισμικού μας, να λάβει αντίγραφο, τόσο του πρωτεύοντος σκληρού δίσκου (δηλαδή του δίσκου στον οποίο έχει γίνει εγκατάσταση το λειτουργικό σύστημα των windows) και στη συνέχεια, να ληφθεί αντίγραφο του μητρώου του λειτουργικού (registry). Λαμβάνοντας το αντίγραφο του δίσκου, μπορεί εν συνεχεία ο αναλυτής να μελετήσει τον εν λόγω ηλεκτρονικό υπολογιστή, χωρίς να διαθέτει φυσική πρόσβαση σ' αυτόν, αλλά φορτώνοντας (mount) εικονικά το ληφθέν αντίγραφο, επί του συστήματός του.

Σε περίπτωση που βρεθεί, στο υπό μελέτη σύστημα και άλλος εγκατεστημένος σκληρός δίσκος, χωρίς όμως λειτουργικό σύστημα (άρα χρησιμεύει μόνο ως αποθηκευτικό μέσο) τότε, συνίσταται η λήψη αντιγράφου και αυτού. Αντίστοιχα, θα πρέπει να ακολουθηθεί η ίδια ακριβώς διαδικασία για να ληφθεί αντίγραφο και όλων των δίσκων/μέσων (external hard disks, usb flash disks) που βρέθηκαν προσαρτημένα/συνδεδεμένα σε θύρα usb, του υπό μελέτη συστήματος.

Η δε λήψη των απαραίτητων πληροφοριών του συστήματος, ολοκληρώνεται με τη συλλογή του χρονοδιαγράμματος ενεργειών (timeline), το οποίο θα παρουσιάσει στον αναλυτή μια χρονική αλυσίδα όλων των πεπραγμένων ενεργειών, επί του συστήματος αυτού.

Μετά τη λήψη όλων των απαραίτητων πληροφοριών, του υπό μελέτη συστήματος, ο αναλυτής έχει τη δυνατότητα να χρησιμοποιήσει το λογισμικό που αναπτύξαμε, με σκοπό την περαιτέρω ανάλυσή τους και την εξαγωγή ασφαλέστερων συμπερασμάτων σχετικά με: (α) την ακριβή χρονική στιγμή που πραγματοποιήθηκε η επίθεση (penetration), (β) τα

εργαλεία/προγράμματα (scripts) που χρησιμοποίησε ο κακόβουλος χρήστης (επιτιθέμενος) για να επιτύχει την επίθεσή του, αλλά και (γ) το μέγεθος της ζημιάς που τυχόν προκλήθηκε, είτε στο ίδιο το σύστημα, είτε στον κάτοχο του συστήματος (ιδιώτης/εταιρεία/δημόσιος οργανισμός).

Τόσο, η συλλογή των πληροφοριών, όσο και η ανάλυσή τους γίνεται κατά κόρον με εντολές κονσόλας (command lines) που μας παρέχει το λειτουργικό σύστημα των windows. Σε ορισμένες δε περιπτώσεις, χρησιμοποιείται και βοηθητικό λογισμικό (κυρίως στη συλλογή και την ανάλυση της registry) καθόσον δεν υποστηρίζονται πλήρως οι ενέργειες αυτές από τις παρεχόμενες εντολές κονσόλας. Οι εντολές που χρησιμοποιήθηκαν, γράφηκαν, είτε εντός κώδικα «java script», είτε δημιουργήθηκαν κατάλληλα «batch files», με σκοπό την χρήση τους από το λογισμικό που αναπτύξαμε. Παρακάτω θα παρουσιάζονται οι χρησιμοποιηθήσες εντολές κονσόλας (command lines) εντός πλαισίου και θα ορίζεται ταυτόχρονα η συμβατότητα της εντολής αυτής, ως προς το λειτουργικό σύστημα, του υπό μελέτη συστήματος (Windows 7 ή/και windows 8 ή/και windows 10). Για την δε ανάπτυξη της δομής αυτού (framework) χρησιμοποιήθηκε το λογισμικό ActiveX.

Όσον αφορά την οργάνωση της εν λόγω μεταπτυχιακής εργασίας, επιλέχθηκε ο εξής τρόπος:

- Κεφάλαιο 1: Εισαγωγή
  Στο κεφάλαιο αυτό, περιγράφουμε το αντικείμενο της μεταπτυχιακής εργασίας και ορίζουμε τα πλεονεκτήματα του λογισμικού που αναπτύξαμε.
- Κεφάλαιο 2: Σημαντικότητα Εγκληματολογικής Έρευνας Ηλεκτρονικών Υπολογιστών
  Αφού καθορίζουμε τους όρους «Εγκληματολογία» και «Ψηφιακή Εγκληματολογία», αναπτύσσουμε τα βασικά βήματα που απαρτίζουν μια εγκληματολογική έρευνα, που σχετίζεται με ένα έγκλημα της Πληροφορικής.
- Κεφάλαιο 3: Συλλογή Πληροφοριών
  Προσδιορίζουμε στο κεφάλαιο αυτό, τις ενέργειες που οφείλει να ακολουθήσει ένας ερευνητής, για την ολοκληρωμένη συλλογή πληροφοριών από έναν ηλεκτρονικό υπολογιστή, που έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης, ανεξάρτητα εάν βρέθηκε ενεργοποιημένος ή απενεργοποιημένος κατά την χρονική στιγμή της κατάσχεσής του.
- Κεφάλαιο 4: Ανάλυση Συλλεχθέντων Πληροφοριών
  Αφού έχει ολοκληρωθεί η συλλογή των απαραίτητων πληροφοριών, προσδιορίζουμε τα βήματα που οφείλουν να ακολουθήσουν οι αναλυτές, προκειμένου την ανάλυση αυτών και την εξαγωγή ασφαλών συμπερασμάτων σχετικά με την τέλεση ή μη μιας αξιόποινης πράξης.
- Κεφάλαιο 5: Συμπλήρωση και Υποβολή Αναφορικής Έκθεσης
  Η διαδικασία ολοκληρώνεται με τη δημιουργία μίας αναφορικής έκθεσης από το λογισμικό που αναπτύξαμε και την οποία πρέπει να ολοκληρώσουν οι ερευνητές με τα συμπεράσματά τους. Η αναφορά αυτή, σε συνδυασμό με τα ληφθέντα αποδεικτικά στοιχεία, θα αποτελέσουν τελικά τα τεκμήρια αθωότητας ή ενοχής του χρήστη του υπό μελέτη συστήματος.
- Κεφάλαιο 6: Εξαγωγή συμπερασμάτων και προτάσεις για περαιτέρω επεκτάσεις.
  Κλείνει η μεταπτυχιακή εργασία, προτείνοντας, τόσο πιθανές βελτιώσεις της, όσο και τυχόν μελλοντικές της επεκτάσεις.

ΚΕΦΑΛΑΙΟ 2 – ΣΗΜΑΝΤΙΚΟΤΗΤΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΕΡΕΥΝΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

2.1 Ορισμός Εγκληματολογίας (Forensic science)

Ως «Εγκληματολογία», ορίζουμε την εφαρμογή της επιστήμης (τόσο στο ποινικό, όσο και στο αστικό δίκαιο) κατά τη διάρκεια μίας ποινικής έρευνας όπως αυτή οφείλει να διέπεται από τις νομικές προδιαγραφές των παραδεκτά αποδεικτικών στοιχείων, αλλά και γενικότερα από την προβλεπόμενη ποινική διαδικασία ([1] Wikipedia - The Free Encyclopedia, 2017)

Ερευνητές και επιστήμονες που ασχολούνται με μία ποινική έρευνα, οφείλουν να συγκεντρώσουν, να διαφυλάξουν και να αναλύσουν τα ανευρεθέντα επιστημονικά στοιχεία με μεθόδους και διαδικασίες που προβλέπονται από τον νόμο, ως «νόμιμα» και «αποδεκτά».

Κατά τη διάρκεια της έρευνας, καλούνται πολλές φορές οι ερευνητές-επιστήμονες να ταξιδέψουν στον τόπο του εγκλήματος, με σκοπό να συλλέξουν οι ίδιοι τις αποδείξεις/ανευρεθέντα τεκμήρια. Άλλοτε όμως, καλούνται να μελετήσουν, να αναλύσουν και να συλλέξουν πληροφορίες/τεκμήρια από στοιχεία/αντικείμενα που προσκομίζουν σε αυτούς, οι διωκτικές αρχές.

Εκτός από τον εργαστηριακό τους ρόλο, αυτοί οι ερευνητές/επιστήμονες μπορούν να καταθέσουν, είτε ως μάρτυρες υπερασπίσεως, είτε και ως μάρτυρες κατηγορίας, ακριβώς λόγω της εξειδίκευσής τους αυτή.

2.2 Ορισμός Ψηφιακής Εγκληματολογίας (Digital Forensics)

Ως «Ψηφιακή Εγκληματολογία» ή ως «Επιστήμη της Ψηφιακής Εγκληματολογίας», ορίζουμε τον κλάδο εκείνο ο οποίος περιλαμβάνει την ανάκτηση και τη διερεύνηση των υλικών, που βρέθηκαν σε ψηφιακές συσκευές και συνήθως σχετίζονται με ένα έγκλημα της πληροφορικής ([2] Wikipedia - The Free Encyclopedia, 2017) .

Ο όρος ψηφιακή εγκληματολογία, χρησιμοποιήθηκε αρχικά ως συνώνυμο της «εγκληματολογίας ηλεκτρονικού υπολογιστή», αλλά έχει επεκταθεί πλέον με σκοπό να μπορεί να καλύψει όλες εκείνες τις συσκευές που μπορούν να αποθηκεύσουν ψηφιακά δεδομένα (κινητά τηλέφωνα, φορητοί ηλεκτρονικοί υπολογιστές, κλπ).

Οι ψηφιακές έρευνες εγκληματολογίας έχουν μια ποικιλία εφαρμογών. Το πιο συνηθισμένο είναι να υποστηρίξουν ή να αντικρούσουν μια υπόθεση ενώπιον των ποινικών ή αστικών δικαστηρίων (ως μέρος της ηλεκτρονικής διαδικασίας ανακάλυψης). Φυσικά, ψηφιακές έρευνες εγκληματολογίας, μπορούν να ασκηθούν και από ιδιωτικές εταιρείες ή ακόμα και από ειδικά τμήματα που διαθέτουν μεγάλες εταιρείες, με σκοπό την έρευνα τυχόν εισβολής κακόβουλων χρηστών (μη εξουσιοδοτημένη διείσδυση στο εσωτερικό του δικτύου μιας εταιρείας).

Η τεχνική πτυχή της ψηφιακής εγκληματολογικής έρευνας, χωρίζεται συνήθως σε διάφορους υπο-κλάδους, που σχετίζονται με το είδος των ψηφιακών συσκευών που εμπλέκονται σε μία αξιόποινη πράξη. Έτσι, υπάρχει η εγκληματολογία ηλεκτρονικών υπολογιστών, η εγκληματολογία δικτύου, η εγκληματολογική ανάλυση δεδομένων και η εγκληματολογία κινητών τηλεφωνικών συσκευών.

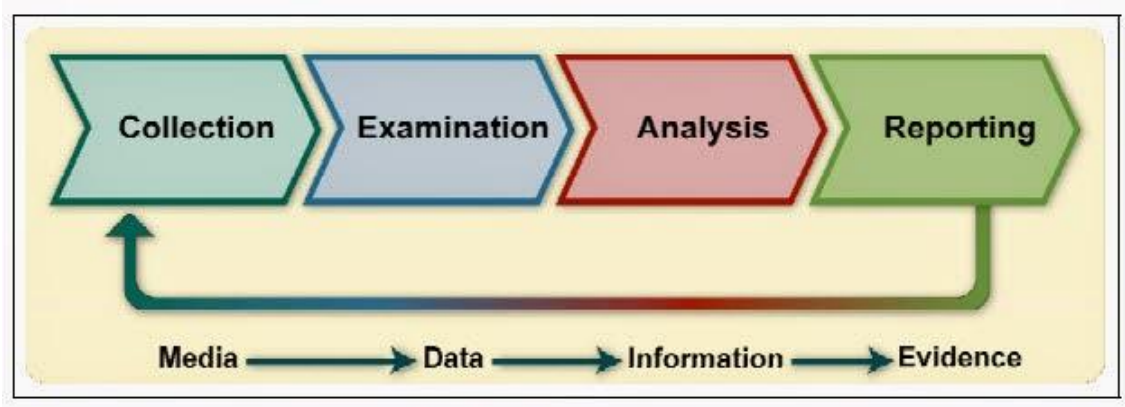
Η συνήθης τυπική ιατροδικαστική διαδικασία, περιλαμβάνει την κατάσχεση, της υπό μελέτη συσκευής, την ιατροδικαστική απεικόνιση (συλλογή απαραίτητων πληροφοριών που αποδεικνύουν την τέλεση αξιόποινης πράξης) και την ανάλυση των ψηφιακών μέσων (πειστηρίων), με σκοπό την σύνταξη/παραγωγή μιας έκθεσης η οποία να αναφέρει: (α) τα στοιχεία των ερευνητών, (β) τα συλλεχθέντα δεδομένα (τεκμήρια), (γ) την ανάλυση αυτών και (δ) την εξιστόρηση των γεγονότων όπως αυτά έχουν καταγραφεί από τα ψηφιακά πειστήρια.

Όπως είναι λοιπόν κατανοητό, η ψηφιακή εγκληματολογία μπορεί να χρησιμοποιηθεί όχι μόνο για τη συλλογή τεκμηρίων που επιβεβαιώνουν την τέλεση μιας αξιόποινης πράξης (που σχετίζεται με την πληροφορική), αλλά μπορεί κιόλας να επιβεβαιώσει το άλλοθι ή την αδυναμία τέλεσης της αξιόποινης πράξης από κάποιον ή κάποιους συγκεκριμένους χρήστες, του υπό μελέτη συστήματος.

2.3 Στάδια Ψηφιακής Εγκληματολογικής Έρευνας

Η ψηφιακή ιατροδικαστική διαδικασία, είναι μια αναγνωρισμένη επιστημονική και ιατροδικαστική διαδικασία που χρησιμοποιείται στις ψηφιακές εγκληματολογικές έρευνες. Ο γνωστός ερευνητής εγκληματολογίας «Eoghan Casey», ορίζει πως η διαδικασία της ψηφιακής εγκληματολογικής έρευνας απαρτίζεται από έναν αριθμό βημάτων ξεκινώντας από την αρχική ειδοποίηση για το συμβάν μη εξουσιοδοτημένης πρόσβασης σε ηλεκτρονικό μέσο, έως και την τελική αναφορά των ευρημάτων ([3] Wikipedia - The Free Encyclopedia, 2016).

Η διαδικασία που θα αναπτύξουμε παρακάτω, χρησιμοποιείται, κατά κύριο λόγο, στην έρευνα μη εξουσιοδοτημένης πρόσβασης σε ηλεκτρονικό υπολογιστή. Τα τρία βασικά στάδια αυτής είναι: (α) η συλλογή πληροφοριών (acquisition), (β) η ανάλυση των συλλεχθέντων δεδομένων (analysis) και (γ) η συμπλήρωση και υποβολή σχετικής αναφορικής έκθεσης (Εικόνα 2.3.1).



Εικόνα 2.3.1: Στάδια Ψηφιακής Εγκληματολογικής Έρευνας

Κατά τα στάδια της διαδικασίας αυτής, απαιτείται πολλές φορές η εμπλοκή ερευνητών/επιστημόνων διαφορετικής εξειδικευμένης κατάρτισης και γνώσης.Γι'αυτό χωρίζουμε το εμπλεκόμενο προσωπικό, σε δύο (2) βασικές κατηγορίες:

1) Τεχνικοί Ψηφιακής Εγκληματολογικής Έρευνας και
2) Εξεταστές Ψηφιακών Αποδεικτικών Στοιχείων

Οι τεχνικοί Ψηφιακής Εγκληματολικής Έρευνας, είναι υπεύθυνοι αρχικά για τη συλλογή των απαραίτητων πληροφοριών, με βάση τον τομέα πάντα της κατάρτισής τους. Είναι επιπλέον υπεύθυνοι για την σωστή διαχείριση της τεχνολογίας (π.χ. για τη διατήρηση των αποδεικτικών στοιχείων). Τα μέσα που χρησιμοποιούν για τη λήψη των απαραίτητων πληροφοριών, πρέπει να είναι άρτια (να μην έχουν μολυνθεί από τυχόν κακόβουλα λογισμικά) και η αρτιότητά τους, επιβαρύνει, τους εν λόγω τεχνικούς. Μπορούν να χρησιμοποιηθούν δε λογισμικά, είτε δωρεάν (freeware), είτε με νόμιμες πληρωτέες άδειες.

Οι δε Εξεταστές Ψηφιακών Αποδεικτικών Στοιχείων, μπορούν να είναι άτομα που, είτε ειδικεύονται σε έναν συγκεκριμένο τομέα των ψηφιακών αποδεικτικών στοιχείων (π.χ. αναλυτές ψηφιακών εικόνων), είτε σε ευρύ επίπεδο (π.χ. αναλυτές ηλεκτρονικών υπολογιστών).

2.3.1 Συλλογή Πληροφοριών

Η διαδικασία ξεκινάει συνήθως, με την κατάσχεση των ψηφιακών μέσων των οποίων απαιτείται η μελέτη για την ανίχνευση τυχόν μη εξουσιοδοτημένης πρόσβασης. Στη νομική ορολογία, τα ψηφιακά μέσα, αυτά που κατασχέθηκαν για την έρευνα, καλούνται συνήθως ως «έκθεμα».

Στο σημείο αυτό, διαχωρίζουμε τον τρόπο με τον οποίο θα λειτουργήσουν οι τεχνικοί της ψηφιακής εγκληματολογικής έρευνας, ανάλογα εάν το έκθεμα έχει βρεθεί ενεργοποιημένο ή εάν έχει βρεθεί απενεργοποιημένο, κατά τη χρονική στιγμή της κατάσχεσης.

Στην περίπτωση που βρεθεί ενεργοποιημένο, τότε είναι υποχρεωτική η δημιουργία ενός ακριβές αντίγραφου του πρωτεύοντος σκληρού του δίσκου (sector level duplicate / forensic duplicate/ imaging). Για τη δημιουργία του ειδώλου αυτού, μπορούν να χρησιμοποιηθούν ειδικές συσκευές ή ειδικά λογισμικά απεικόνισης όπως τα DCFLdd, IXimager, Guymager, TrueBack, FTK Imager ή FDAs κλπ. Επειδή δε πολλές φορές σε έναν ηλεκτρονικό υπολογιστή μπορούν να βρεθούν συνδεδεμένοι και κάποιοι εξωτερικοί σκληροί δίσκοι (external disk drives) ή άλλα μέσα αποθήκευσης (usb flash disks), γι'αυτό επιβάλλεται η δημιουργία ακριβές αντίγραφου και των μέσων αυτών.

Πέρα από τα αντίγραφα (α) του πρωτεύοντος σκληρού δίσκου και (β) των εξωτερικών αποθηκευτικών μέσων, επιβάλλεται η δημιουργία ενός αντίγραφου της μνήμης, καθόσον εμπεριέχει χρήσιμες πληροφορίες, οι οποίες θα χαθούν με την απενεργοποίηση του συστήματος. Παράλληλα, απαιτείται η λήψη ενός αντίγραφου του μητρώου του λειτουργικού συστήματος (windows registry), καθόσον εμπεριέχει πληροφορίες σχετικές με το προφίλ και τις ρυθμίσεις του συνδεδεμένου χρήστη, οι οποίες θα χαθούν και αυτές με την απενεργοποίηση του συστήματος.

Η τελευταία πληροφορία που πρέπει να ληφθεί από το ενεργοποιημένο σύστημα, είναι η χρονοαλυσίδα των πεπραγμένων γεγονότων/ενεργειών (timeline), διότι μπορεί να μας παρουσιάσει την αλληλουχία των κινήσεων του κακόβουλου λογισμικού ή του κακόβουλου χρήστη. Εν συνεχεία, το έκθεμα, κατάσχεται και φυλάσσεται με σκοπό την προστασία του από τυχόν αθέμιτη/μη εξουσιοδοτημένη πρόσβαση, σε αυτό.

Εάν το έκθεμα βρεθεί απενεργοποιημένο κατά την χρονική στιγμή της κατάσχεσής του, τότε είναι υποχρεωτική η δημιουργία ενός ακριβές αντίγραφου, του πρωτεύοντος σκληρού του δίσκου (sector level duplicate / forensic duplicate/ imaging) ή τυχόν άλλων εξωτερικών σκληρών δίσκων (external disk drives) ή άλλων μέσων αποθήκευσης (usb flash disks) που βρέθηκαν συνδεδεμένα στο υπό κατάσχεση σύστημα. Στην περίπτωση αυτή, η αρχική μονάδα δίσκου αποθηκεύεται σε κατάλληλες συνθήκες φύλαξης με σκοπό: (α) την αποφυγή καταστροφής της από τις συνθήκες περιβάλλοντος αλλά και (β) για την προστασία της από τυχόν αθέμιτη/μη εξουσιοδοτημένη πρόσβαση.

Σε κάθε περίπτωση, είτε ο τεχνικός, είτε ο εξεταστής, οφείλει να επαληθεύσει τα ληφθέντα δεδομένα με τη χρήση των λειτουργιών SHA-1 ή MD5 hash, ενέργεια η οποία θα πρέπει να επαναλαμβάνεται περιοδικά κατά την διεξαγωγή των επόμενων βημάτων της διαδικασίας, με σκοπό την εξασφάλιση των αποδεικτικών στοιχείων, ότι δηλαδή είναι ακόμα στην αρχική τους κατάσταση.

2.3.2 Ανάλυση Συλλεχθέντων Πληροφοριών

Το επόμενο βήμα που οφείλουν να ακολουθήσουν οι τεχνικοί ψηφιακής εγκληματολογικής έρευνας, είναι η ανάλυση των συλλεχθέντων πληροφοριών. Η ανάλυση αυτή πραγματοποιείται προκειμένου να εντοπιστούν στοιχεία που να αποδεικνύουν ή να αντικρούουν την τέλεση μίας αξιόποινης πράξης.

Κατά την ανάλυση αυτή, οι ερευνητές χρησιμοποιούν μια σειρά από διαφορετικές μεθοδολογίες και εργαλεία (άλλοτε δωρεάν λογισμικά και άλλοτε λογισμικά με νόμιμες πληρωτέες άδειες).

Η χρήση εξειδικευμένων εργαλείων, αποβλέπει στην πρόσβαση σε συγκεκριμένο είδος πληροφοριών κάθε φορά. Δηλαδή, ανάλογα με το είδος της κακόβουλης ενέργειας, μπορεί η έρευνα να εστιάσει μόνο σε πληροφορίες που σχετίζονται με το ηλεκτρονικό ταχυδρομείο του

χρήστη, του υπό μελέτη συστήματος, ή την καταγραφή των διαδικτυακών του συνομιλιών (chat μέσω skype,viber, yahoo messenger κλπ), ή τυχόν εικόνες πορνογραφικού και μη περιεχόμενου που κατέβασε παράνομα από το διαδίκτυο, ή τυχόν έγγραφα εξυβριστικού, τρομοκρατικού ή άλλου παράνομου περιεχομένου.

Οι ερευνητές, οφείλουν να αναζητήσουν μέσα στις πληροφορίες που περισυνέλεξαν, λέξεις κλειδιά ή αρχεία συγκεκριμένης μορφής (scripts) τα οποία παραπέμπουν σε κακόβουλη ενέργεια. Πολλές φορές μάλιστα, καλούνται να εντοπίσουν διαγραμμένα ή κρυπτογραφημένα αρχεία. Είναι λοιπόν αναγκαία, είτε η επαναφορά τέτοιων κατακερματισμένων αρχείων, είτε η αποκρυπτογράφησή τους, με σκοπό τον εντοπισμό του περιεχομένου τους.

Υπάρχουν δε περιπτώσεις όπου οι κακόβουλοι χρήστες έχουν διαγράψει αρχεία από τον ηλεκτρονικό υπολογιστή, με τέτοιο τρόπο ώστε να είναι αδύνατη η επαναφορά τους ή γενικότερα η ανάκτησή τους. Σε αυτές τις περιπτώσεις, γίνεται δυσχερέστερο το έργο των ερευνητών, καθόσον η ανάλυση των δεδομένων και η εξαγωγή ασφαλών συμπερασμάτων πρέπει να γίνει μέσω της μελέτης της χρονικής αλυσίδας των πεπραγμένων ενεργειών, στο υπό μελέτη σύστημα. Ενέργεια, που απαιτεί χρόνο και εξοικείωση του προσωπικού με την συγκεκριμένη μορφή του αρχείου.

Σε κάθε περίπτωση όμως, η ανάλυση των πληροφοριών οδηγεί στην ανακατασκευή των γεγονότων ή επενεργειών, το οποίο βοηθάει τους ερευνητές στην εξαγωγή ασφαλών συμπερασμάτων για την τέλεση ή μη αξιόποινης πράξης.

Τέλος, οι ερευνητές που ασχολήθηκαν με την ανάλυση αυτή, μπορούν να κληθούν ως μάρτυρες (εμπειρογνώμονες) σε ποινική δίκη για να υποστηρίξουν ή να αντικρούσουν την ενοχή ή την αθωότητα του χρήστη, του υπό μελέτη συστήματος.

2.3.3 Συμπλήρωση & Υποβολή Αναφορικής Έκθεσης

Όταν μια έρευνα ολοκληρωθεί, δηλαδή όταν έχουν αναλυθεί όλες οι συλλεχθείσες πληροφορίες, τότε συντάσσεται μία έκθεση, η μορφή της οποίας πρέπει να είναι τέτοια, ώστε να μπορεί να αναγνωσθεί και από άτομα που δεν κατέχουν τις γνώσεις και την εξειδίκευση των ερευνητών.

Η έκθεση αυτή ή οι εκθέσεις αυτές, περιέχουν πάντα: (α) τα ονόματα των ερευνητών που απασχολήθηκαν με τη συλλογή και την ανάλυση των πληροφοριών της συγκεκριμένης υπόθεσης, (β) τις ημερομηνίες που έγιναν η κατάσχεση του ηλεκτρονικού μέσου, η συλλογή και η ανάλυση των πληροφοριών, (γ) ο αριθμός πρωτοκόλλου που δόθηκε για την υπόθεση αυτή σε περίπτωση που η έρευνα γίνεται από δημόσιο οργανισμό (αστυνομικές αρχές ή στρατιωτικές αρχές), (δ) τα πλήρη στοιχεία του ηλεκτρονικού υπολογιστή, (ε) η χρονική αλυσίδα των πεπραγμένων κακόβουλων ενεργειών, (στ) τα αρχεία που χρησιμοποιήθηκαν κατά την κακόβουλη/αξιόποινη πράξη και τέλος (η) τα συμπεράσματα των εμπειρογνωμόνων σχετικά με την τέλεση ή μη αξιόποινης πράξης.

Οι εκθέσεις αυτές, μεταβιβάζονται σε αυτόν που όρισε την έναρξη της όλης διαδικασίας, δηλαδή, είτε στον εισαγγελέα, σε περίπτωση εκτέλεσης προανακριτικών ή ανακριτικών ενεργειών (ποινική υπόθεση), είτε στην εντολοδόχο εταιρεία (σε περίπτωση αστικής υπόθεσης).

Σε κάθε περίπτωση όμως, αυτή η αναφορική έκθεση, αποτελεί το έγγραφο μέρος ενός συνολικού πακέτου αποδεικτικών στοιχείων, καθόσον τα τεκμήρια/αποδείξεις θα πρέπει πάντα να συμπεριλαμβάνονται σε ένα ψηφιακό μέσο (συνήθως σε έναν οπτικό δίσκο cd ή dvd).

2.4 Ανασκόπηση Κεφαλαίου 2

Στο κεφάλαιο 2, ορίστηκε η έννοια του όρων «Εγκληματολογία» και «Ψηφιακή Εγκληματολογία» αναλύοντας ταυτόχρονα την σημαντικότητα αυτών, για την Ελληνική Δικαιοσύνη. Επιπρόσθετα, παρουσιάστηκαν τα βήματα/στάδια της Ψηφιακής Εγκληματολογίας, τα οποία και ακολουθήθηκαν προκειμένου την ανάπτυξη του λογισμικού μας.

Παρακάτω, θα παρουσιάσουμε τον τρόπο με τον οποίο, το λογισμικό μας, συλλέγει, εξετάζει και αναλύει τα δεδομένα ενός ηλεκτρονικού υπολογιστή, που έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης από κακόβουλο χρήστη, περιγράφοντας ταυτόχρονα και την αναφορά που θα δημιουργηθεί στο τέλος της διαδικασίας αυτής.

ΚΕΦΑΛΑΙΟ 3 – ΣΥΛΛΟΓΗ ΠΛΗΡΟΦΟΡΙΩΝ

3.1 Εισαγωγή

Στο κεφάλαιο αυτό, θα περιγράψουμε τον τρόπο με τον οποίο συλλέγονται τα ψηφιακά πειστήρια, τόσο εάν το έκθεμα έχει βρεθεί ενεργοποιημένο, όσο και εάν έχει βρεθεί απενεργοποιημένο, κατά την χρονική στιγμή της κατάσχεσής του.

Ξεκινώντας λοιπόν την διαδικασία, ο τεχνικός της ψηφιακής εγκληματολογικής έρευνας, θα πρέπει να ανοίξει το λογισμικό που αναπτύξαμε. Εάν το λογισμικό αυτό βρίσκεται σε ένα εξωτερικό αποθηκευτικό μέσο, το οποίο είναι συνδεδεμένο στο υπό μελέτη σύστημα, τότε αυτό συνεπάγεται ότι το έκθεμα έχει βρεθεί ενεργοποιημένο. Εάν όμως, το λογισμικό βρίσκεται σε εξωτερικό δίσκο ο οποίος είναι συνδεδεμένος στο σύστημα του αναλυτή, αυτό συνεπάγεται ότι, το έκθεμα βρέθηκε απενεργοποιημένο και ο πρωτεύων σκληρός του δίσκος, έχει αφαιρεθεί και έχει προσαρτηθεί ως εξωτερικό αποθηκευτικό μέσο, πάνω στον ηλεκτρονικό υπολογιστή του αναλυτή. Για το λόγο αυτό, με το άνοιγμα του λογισμικού, τρέχει αυτόματα η παρακάτω εντολή κονσόλας και λαμβάνεται η εγγραφή του πεδίου "System Type" ([17] Microsoft Technet, 2017):

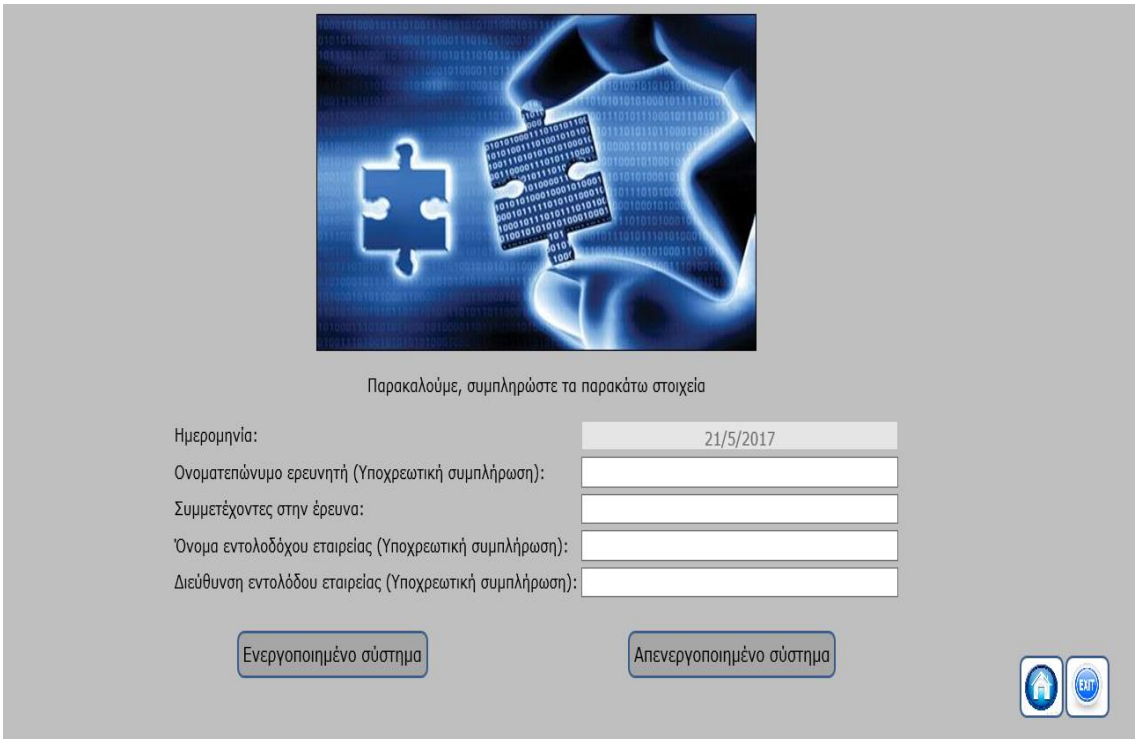
```
Systeminfo >  όνομα δίσκου\collected_information\General_information\systeminfo.txt
```

Ο λόγος που λαμβάνουμε την εγγραφή του πεδίου αυτού, είναι προκειμένου να εντοπίσουμε την έκδοση του λειτουργικού συστήματος, ώστε να γνωρίζουμε τα βοηθητικά προγράμματα που θα χρησιμοποιήσουμε, τόσο για την συλλογή, όσο και για την ανάλυση πληροφοριών, εάν θα πρέπει να χρησιμοποιήσουμε την 32 bit ή την 64 bit έκδοσή τους.

Με το άνοιγμα δε του λογισμικού, θα τρέξει το τυχόν εγκατεστημένο αντιβιοτικό (είτε του υπό μελέτη συστήματος, είτε του υπολογιστή του αναλυτή) και θα εξουδετερώσει αρκετά από τα χρησιμοποιηθέντα εργαλεία του λογισμικού μας. Για το λόγο αυτό, θα πρέπει να απενεργοποιηθεί το αντιβιοτικό, πρίν συνδεθεί ο εξωτερικός σκληρός δίσκος που περιέχει το λογισμικό μας. Επιπλέον επειδή η εφραμογή μας δεν έχει φορτωθεί σε κάποιο «webserver» γι αυτό θα σας ζητηθεί να αποδεχτείται αρκετές φορές την εκτέλεση των εντολών ActiveX.
Έτσι λοιπόν, φορτώνεται στον περιηγητή ιστού (Internet Explorer) η αρχική σελίδα (Εικόνα 3.1.1), στην οποία ο χρήστης θα πρέπει να πατήσει στο κουμπί «Συλλογή πληροφοριών» με σκοπό να ακολουθήσει την προβλεπόμενη διαδικασία συλλογής ψηφιακών πειστηριών.

Εικόνα 3.1.1: Αρχική Σελίδα

Στο σημείο αυτό, ο χρήστης του λογισμικού καλείται να συμπληρώσει κάποια πεδία (Εικόνα 3.1.2), τα οποία θα εισαχθούν αργότερα (αυτόματα) στην αναφορική έκθεση (Κεφάλαιο 5). Τα πεδία αυτά είναι: (α) το ονοματεπώνυμο του ερευνητή, δηλαδή του ατόμου που έχει αναλάβει την παρακολούθηση της εξέλιξης της εγκληματολογικής έρευνας, της εν λόγω υπόθεσης, (β) τα ονοματεπώνυμα των συμμετεχόντων στην έρευνα (τα οποία θα πρέπει να διαχωρίζονται με κόμμα), (γ) το όνομα της εντελοδόχου εταιρείας, η οποία αιτήθηκε την εγκληματολογική έρευνα ή στην περίπτωση της αυτόφωρης διαδικασίας, τότε αναγράφουμε το ονοματεπώνυμο του κατηγορούμενου και μέσα σε παρένθεση συμπληρώνουμε την έκφραση «αυτόφωρη διαδικασία» και (δ) τη διεύθυνση της εντολοδόχου εταιρείας ή την διεύθυνση από όπου πραγματοποιήθηκε η κατάσχεση του εκθέματος. Η συμπλήρωση των παραπάνω α,γ και δ πεδίων είναι υποχρεωτική και στην περίπτωση, της μη συμπλήρωσής τους, δεν μπορεί να συνεχιστεί η διαδικασία συλλογής των ψηφιακών πειστηρίων. Το δε πεδίο «Ημερομηνία» συμπληρώνεται αυτόματα, βάση της ημερομηνίας του συστήματος που αναγράφεται στο κάτω δεξί μέρος της οθόνης αυτού.



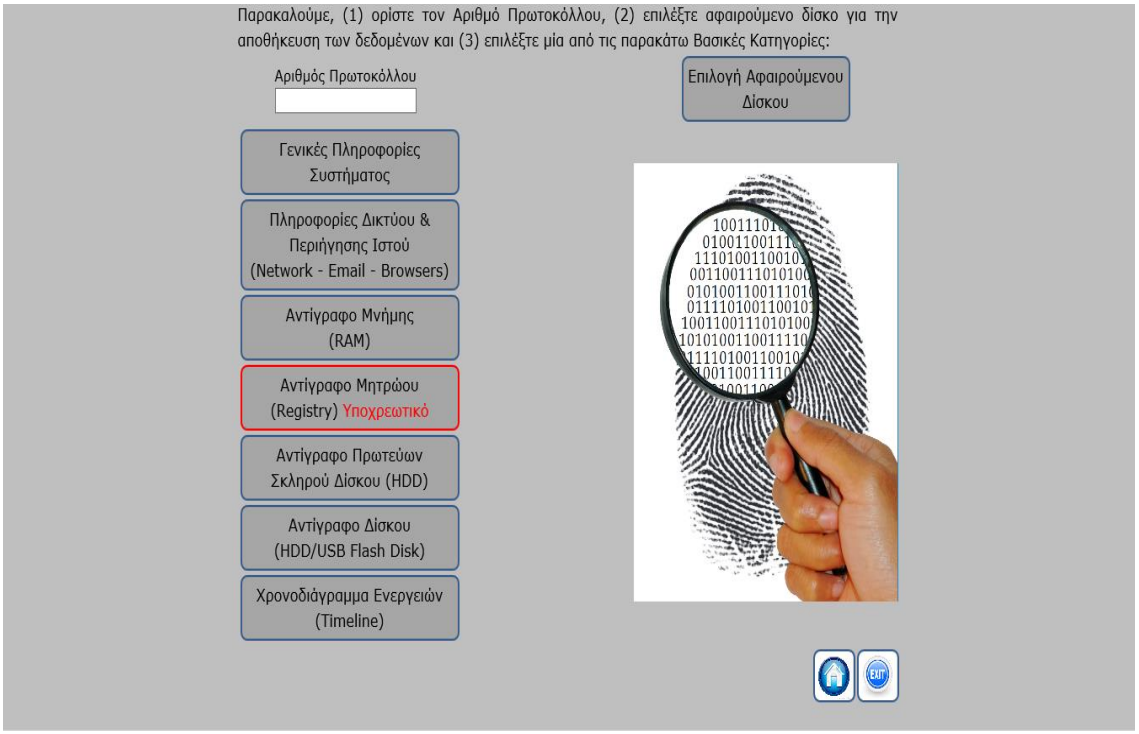
Εικόνα 3.1.2: Επιλογή Συλλογής Πληροφοριών από Ενεργοποιημένο/Απενεργοποιημένο Σύστημα

Εν συνεχεία, ο χρήστης, καλείται να επιλέξει πατώντας, σε ένα, από τα δύο (2) κουμπιά «Ενεργοποιημένο Σύστημα» ή «Απενεργοποιημένο Σύστημα», προκειμένου να ανοίξει η αντίστοιχη σελίδα με τις επιλογές συλλογής πληροφοριών, ανάλογα πάντα με την κατάσταση που βρέθηκε το έκθεμα. Για το λόγο αυτό, παρακάτω, θα διαχωρίσουμε τις δύο (2) αυτές περιπτώσεις και θα περιγράψουμε την διαδικασία συλλογής πληροφοριών και τις δυνατότητες που δίνονται, κάθε φορά, σε ξεχωριστά υποκεφάλαια.

Σε κάθε περίπτωση, ο χρήστης, οποτεδήποτε θελήσει να επιστρέψει στην αρχική σελίδα (Εικόνα 3.1.1), αρκεί να πατήσει στο κουμπί «Home», ενώ σε περίπτωση που επιθυμεί να εξέλθει από την εφαρμογή, αρκεί να πατήσει στο κουμπί «Exit». Μάλιστα, στην δεύτερη περίπτωση, το λογισμικό εκτελεί δύο (2) ενέργειες: (α) ελέγχει εάν εκκρεμούν τυχόν λειτουργίες και εμφανίζει σχετικό μήνυμα και (β) δημιουργεί αρχείο με την κατάληξη .csv το οποίο θα περιέχει πληροφορίες σχετικές με τα συλλεχθέντα ψηφιακά πειστήρια και το οποίο θα πρέπει να εισαχθεί ως πίνακας στην τελική αναφορική έκθεση (Κεφάλαιο 5).

3.2 Συλλογή Πληροφοριών από Ενεργοποιημένο Σύστημα

Ο χρήστης, πατώντας στο κουμπί «Ενεργοποιημένο Σύστημα», φορτώνεται αυτόματατα από τον περιηγητή ιστού του (Internet Explorer), η παρακάτω σελίδα (Εικόνα 3.2.1), όπου θα πρέπει αρχικά να συμπληρώσει τον «Αριθμό Πρωτοκόλλου», της εν λόγω υπόθεσης.



Εικόνα 3.2.1: Συλλογή Πληροφοριών από Ενεργοποιημένο Σύστημα

Επειδή ο αριθμός που θα πληκτρολογήσει, θα χρησιμοποιηθεί ως όνομα φακέλου (θα δημιουργηθεί αυτόματα και θα περιέχει όλα τα συλλεχθέντα ψηφιακά δεδομένα), γι' αυτό θα πρέπει να είναι πολύ προσεκτικός, καθόσον το λειτουργικό σύστημα των windows δεν επιτρέπει την χρήση των ειδικών χαρακτήρων (/, \, <, >, ", :, *, ?, |).

Εν συνεχεία, θα πρέπει να πατήσει στο κουμπί «Επιλογή Αφαιρούμενου Δίσκου», ώστε στο αναδυόμενο παράθυρο, να επιλέξει σε πιο αποθηκευτικό μέσο επιθυμεί να δημιουργηθεί ο ανωτέρω φάκελος (πιο συγκεκριμένα θα πρέπει να επιλέξει το φάκελο με το όνομα «Windows Forensics» που περιλαμβάνει όλα τα βοηθητικά εργαλεία και το λογισμικό μας, τα οποία βρίσκονται στον σκληρό δίσκο αυτό). Το χαρακτηριστικό αναγνωριστικό (γράμμα που δίνουν τα windows) του αποθηκευτικού μέσου που επιλέχθηκε, θα χρησιμοποιηθεί, αυτόματα, σε όλες τις εντολές κονσόλας που θα εκτελέσει το λογισμικό που αναπτύξαμε, κατά τη συλλογή και αποθήκευση των ψηφιακών πειστηρίων.

Στο σημείο αυτό, ο ερευνητής έχει τη δυνατότητα να επιλέξει τη συλλογή συγκεκριμένης κατηγορίας πληροφοριών, πατώντας σε ένα από τα παρακάτω κουμπιά:

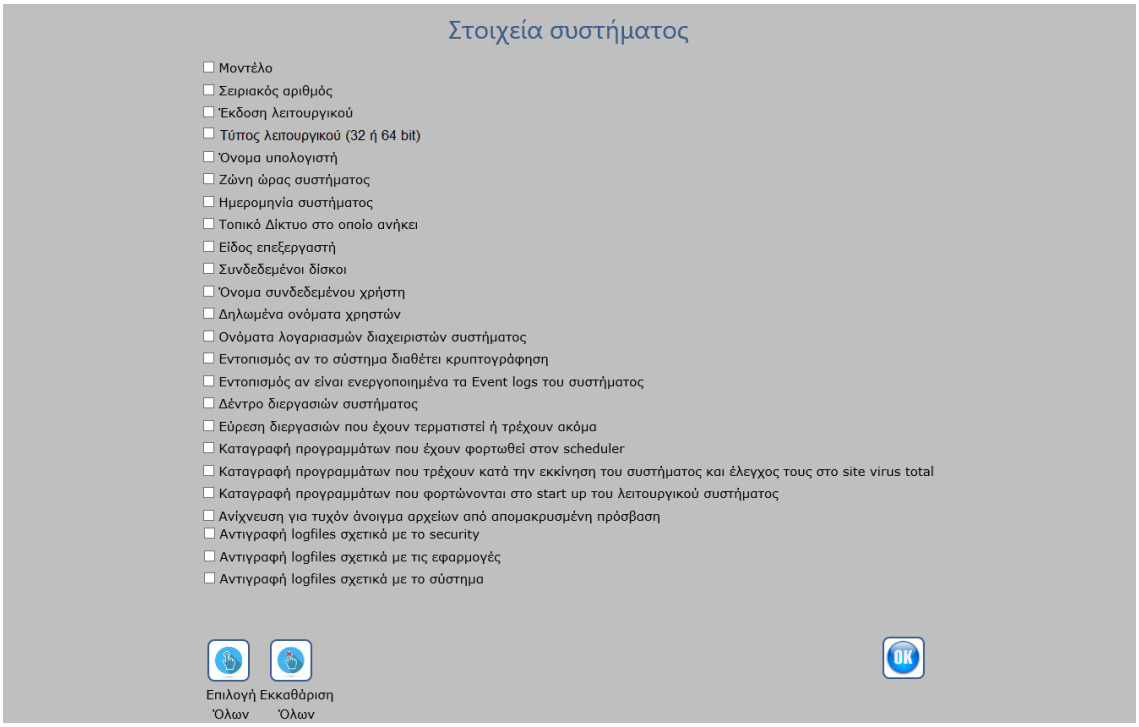
- Γενικές Πληροφορίες Συστήματος
- Πληροφορίες Δικτύου & Περιηγητών Ιστού (Network – Email - Browsers)
- Αντίγραφο Μνήμης (Ram)
- Αντίγραφο Μητρώου (Registry)
- Αντίγραφο Πρωτεύων Σκληρού Δίσκου (Hdd)
- Αντίγραφο Δίσκου (Hdd / Usb Flash Disk)
- Χρονοδιάγραμμα Ενεργειών (Timeline)

Θα αναλύσουμε δε, το κάθε ένα από αυτά, στα επόμενα υποκεφάλαια.

3.2.1 Συλλογή Γενικών Πληροφοριών Συστήματος

Εάν ο χρήστης, πατήσει στο κουμπί «Γενικές Πληροφορίες Συστήματος», τότε, ανοίγει μία νέα σελίδα στον περιηγητή του, στην οποία του δίνεται η δυνατότητα επιλογής, μεταξύ πολλών πληροφοριών (Εικόνα 3.2.1.1).

Θα πρέπει λοιπόν να επιλέξει ποιες από τις πληροφορίες αυτές τον ενδιαφέρουν, πατώντας στο αντίστοιχο κουτί επιλογής (check box) που βρίσκεται μπροστά από κάθε περιγραφή. Στην περίπτωση δε, που επιθυμεί να συλλέξει πληροφορίες για όλα τα αναγραφόμενα, τότε, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων», που βρίσκεται στο κάτω μέρος της οθόνης. Μάλιστα, στην περίπτωση που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών και θέλει μόνο την συλλογή ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν.



Εικόνα 3.2.1.1: Επιλογή Γενικών Πληροφοριών Συστήματος

Οι δε πληροφορίες που μπορούν να συλλεχθούν, είναι οι εξής:

1. Το μοντέλο του συστήματος για το οποίο χρησιμοποιήθηκε η εντολή κονσόλας ([6] Microsoft Developer Software, 2017):

```
Wmic csproduct get name
```

2. Ο σειριακός αριθμός της κεντρικής πλακέτας (mainboard) του συστήματος ([6] Microsoft Developer Software, 2017):

```
Wmic bios get serialnumber
```

3. Η έκδοση του Λειτουργικού Συστήματος των Windows, που έχει εγκατασταθεί στο έκθεμα (τιμή πεδίου OS Name) και αποθηκεύεται στο αρχείο με το όνομα systeminfo.txt ([17] Microsoft Technet, 2017):

```
Systeminfo > όνομα δισκου\collected_information\general_information\systeminfo.txt
```

4. Ο τύπος του Λειτουργικού Συστήματος των Windows, που έχει εγκατασταθεί στο έκθεμα (τιμή πεδίου System Type) και αποθηκεύεται στο αρχείο με το όνομα systeminfo.txt ([17] Microsoft Technet, 2017):

```
Systeminfo > όνομα δισκου\collected_information\general_information\systeminfo.txt
```

5. Το όνομα του Υπολογιστή, που δόθηκε κατά την εγκατάσταση του Λειτουργικού Συστήματος των Windows, (τιμή πεδίου Host Name) και αποθηκεύεται στο αρχείο με το όνομα systeminfo.txt ([17] Microsoft Technet, 2017):

```
Systeminfo > όνομα δισκου\collected_information\general_information\systeminfo.txt
```

6. Η ζώνη ώρας που έχει ρυθμιστεί, στο υπό μελέτη σύστημα (τιμή πεδίου Time Zone) και αποθηκεύεται στο αρχείο με το όνομα systeminfo.txt ([17] Microsoft Technet, 2017):

```
Systeminfo > όνομα δισκου\collected_information\general_information\systeminfo.txt
```

7. Η πλήρης ημερομηνία που δείχνει το σύστημα (κατά την λήψη των πληροφοριών), στο δεξί κάτω μέρος της οθόνης:

```
Echo %DATE% %TIME%
```

8. Το όνομα του τοπικού δικτύου, στο οποίο ανήκει το υπό μελέτη σύστημα (τιμή πεδίου Domain) και αποθηκεύεται στο αρχείο με το όνομα systeminfo.txt ([17] Microsoft Technet, 2017):

```
Systeminfo > όνομα δισκου\collected_information\general_information\systeminfo.txt
```

9. Το είδος του εγκατεστημένου επεξεργαστή (Intel ή amd και το μοντέλο του), στο υπό μελέτη σύστημα (τιμή πεδίου Processor Type) και αποθηκεύεται στο αρχείο με το όνομα hardware_processor_type.txt ([8]Microsoft TechNet, 2016):

```
wmic cpu get Name > όνομα δισκου\collected_information\general_information\
hardware_processor_typpe.txt
```

10. Τα ονόματα, τα είδη και το μέγεθος των συνδεδεμένων σκληρών δίσκων, οπτικών οδηγών και αφαιρούμενων μέσων αποθήκευσης (τιμή πεδίου Volume Type) και αποθηκεύονται στο αρχείο με το όνομα hardware.txt ([8]Microsoft TechNet, 2016):

```
Psinfo -d -s /AcceptEula > όνομα δισκου\collected_information\general_information\
hardware.txt
```

11. Το όνομα του χρήστη, που ήταν συνδεδεμένος κατά την ώρα κατάσχεσης του εκθέματος και αποθηκεύονται στο αρχείο με το όνομα ConnectedUser.txt ([16]LifeWire, 2017):

```
Echo %username% > όνομα δίσκου:\collected_information\general_information\
ConnectedUser.txt
```

12. Όλα τα ονόματα των χρηστών που διαθέτουν λογαριασμό, στο υπό μελέτη σύστημα και αποθηκεύονται στο αρχείο με το όνομα NetUser.txt ([16]LifeWire, 2017):

```
Net users > όνομα δίσκου:\collected_information \general_information\netusers.txt
```

13. Όλα τα ονόματα των διαχειριστών του συστήματος αυτού και αποθηκεύονται στο αρχείο με το όνομα Administrators.txt ([16]LifeWire, 2017):

```
Net localgroup administrators > όνομα δίσκου\collected_information\
general_information\administrators.txt
```

14. Εντοπισμός ύπαρξης τυχόν κρυπτογραφίας και εάν διαθέτει, τότε ποια είναι. Τα δε αποτελέσματα της αναζήτησης αυτής, αποθηκεύονται στο αρχείο με το όνομα Encryption_on_system.txt ([23]Magnet Forensics, 2017):

```
Edd /AcceptEula /batch > όνομα δίσκου\collected_information \general_information\
encryption_on_system.txt
```

15. Εντοπισμός, εάν στο σύστημα, έχει ενεργοποιηθεί ή όχι, η καταγραφή ενεργειών του χρήστη (Event Logs). Τα δε αποτελέσματα της αναζήτησης αυτής, αποθηκεύονται στο αρχείο με το όνομα Eventlogs_on_for.txt ([6] Microsoft Developer Software, 2017):

```
Wmic nteventlog get name > όνομα δίσκου\collected_information \general_information\
eventlogs_on_for.txt
```

16. Καταγραφή του δέντρου των Διεργασιών, του υπό μελέτη συστήματος (Process ID) και τα αποτελέσματα της αναζήτησης αυτής, αποθηκεύονται στο αρχείο με το όνομα processes.txt ([6] Microsoft Developer Software, 2017):

```
Wmic process get executablepath,parentprocessid, processid, name > όνομα δίσκου\
collected_information\general_information\processes.txt
```

17. Καταγραφή των Διεργασιών που έχουν τερματιστεί ή που τρέχουν ακόμα στο σύστημα, αποθήκεύοντας τα αποτελέσματα στο αρχείο, με το όνομα running-stopped_services.txt ([6] Microsoft Developer Software, 2017):

```
Wmic service list brief > όνομα δίσκου\ collected_information\general_information\ running-
stopped_services.txt
```

18. Καταγραφή των εφαρμογών που έχουν φορτωθεί στον αυτόματο χρονοπρογραμματιστή ενεργειών (Sheduler), ώστε να τρέχουν αυτόματα, είτε με την ενεργοποιήση, του λειτουργικού συστήματος των Windows, είτε σε κάποια καθορισμένη χρονική στιγμή. Τα δε αποτελέσματα της αναζήτησης αυτής, αποθηκεύονται στο αρχείο με το όνομα programmas_scheduler.txt συστήματος([8]Microsoft TechNet, 2016):

```
Schtasks.exe /query /v /fo list > όνομα δίσκου\ collected_information\
general_information\programms_scheduler.txt
```

19. Καταγραφή των εφαρμογών που εκτελούνται κατά την εκκίνηση του συστήματος, με ταυτόχρονο έλεγχό τους, στον ιστότοπο VirusTotal, για την εξερεύνησή τους, εάν πρόκειται για ιομορφικό λογισμικό ή όχι. Τα αποτελέσματα της αναζήτησης αυτής, αποθηκεύονται στο αρχείο με το όνομα programmas_autorun.txt ([14]Microsoft Technet, 2016):

```
Autorunsc.exe -a behw -vt -v /AcceptEula > όνομα δίσκου\ collected_information\
general_information\programms_autorun.txt
```

20. Καταγραφή των εφαρμογών που εκτελούνται κατά την εκκίνηση του λειτουργικού συστήματος των windows, στο υπό μελέτη σύστημα και αποθήκευσή τους, στο αρχείο με το όνομα start_up_programms.txt ([6] Microsoft Developer Software, 2017):

```
Wmic startup list brief > όνομα δίσκου\ collected_information \general_information\
start_up_programms.txt
```

21. Εντοπισμός τυχόν προσπέλασης αρχείων, από απομακρυσμένη πρόσβαση και αποθήκευση των αποτελέσματα της αναζήτησης αυτής, στο αρχείο με το όνομα open_remote_files.txt ([8]Microsoft TechNet, 2016):

```
Openfiles /query /fo csv > όνομα δίσκου\ collected_information \general_information\
open_remote_files.txt
```

22. Αντιγραφή όλων των πληροφοριών, σχετικά με τις ενέργειες του χρήστη (Log Files) που αφορούν το Security ([8]Microsoft TechNet, 2016):

```
Psloglist -s -t \t security /AcceptEula > c όνομα δίσκου\ collected_information
\general_information\security_log_files.txt
```

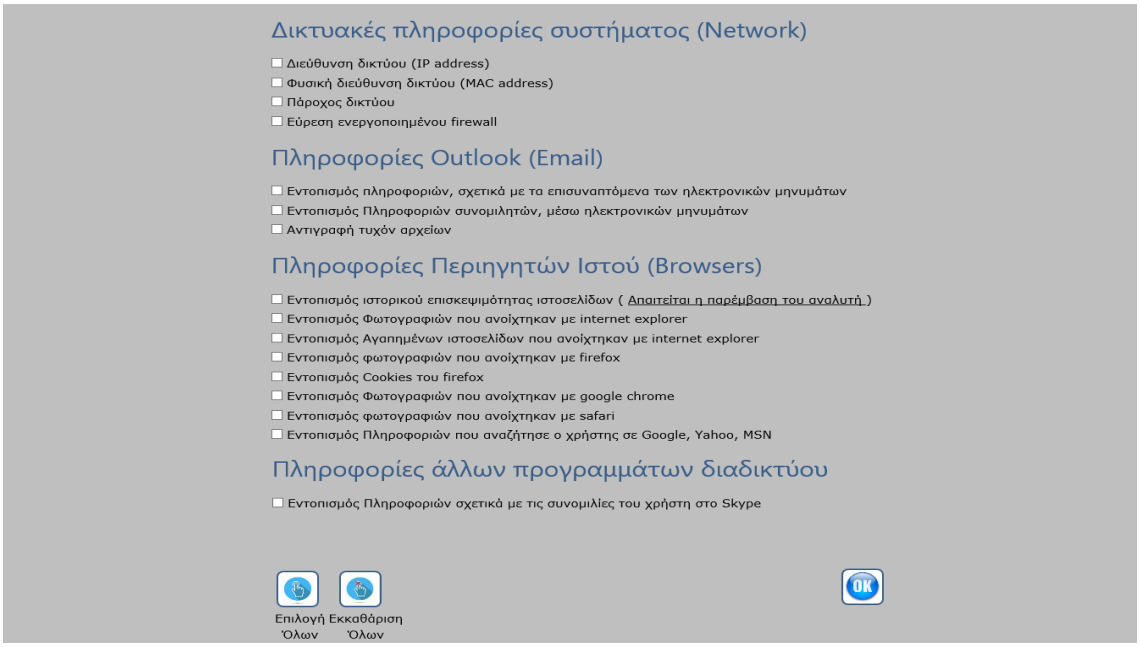
23. Αντιγραφή όλων των πληροφοριών, σχετικά με τις ενέργειες του χρήστη (Log Files) που αφορούν (α) την ασφάλεια και αποθηκεύονται στο Security, (β) τις εφαρμογές και αποθηκεύονται στο Software και (γ) το σύστημα και αποθηκεύονται στο System ([8]Microsoft TechNet, 2016):

```
Psloglist -s -t \t security /AcceptEula > όνομα δίσκου\ collected_information\
general_information\security_log_files.txt

Psloglist -s -t \t application /AcceptEula > όνομα δίσκου\ collected_information\
general_information \application_log_files.txt

Psloglist -s -t \t system /AcceptEula > όνομα δίσκου\ collected_information\
general_information \system_log_files.txt
```

Μετά το πέρας των επιλογών του, ο χρήστης, αρκεί να πατήσει στο κουμπί «OK», ώστε να επιστρέψει στη σελίδα της εικόνας 3.2.1.

3.2.2 Συλλογή Πληροφοριών Δικτύου & Περιηγητών Ιστού (Network – Email - Browsers)

Η δεύτερη δυνατότητα που δίνεται στον χρήστη της εφαρμογής, είναι η συλλογή πληροφοριών σχετικές με το δίκτυο και τους Περιηγητές Ιστού, του υπό μελέτη συστήματος (Εικόνα 3.2.2.1).



Εικόνα 3.2.2.1: Επιλογή Πληροφοριών Δικτύου & Περιηγητών Ιστού

Πατώντας πάνω στο κουμπί «Πληροφορίες Δικτύου & Περιηγητών Ιστού (Network – Email - Browsers)», τότε, ανοίγει η παραπάνω σελίδα στην οποία γίνεται διαχωρισμός των πληροφοριών, σε τέσσερις βασικές κατηγορίες:

- Δικτυακές Πληροφορίες Συστήματος (Network)
- Πληροφορίες Outlook (Email)
- Πληροφορίες Περιηγητών Ιστού (Browsers)
- Πληροφορίες άλλων προγραμμάτων διαδικτύου

Θα πρέπει λοιπόν να επιλέξει, ποιες από τις πληροφορίες αυτές τον ενδιαφέρουν, πατώντας στο αντίστοιχο κουτί επιλογής (check box) που βρίσκεται μπροστά από κάθε περιγραφή. Οι δε πληροφορίες που μπορούν να συλλεχθούν, σχετικά με το δίκτυο, του υπό μελέτη συστήματος, είναι οι εξής:

1. Η διεύθυνση δικτύου – Ip address, η οποία θα αποθηκευτεί στο αρχείο ipaddress.txt ([6] Microsoft Developer Software, 2017):

```
Wmic nicconfig get IPAddress > όνομα δίσκου\ collected_information\Email-Browsers\ ipaddress.txt
```

2. Η Φυσική διεύθυνση του δικτύου – MAC Address, η οποία θα αποθηκευτεί στο αρχείο macaddress.txt ([6] Microsoft Developer Software, 2017):

```
Wmic nicconfig get macaddress > όνομα δίσκου\collected_information\Email-Browsers\ macaddress.txt
```

3. Εντοπισμός πληροφοριών σχετικά με τον πάροχο του δικτύου, του υπό μελέτη συστήματος, οι οποίες εμπεριέχονται στο πεδίο «Connection-specific DNS Suffix», της παρακάτω εντολής κονσόλας και οι οποίες θα αποθηκευτούν στο αρχείο provider. txt ([6] Microsoft Developer Software, 2017):

```
Ipconfig / allcompartments /all > όνομα δίσκου\collected_information\Email-Browsers\ provider.txt
```

4. Εντοπισμός, εάν, στο υπό μελέτη σύστημα, έχει ενεργοποιηθεί η προστασία προς και από το διαδίκτυο, με τη χρήση του firewall, που προσφέρει το λειτουργικό σύστημα των windows. Τα αποτελέσματα δε της αναζήτησης αυτής, θα αποθηκευτούν στο αρχείο firewall.txt ([7]Microsoft Technet, 2017):

```
Netsh firewall show state > όνομα δίσκου\collected_information\Email-Browsers\ firewall.txt
```

Όσο αναφορά τις πληροφορίες που έχουν σχέση με τα μηνύματα ηλεκτρονικού ταχυδρομείου, χρησιμοποιώντας το λογισμικό «Outlook» ή «Outlook Express» της εταιρείας Microsft, ο χρήστης μπορεί να επιλέξει τα εξής:

1. Εντοπισμός περιεχομένου επισυναπτόμενων αρχείων (του χρήστη που ήταν συνδεδεμένος κατά την χρονική στιγμή κατάσχεσης του εκθέματος), σε ηλεκτρονικά μηνύματα ανεξάρτητα εάν αυτά είναι κείμενα, φωτογραφίες ή κάποιας άλλης μορφής αρχεία. Τα αποτελέσματα αυτής της αναζήτησης θα αποθηκευτούν στο αρχείο outlook_attached_list.txt ([46]NirSoft, 2009-2017):

```
Outlookattachview /stext όνομα δίσκου\collected_information\Email\ονομα συνδεδεμένου χρήστη\outlook_attached_list.txt
```

2. Εντοπισμός πληροφοριών, σχετικών με τους χρήστες που απέστειλαν ή που έλαβαν μήνυμα ηλεκτρονικού ταχυδρομείου, από τον χρήστη που ήταν συνδεδεμένος τη στιγμή της κατάσχεσης, του υπό μελέτη συστήματος. Οι πληροφορίες αυτές, θα αποθηκευτούν στο αρχείο outlook_user_statistics.txt ([47]NirSoft, 2009-2016):

```
Outlookstatview /stext όνομα δίσκου \collected_information\Email\ ονομα συνδεδεμένου χρήστη\outlook_user_statistics.txt
```

3. Εντοπισμός και αντιγραφή τυχόν αντιγράφων ασφάλειας (αρχεία back up), που είχει λάβει ο χρήστης, μέσω της δυνατότητας/επιλογής που προσφέρει, τόσο το λογισμικό «Outlok», όσο και το «Outlook Express», της εταιρείας Microsft. Τα αρχεία αυτά, ανάλογα την έκδοση της σουίτας προγραμμάτων «Office», της Microsoft, μπορούν να έχουν τις καταλήξεις: (α) .pst, (β) .pab, (γ) .pff, (δ) .ost και (ε) .off. Τα αποτελέσματα της παραπάνω αναζήτησης, αποθηκεύονται αυτόματα σε υποφάκελο, με το όνομα του χρήστη, ο οποίο θα βρίσκεται μέσα στο φάκελο email ([48]Forensicswiki, 2016):

```
Copy c:\users\όνομα συνδεδεμένου χρήστη\AppData\Local\Microsoft\Outlook\*.κατάληξη αρχείου όνομα δίσκου\collected_information\Email\Ονομα συνδεδεμένου χρήστη \Ονομα αρχειου
```

Στην ίδια σελίδα, δίνεται η δυνατότητα στον ερευνητή, να λάβει γνώση και των πληροφοριών που σχετίζονται με τη δράση του χρήστη στο διαδίκτυο (internet). Μπορεί να επιλέξει λοιπόν, μεταξύ των εξής δυνατοτήτων:

1. Εύρεση και καταγραφή του ιστορικού επισκεψιμότητας ιστοσελίδων και τα αποτελέσματα να αποθηκευτούν στο αρχείο browsers_history.txt ([9]NirSoft, 2012-2017):

```
Browsinghistoryview /stext όνομα δίσκου\collected_information\Browsers\ browsers_history.txt
```

2. Εντοπισμός φωτογραφιών, που άνοιξε ο χρήστης από τον Περιηγητή Ιστού «Internet Explorer» και αποθήκευση των πληροφοριών αυτών στο αρχείο ie_cache.txt ([10]NirSoft, 2007-2016):

```
IEcacheview /stext όνομα δίσκου \collected_information\Browsers\ie_cache.txt
```

3. Εντοπισμός ιστοσελίδων που αποθηκεύτηκαν ως αγαπημένες στον Περιηγητή Ιστού «Internet Explorer» και αποθήκευση των πληροφοριών αυτών στο αρχείο ie_favorites.txt ([49]NirSoft, 2004-2013) :

```
Faview /stext όνομα δίσκου\collected_information\Browsers\ie_favorites.txt
```

4. Εντοπισμός φωτογραφιών, που άνοιξε ο χρήστης από τον Περιηγητή Ιστού «Firefox Mozilla» και αποθήκευση των πληροφοριών αυτών στο αρχείο firefox_cache.txt ([11]NirSoft, 2007-2015):

```
Mozillacacheview /stext όνομα δίσκου\collected _information\Browsers\firefox_cache.txt
```

5. Εντοπισμός και αντιγραφή των αρχείων «cookies», που αποδέχτηκε ο χρήστης, χρησιμοποιώντας τον Περιηγητή Ιστού «Firefox Mozilla» και αποθήκευση των πληροφοριών αυτών στο αρχείο firefox_cookies.txt ([50]NirSoft, 2004-2016):

```
Mzcv /stext όνομα δίσκου\collected _information\Browsers\firefox_cookies.txt
```

6. Εντοπισμός φωτογραφιών, που άνοιξε ο χρήστης, από τον Περιηγητή Ιστού «Google Chrome» και αποθήκευση των πληροφοριών αυτών στο αρχείο chrome_cache.txt ([12]NirSoft, 2008-2016):

```
Chromecacheview /stext όνομα δίσκου\collected _information\Browsers\ chrome_cache.txt
```

7. Εντοπισμός φωτογραφιών, που άνοιξε ο χρήστης, από τον Περιηγητή Ιστού «Safari» και αποθήκευση των πληροφοριών αυτών στο αρχείο safari_cache.txt ([13]NirSoft, 2011-2012):

```
Safaricacheview /stext όνομα δίσκου\collected_information\Browsers\safari_cache.txt
```

8. Εντοπισμός πληροφοριών σχετικές με τις αναζητήσεις του χρήστη, χρησιμοποιώντας τις μηχανές αναζήτησης Google, Yahoo και MSN. Οι πληροφορίες αυτές θα αποθηκευτούν στο αρχείο last_search.txt ([45]NirSoft, 2007-2015):

```
Mylastsearch /stext όνομα δίσκου\collected_information\Browsers\last_search.txt
```

Τέλος, ο ερευνητής, μπορεί εάν επιθυμεί, να λάβει γνώση και για τις συνομιλίες του χρήστη (με άλλους χρήστες του διαδικτύου), στην περίπτωση που χρησιμοποίησε το λογισμικό «Skype». Στην περίπτωση αυτή, τα αποτελέσματα της εν λόγω αναζήτησης θα αποθηκευτούν στο αρχείο skype_history.txt ([36]NirSoft, 2008-2014):

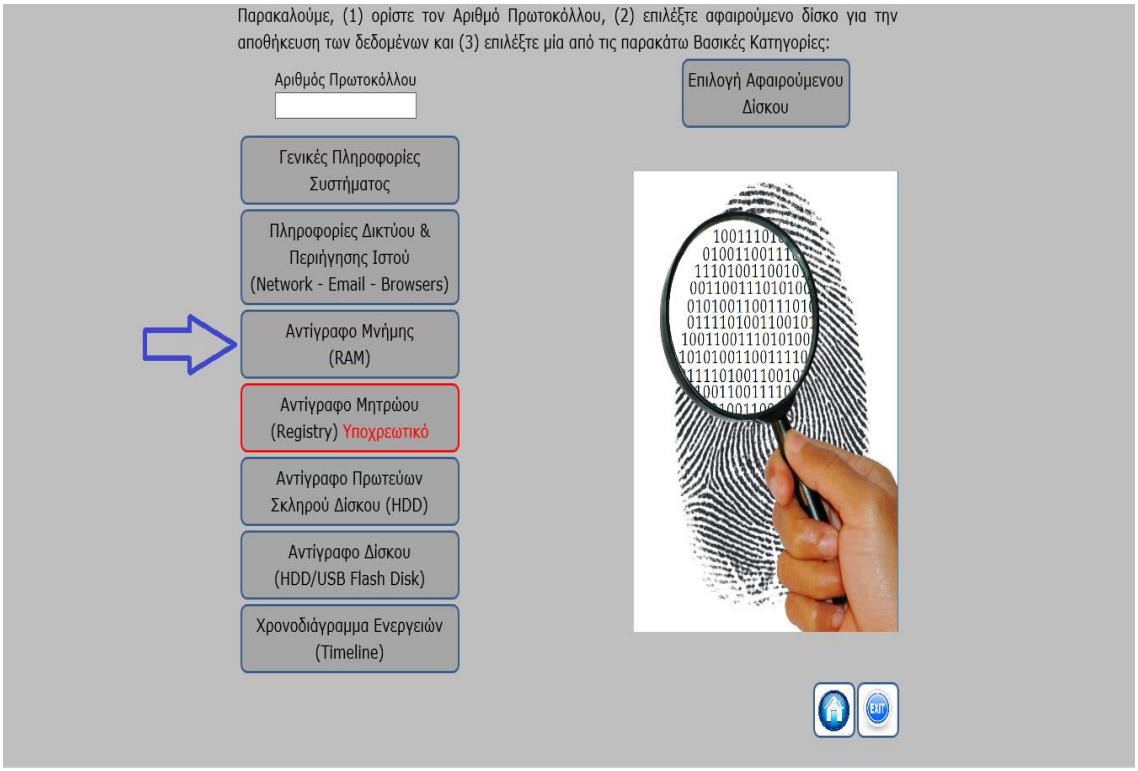
```
Skypelogview /stext  όνομα δίσκου\collected_information\Browsers\Skype_History.txt
```

3.2.3 Συλλογή Πληροφοριών από την Μνήμη (Ram)

Επόμενο βήμα για έναν ερευνητή εγκληματολογικής έρευνας είναι η λήψη αντιγράφου της μνήμης «RAM» (Εικόνα 3.2.3.1), καθόσον μόλις απενεργοποιηθεί το σύστημα, για να μεταφερθεί στα εγκληματολογικά εργαστήρια, θα διαγραφούν οι πληροφορίες (από την μνήμη).

Πατώντας στο κουμπί «Αντίγραφο Μνήμης (Ram)», αυτόματα εκτελείται το λογισμικό «MagnetRamCapture» και λαμβάνεται ένα πλήρες αντίγραφο της μνήμης (αρχείο με την κατάληξη .dmp), το οποίο και αποθηκεύεται στον υποφάκελο «ram». Η δε εντολή που τρέχει με το πάτημα του κουμπιού αυτού, είναι ([52]Magnet Forensics, 2017):

```
Magnetramcapture /go
```



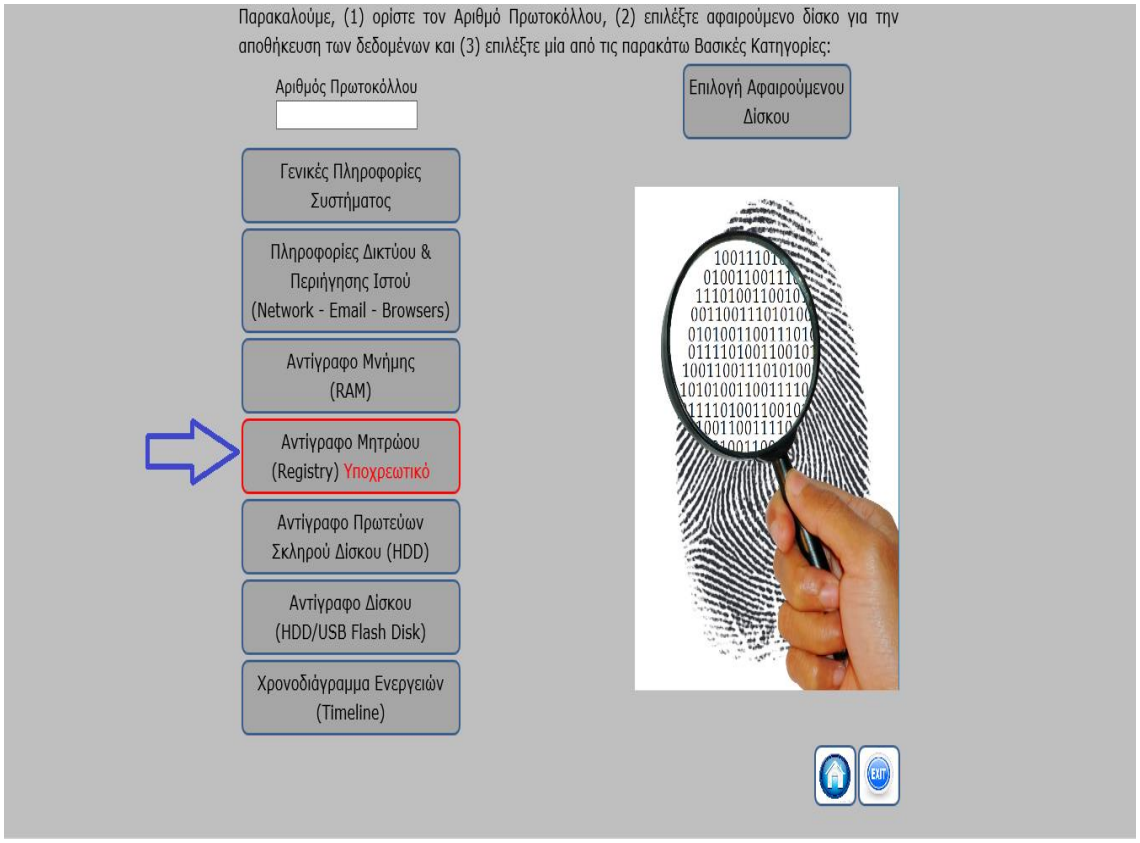
Εικόνα 3.2.3.1: Λήψη Αντιγράφου Μνήμης (Ram)

3.2.4 Συλλογή Πληροφοριών από το Μητρώο του Συστήματος (Registry)

Σε ένα σύστημα στο οποίο έχει εγκαταστασθεί το λειτουργικό σύστημα των windows, μόλις ο χρήστης ενεργοποιεί το σύστημα αυτό, τότε, φορτώνεται το λειτουργικό και ταυτόχρονα αναδιπλώνεται το μητρώο καταγραφών του συστήματος (Registry). Δηλαδή, εάν συγκρίνουμε τα περιεχόμενα του μητρώου, στο ίδιο σύστημα όταν αυτό είναι ερνεργοποιημένο και όταν είναι απενεργοποιημένο, θα παρατηρήσουμε διαφορά στην ποσότητα και στο περιέχομενο των κυψελών (Hives) του μητρώου.

Η διαφορά αυτή, στηρίζεται στην αναδίπλωση που προαναφέραμε και για το λόγο αυτό όταν ένα έκθεμα βρεθεί ενεργοποιημένο, κατά την κατάσχεσή του, απαιτείται η λήψη αντιγράφου του μητρώου (έχουμε προσθέσει κατάλληλη συνθήκη ελέγχου, ώστε να υποχρεώνουμε το χρήστη, να λάβει αντίγραφο του μητρώου καθόσον θα χρησιμεύσει στην μετέπειτα ανάλυση – Κεφάλαιο 4).

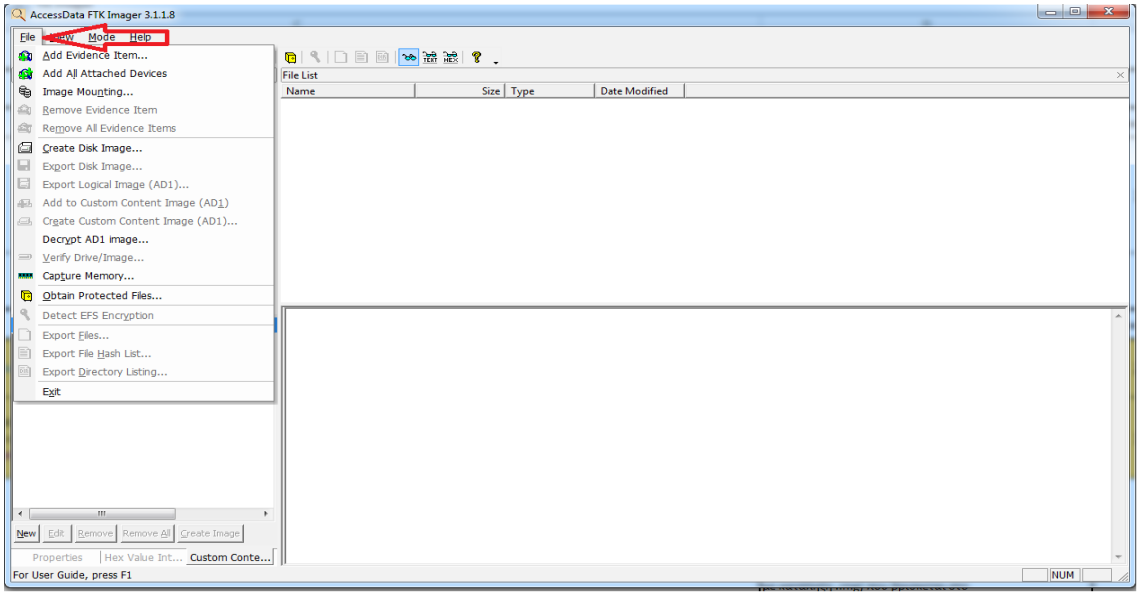
Πατώντας λοιπόν στο κουμπί «Αντίγραφο Μητρώου (Registry)», αυτόματα εκτελείται το λογισμικό «FTK Imager Lite» (Εικόνα 3.2.4.1). Να αναφέρουμε δε, ότι, είναι το μοναδικό βοηθητικό εργαλείο, που χρησιμοποιεί το λογισμικό μας και το οποίο απαιτεί την παρέμβαση του ερευνητή ([19]Access Data, 2016).



Εικόνα 3.2.4.1: Λήψη Αντιγράφου Μητρώου (Registry)

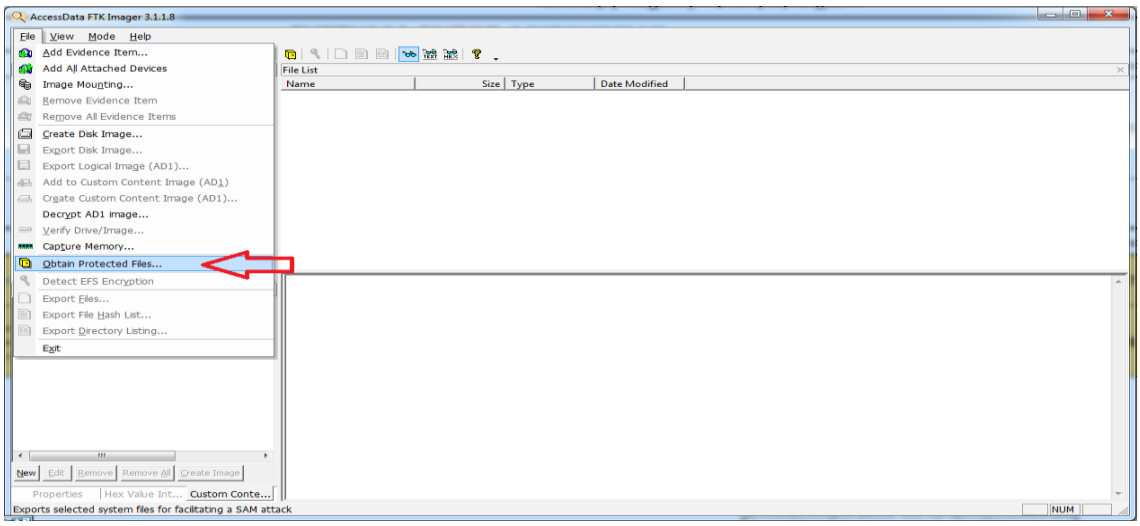
Στο σημείο αυτό, ο ερυνητής, οφείλει να ακολουθήσει τα εξής βήματα, προκειμένου να καταφέρει να συλλέξει πλήρως το μητρώο, του υπό μελέτη συστήματος:

1) Επιλογή της κατηγορίας «File» (με μονό πάτημα του αριστερού πλήκτρου του ποντικιού) που βρίσκεται στην αριστερή πάνω γωνία (Εικόνα 3.2.4.2) με σκοπό να αναδιπλωθεί το παράθυρο επιλογών, καθόσον, στο επόμενο βήμα, θα επιλέξουμε μία εξ αυτών.



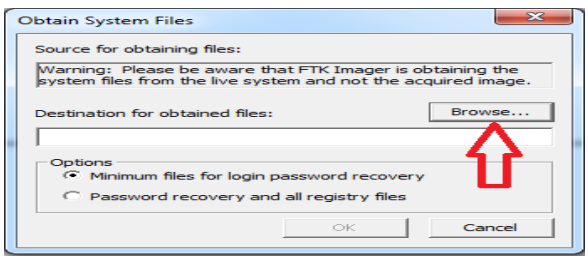
Εικόνα 3.2.4.2: FTK Imager Lite – Βήμα 1

2) Επιλογή της υποκατηγορίας «Obtain Protected Files» (με μονό πάτημα του αριστερού πλήκτρου του ποντικιού), με σκοπό να εμφανιστεί το νέο παράθυρο επιλογών (Εικόνα 3.2.4.2),.



Εικόνα 3.2.4.3: FTK Imager Lite – Βήμα 2

3) Πάτημα πλήκτρου «Browse», με σκοπό να εμφανιστεί αναδυόμενο παράθυρο στο οποίο καλούμαστε να επιλέξουμε που επιθυμούμε να αποθηκευτεί το αντίγραφο που θα ληφθεί (Εικόνα 3.2.4.3).



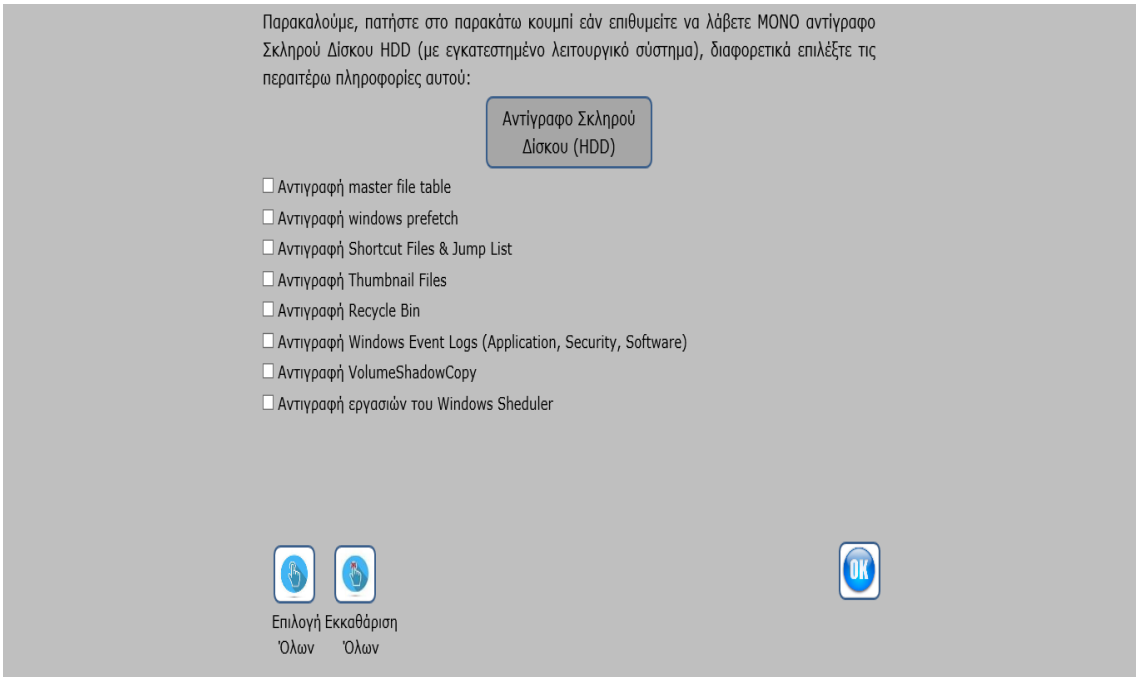
Εικόνα 3.2.4.4: FTK Imager Lite – Βήμα 3

4) Επιλογή, από το αναδυόμενο παράθυρο, του φακέλου που δημιουργήθηκε αυτόματα κατά το άνοιγμα της εν λόγω εφαρμογής (εχει όνομα «registry» και βρίσκεται μέσα στο φάκελο με όνομα τον αριθμό του πρωτοκόλλου που πληκτρολογήσαμε και ο οποίος βρίσκεται στο δίσκο αποθήκευσης που επιλέξαμε νωρίτερα, όπως περιγράψαμε στο κεφάλαιο 3.2) και πάτημα του κουμπιού «OK».
5) Πάτημα του αντίστοιχου κουτιού επιλογής (check box), που βρίσκεται μπροστά από την πρόταση που αναγράφει «Password recovery and all registry files», στο παράθυρο της εικόνας 3.2.4.2
6) Πάτημα του πλήκτρου «OK», του παραθύρου της εικόνας 3.2.4.2 για αυτόματη λήψη αντιγράφου, από τις πέντε (5) βασικές κυψέλες (Hives) του μητρώου. Δημιουργείται δε ένας επιπλέον φάκελος, με το όνομα «users» που περιέχει σημαντικές πληροφορίες του μητρώου, για κάθε έναν από τους χρήστες, που έχουν ενεργό λογαριασμό, στο υπό μελέτη σύστημα.

3.2.5 Συλλογή Πληροφοριών από την Πρωτεύων Σκληρό Δίσκο (Hdd)

Με τον όρο «Πρωτεύων Δίσκο», καλούμε τον φυσικό δίσκο στον οποίο έχει γίνει εγκατάσταση του λειτουργικού συστήματος των Windows, χωρίς όμως να μας ενδιαφέρει εάν αυτός έχει τεμαχιστεί σε επιμέρους κομμάτια (hdd partitions) ή όχι.

Χρήσιμο είναι λοιπόν, ο ερευνητής, να λάβει ένα πλήρες αντίγραφο του δίσκου (είδωλο δίσκου), του υπό μελέτη συστήματος, ώστε εάν επιθυμεί εκ των υστέρων, να μπορεί να φορτώσει το είδωλο αυτό (mount) σε μία πλατφόρμα εικονικού περιβάλλοντος (VMWare ή Oracle Virtual Box) για περαιτέρω μελέτη. Θα πρέπει λοιπόν, αρχικά, ο ερευνητής να πατήσει στο κουμπί «Αντίγραφο Πρωτεύων Σκληρού Δίσκου (Hdd)» (Εικόνα 3.2.5.1):



Εικόνα 3.2.5.1: Λήψη Αντίγραφου Πρωτεύοντος Σκληρού Δίσκου

Εν συνεχεία, δίνεται στον ερευνητή η δυνατότητα να επιλέξει εάν θέλει να λάβει μόνο ένα πλήρες αντιγραφο του σκληρού δίσκου, ή εάν επιθυμεί επίσης να λάβει αντίγραφα από επιμέρους πληροφορίες του λειτουργικού συστήματος, που είναι εγκατεστημένο στο δίσκο αυτό. Πατώντας λοιπόν, στο κουμπί «Αντίγραφο Σκληρού Δίσκου», εκτελείται η παρακάτω εντολή και δημιουργείται το είδωλο του σκληρού δίσκου ([18]Crysocome, 2010):

```
dd if=\\?\device\harddisk0\partition0 of=όνομα δίσκου\collected_information\hdd\ON\hdd_image.dd bs=1440κ
```

Ανάλογα δε, εάν στον δίσκο αυτό ήταν εγκατεστημένο το λειτουργικό σύστημα των Windows 7 (οποιαδήποτε έκδοσης αυτού) ή μεταγενέστερο λειτουργικό (windows 8, Windows 8.1 ή Windows 10), το είδωλο που θα δημιουργηθεί θα έχει αντίστοιχα την κατάλληξη .vpc ή .vhdx.

Ο ερευνητής μπορεί λοιπόν να επιλέξει ποιες από τις πληροφορίες αυτές τον ενδιαφέρουν, πατώντας στο αντίστοιχο κουτί επιλογής (check box) που βρίσκεται μπροστά από κάθε περιγραφή. Οι δε πληροφορίες που μπορούν να συλλεχθούν σχετικά με το εγκατεστημένο λειτουργικό είναι:

1. Αντιγραφή του κύριου πίνακα αρχείων (Master File Table), του λειτουργικού συστήματος των windows ([5]EaseUS, 2004-2017):

```
Rawcopy64.exe C:\$MFT όνομα δίσκου\collected_information\hdd
```

2. Αντιγραφή αρχείου (Windows Prefetch), στο οποίο διατηρούνται πληροφορίες των εφαρμογών που συνήθιζε να ανοίγει ο χρήστης, με σκοπό να φορτώνονται μαζί με το λειτουργικό σύστημα των windows και αποθήκευσή του, στο αρχείο prefetch.xml ([4]NirSoft, 2010-2016):

```
Winprefetchview.exe /sxml όνομα δίσκου\collected_information\hdd\prefetch.xml
```

3. Αντιγραφή αρχείου συντομεύσεων και παραπομπών (Shortcut files & Jump lists), στο οποίο διατηρούνται πληροφορίες σχετικές με τα αρχεία και τις εφαρμογές, του υπό μελέτη συστήματος ([30]WikiHow to do anything, 2017):

```
Xcopy c:\users\ονομα συνδεδεμένου χρηστη\appdata\roaming\microsoft\windows\recent\* όνομα δίσκου\collected_information\hdd\users\ονομα συνδεδεμένου χρηστη\recent_files /e /i /h
```

4. Αντιγραφή αρχείου μικρογραφιών εικόνων (Thumbnail files), που εμπλουτίζεται κάθε φορά που ο χρήστης ανοίγει μία εικόνα μέσα από το λειτουργικό σύστημα των windows ([30]WikiHow to do anything, 2017):

```
Xcopy c:\users\ονομα συνδεδεμένου χρηστη\appdata\local\microsoft\windows\explorer\thumb*.db όνομα δίσκου\collected_information\hdd\users\ονομα χρηστη\thumbnail_files /e /i /h
```

5. Αντιγραφή των περιεχομένων του κάδου ανακύκλωσης (Recycle Bin) του λειτουργικού συστήματος των windows :

```
Xcopy c:\$recycle.bin\*.* όνομα δίσκου\collected_information\hdd\recycle_bin /e /i /h
```

6. Αντιγραφή, όλων των αρχείων καταγραφής γεγονότων (Event Logs – Application,Security, Software) του λειτουργικού συστήματος των windows και αποθήκευση τους με τα ονόματα application_logs.evt, security_logs.evt και system_logs.evt, αντίστοιχα ([37]Windows Command Line):

```
Wmic nteventlog where filename='application' backupeventlog όνομα δίσκου\collected_information\hdd\application_logs.evt
Wmic nteventlog where filename='security' backupeventlog όνομα δίσκου \collected_information\hdd\security_logs.evt
Wmic nteventlog where filename='system' backupeventlog όνομα δίσκου \collected_information\hdd\system_logs.evt
```

7. Αντιγραφή, όλων των αντιγράφων ασφάλειας (Volume Snapshot Service, Volume Shadow Copy Services, VSS), που λήφθηκαν αυτόματα από την εν λόγω δυνατότητα/λογισμικό του λειτουργικού συστήματος των windows και αποθήκευσή τους, στο αρχείο volumeshadowcopy.txt ([39]Microsoft TechNet, 2017):

```
Vssadmin list shadows /for=c: > όνομα δίσκου\collected_information\hdd\VolumeShadowCopy.txt
```

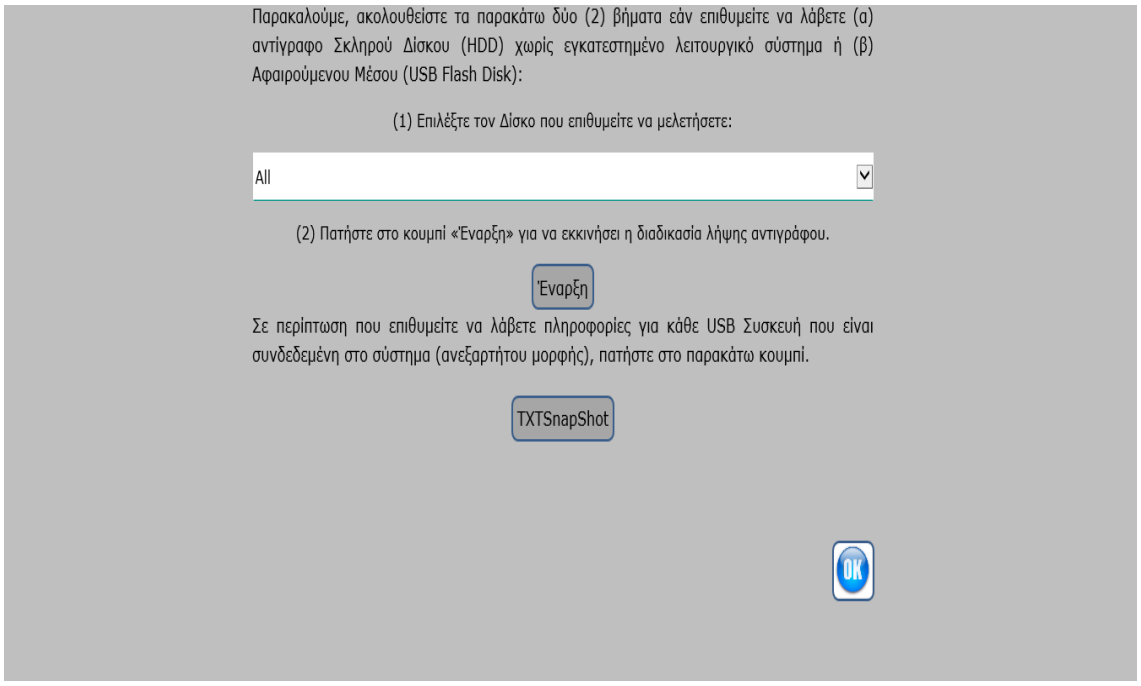
8. Αντιγραφή, όλων των εργασιών, που έχει προγραμματιστεί η ακριβής ημερομηνία και ώρα εκτέλεσής τους, με τη χρήση του λογισμικού «Scheduler» που προσφέρει το λειτουργικό σύστημα των windows και αποθήκευσή τους, στο αρχείο taskscheduler.txt ([40]NirSoft, 2015-2017):

```
TaskSchedulerview /stab όνομα δίσκου\collected_information\hdd\TaskScheduler.txt
```

3.2.6 Συλλογή Πληροφοριών από άλλα αποθηκευτικά μέσα (Hdd – Usb Flash Disks)

Κατά την χρονική στιγμή κατάσχεσης του εκθέματος, μπορεί ο ερευνητής να εντοπίσει περισσότερους από έναν φυσικό σκληρό δίσκο, εντός της κεντρικής μονάδας. Φυσικά, οι δίσκοι αυτοί δεν θα περιέχουν κάποιο λειτουργικό σύστημα, αλλά θα χρησιμεύουν απλά ως αποθηκευτικά μέσα. Την ίδια ακριβως λειτουργία, θα έχουν και όλοι εκείνοι οι σκληροί δίσκοι που δεν είναι εγκατεστημένοι, στο υπό μελέτη σύστημα, αλλά είναι συνδεδεμένοι εξωτερικά, είτε μέσω μια θύρας usb (external hard disks – usb falsh disks), είτε μέσω μιας θύρας δικτύου (wan nash).

Σε κάθε περίπτωση λοιπόν, η εφαρμογή μας, παρέχει στον ερευνητή, τη δυνατότητα λήψης αντιγράφου του σκληρού δίσκου ή του μέσου αποθήκευσης αυτού. Πατώντας στο κουμπί «Αντίγραφο Δίσκου (HDD/USB Flash Disk)», αυτόματα εμφανίζεται η παρακάτω σελίδα (Εικόνα 3.2.6.1):



Εικόνα 3.2.6.1: Λήψη Αντίγραφου Δίσκου (HDD/USB Flash Disk)

Ο χρήστης στο σημείο αυτό, θα πρέπει να ακολουθήσει δυο (2) βασικά βήματα, με σκοπό να επιτευχθεί η λήψη αντιγράφου. Αρχικά, θα πρέπει να επιλέξει από την αναδιπλούμενη λίστα, τον σκληρό δίσκο ή το εξωτερικό αποθηκευτικό μέσο (usb flash disk) του οποίου θέλει να λάβει το αντίγραφό του. Να αναφέρουμε δε, ότι στη λίστα αυτή δεν εμφανίζουμε, ούτε τον πρωτεύων δίσκο του συστήματος, αλλά ούτε και τους εγκατεστημένους οπτικούς δίσκους, του υπό μελέτη συστήματος. Αυτό επιτυγχάνεται, χρησιμοποιώντας την παρακάτω εντολή κονσόλας ([27]NirSoft, 2011-2016):

```
Driveletterview /stext όνομα δίσκου\collected_information\hdd\hdd_usb_flash_disk.txt
```

Αφού λοιπόν ο χρήστης, έχει επιλέξει το επιθυμητό αποθηκευτικό μέσο, αρκεί να πατήσει στο κουμπί «Έναρξη», με σκοπό την εκτέλεση της παρακάτω εντολής, η οποία θα εκκινήσει την διαδικασία λήψης αντιγράφου ([18]Crysocome, 2010):

```
DD if=\\.\γραμμα_δισκου: of=όνομα δίσκου\collected_information\hdd\OFF\
hdd_image.dd bs=1440k
```

Οφείλουμε να αναφέρουμε δε, ότι, η διαδικασία λήψης αντιγράφου δίσκου, είναι μια χρονοβόρα διαδικασία, η οποία εξαρτάται άμεσα από το μέγεθος του δίσκου που επέλεξε στο πρώτο βήμα, ο ερευνητής.

Θα παρατηρήσουμε ότι, στη λίστα αυτή έχει προστεθεί και η έκφραση «ALL», την οποία οφείλει να επιλέξει ο ερευνητής στην περίπτωση που θέλει να λάβει αντίγραφο από όλους τους σκληρούς δίσκους και τα αποθηκευτικά μέσα. Στην περίπτωηση αυτή, μάλιστα, θα εκτελεστεί επαναληπτικά η παραπάνω εντολή και φυσικά ο χρόνος λήψης αντιγράφων, θα είναι σημαντικά μεγαλύτερος.

Τέλος, στην περίπτωση που ο ερευνητής επιθυμεί να λάβει περισσότερες πληροφορίες για κάθε συνδεδεμένη usb συσκευή, του υπό μελέτη συστήματος, τότε αρκεί να πατήσει στο κουμπί «TXTSnapShot», το οποίο θα εκτελέσει αυτόματα την παρακάτω εντολή κονσόλας ([22]NirSoft, 2006-2016). Τα δε αποτελέσματα, θα τα εισάγει αυτόματα σε ένα αρχείο με το όνομα usb_devices.txt, το οποίο αποθηκεύεται στο φάκελο «analyzed_information» (φάκελος που περιέχει όλες τις αναλύσεις των ληφθέντων ψηφιακών πειστηρίων και εξηγείται πλήρως στο Κεφάλαιο 4):

```
Usbdeview /stext όνομα δίσκου\analyzed_information\USB\usb_devices.txt
/displaydisconnected 1 / displayhubs 1 / markconnecteddevices 1 / trayicon 0
```

3.2.7 Συλλογή Χρονοδιαγράμματος Ενεργειών (TimeLine)

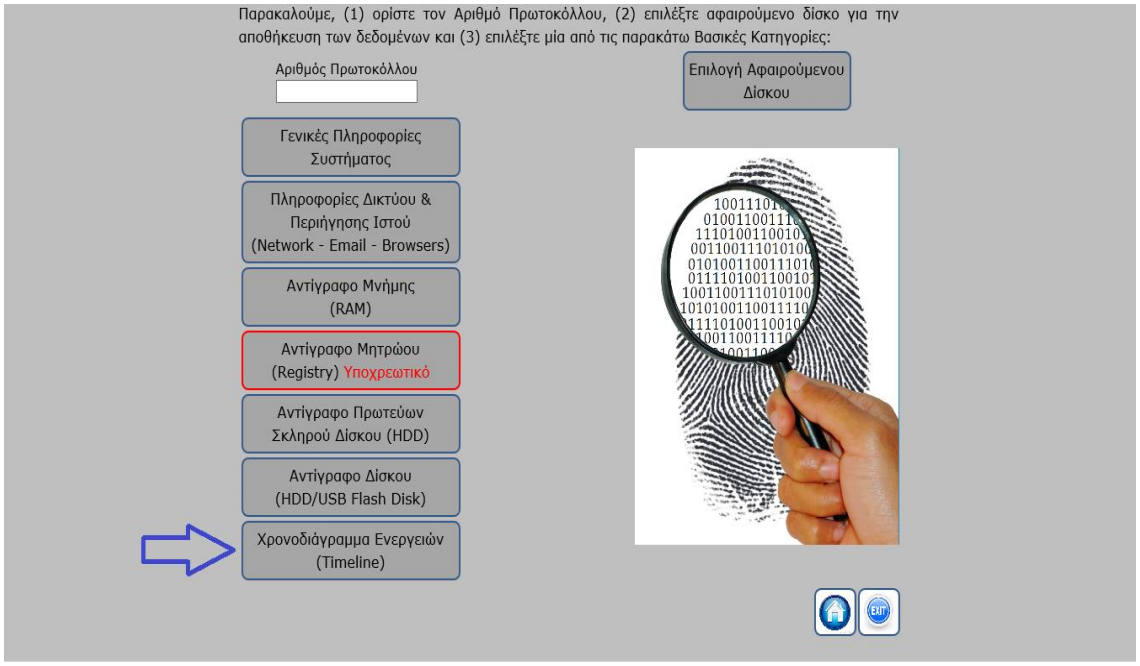
Σε κάθε ηλεκτρονικό υπολογιστή που έχει εγκατασταθεί το λειτουργικό σύστημα των windows, διατηρείται αυτόματα ένα αρχείο καταγραφής όλων των ενεργειών, τόσο από την πλευρά του χρήστη, όσο και από την πλευρά των εφαρμογών. Το αρχείο αυτό είναι γνωστό ως «TimeLine», η μελέτη του οποίου μπορεί να οδηγήσει τον ερευνητή στην κατανόηση της χρονικής αλληλουχίας των γεγονότων, που διαδραματίστηκαν, στο υπό μελέτη σύστημα.

Όταν ο ερευνητής της εγκληματολογικής έρευνας, πατήσει στο κουμπί «Χρονοδιάγραμμα Ενεργειών (Timeline)» (Εικόνα 3.2.7.1), τότε, αυτόματα, γίνεται ένας έλεγχος εάν έχει ληφθεί πλήρες αντίγραφο του Πρωτεύοντος Σκληρού Δίσκου ή όχι. Ο λόγος που δεν βάλαμε το λογισμικό μας να λάβει αντίγραφο του χρονοδιαγράμματος αυτού, είναι διότι η διαδικασία αυτή διαρκεί πάρα πολλές ώρες, έως και ημέρες (για παράδειγμα σε ένα δίσκο της τάξης των 250 gb, χρειάστηκαν 3 ημέρες για να ληφθεί το πλήρες αντίγραφο του χρονοδιαγράμματος ενεργειών).

Παρόλα αυτά όμως, το λογισμικό μας, δημιουργεί μια υποτυπώδη χρονική αλυσίδα, αλλά μόνο από το «FileSystem», του υπό μελέτη συστήματος, εκτελώντας την κάτωθι εντολή και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα filesystem_timeline.txt ([54}SleuthKit):

```
Fls.exe -i raw -m 'C:/' -f ntfs -z CST6CDT -r -p \\.\C: > όνομα δίσκου\collected_information\Timeline\Filesystem_Timeline.txt
```

Εάν, στο υπό μελέτη σύστημα, έχει ληφθεί αντίγραφο Πρωτεύοντος Σκληρού Δίσκου (άρα έχει δημιουργηθεί το αρχείο hdd.vhdx ή hdd.vpc μέσα στο φάκελο hdd\on) θα εμφανιστεί μήνυμα στην οθόνη που θα αναγράφει ότι δεν απαιτούνται περαιτέρω ενέργειες. Ενώ, εάν δεν έχει ληφθεί το σχετικό αντίγραφο, τότε, το μήνυμα θα διαφέρει και θα παραπέμπει τον ερευνητή στην λήψη του αντιγράφου αυτού (βλέπε υποκεφάλαιο 3.2.5).



Εικόνα 3.2.7.1: Συλλογή Χρονοδιαγράμματος Ενεργειών (TimeLine)

Στο σημείο αυτό, ολοκληρώνεται η διαδιακασία λήψης ψηφιακών πειστηρίων από ένα ενρεγοποιημένο σύστημα και αρκεί ο ερευνητής να πατήσει, είτε στο κουμπί «Home», είτε στο κουμπί «Exit». Και στις δύο (2) περιπτώσεις, θα ελέγχονται οι διεργασίες του συστήματος με σκοπό να βρεθεί εάν εκκρεμεί κάποια διεργασία σχετιζόμενη με τις εντολές κονσόλας (command lines) εμφανίζοντας σχετικό μήνυμα, περί μη ολοκλήρωσης των διαδικασιών που ζητήθηκαν.

Μετά το πέρας αυτών των διεργασιών, αυτόματα, η εφαρμογή, δημιουργεί και συμπληρώνει τμήμα της αναφορικής έκθεσης (που θα περιγραφεί στο κεφάλαιο 5).

3.3 Συλλογή Πληροφοριών από Απενεργοποιημένο Σύστημα

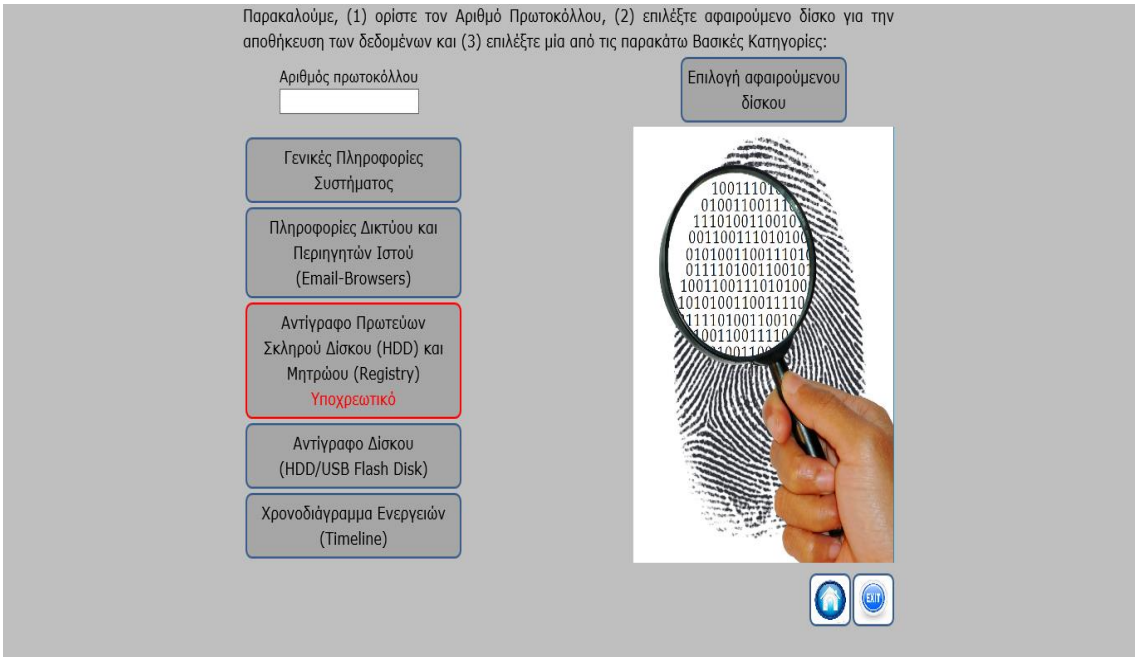
Σε ένα απενεργοποιημένο σύστημα, δεν είναι δυνατή η συλλογή τόσων πληροφοριών, όσο σε ένα ενεργοποιημένο σύστημα. Ο λόγος της διαφοράς αυτής, είναι καθόσον το σύστημα δεν έχει ακόμα ενεργοποιηθεί, δεν έχει αναδιπλωθεί το μητρώο του (Registry) και έτσι δεν έχουν ενεργοποιηθεί ακόμα όλες οι κυψέλες (Hives) αυτού.

Κατά συνέπεια, δεν έχουν αναγνωρισθεί ακόμα οι τεχνικές λεπτομέρειες του ηλεκτρονικού υπολογιστή (όπως ο σειριακός αριθμός της κεντρικής πλακέτας, ο κατασκευαστής αυτού, κλπ). Επιπλέον, σε ένα απενεργοποιημένο σύστημα, δεν έχει γίνει ο απαραίτητος προταρχικός έλεγχος (POST) από το «Bios» του συστήματος, με αποτέλεσμα πολλές συσκευές αυτού (κάρτα ήχου, κάρτα δικτύου, κλπ) να μην έχουν λάβει ακόμα ρεύμα. Έτσι, δεν είναι ακόμα δυνατόν να λάβουμε ακόμα πληροφορίες, όπως διεύθυνση δικτύου IP Address, κλπ.

Είναι λοιπόν κατανοητό, πως εάν κατά την κατάσχεση ενός εκθέματος, βρεθεί απενεργοποιημένο, οι πληροφορίες που θα συλλεχθούν θα είναι σαφώς πολύ λιγότερες. Σε μία τέτοια περίπτωση δε, ο ερευνητής της εγκληματολογικής έρευνας, οφείλει να αφαιρέσει τον σκληρό δίσκο του συστήματος και να τον προσαρτήσει ως εξωτερικό δίσκο, στο δικό του σύστημα ή σε οποιαδήποτε άλλο κατάλληλο σύστημα, για τη συλλογή ψηφιακών πειστηρίων απ' αυτό. Εν συνεχεία, μπορεί, είτε να λάβει οπτικά κάποιες πληροφορίες από το ίδιο το σύστημα (hardware), προκειμένου να μπορέσει να συμπληρώσει την αναφορική έκθεση (Κεφάλαιο 5), είτε να τοποθετήσει πίσω τον σκληρό δίσκο στο κατασχεμένο έκθεμα και αφού το ενεργοποιήσει, τότε να χρησιμοποιήσει το λογισμικό μας, για να λάβει τις επί μέρους πληροφορίες που τον ενδιαφέρουν.

Σε περίπτωση που ο ερευνητής αποσπάσει τον σκληρό δίσκο του κατασχεθέντος εκθέματος και τον προσαρτήσει ως εξωτερικό δίσκο στο σύστημά του (το λογισμικό μας μπορεί να βρίσκεται, είτε στον πρωτεύων δίσκο του συστήματος του ερευνητή, είτε σε έναν άλλο εξωτερικό δίσκο, ο οποίος όμως είναι και αυτός προσαρτημένος στο σύστημα του ερευνητή).

Στην περίπτωση αυτή, πατώντας στο κουμπί «Απενεργοποιημένο Σύστημα» φορτώνεται αυτόματατα από τον περιηγητή ιστού του (Internet Explorer) η παρακάτω σελίδα (Εικόνα 3.3.1), όπου θα πρέπει αρχικά ο ερευνητής, να συμπληρώσει τον «Αριθμό Πρωτοκόλλου», της εν λόγω υπόθεσης.



Εικόνα 3.3.1: Συλλογή Πληροφοριών από Απενεργοποιημένο Σύστημα

Επειδή ο αριθμός που θα πληκτρολογήσει, θα χρησιμοποιηθεί ως όνομα φακέλου (θα δημιουργηθεί αυτόματα και θα περιέχει όλα τα συλλεχθέντα ψηφιακά δεδομένα) γι'αυτό θα πρέπει να είναι πολύ προσεκτικός, καθόσον το λειτουργικό σύστημα των windows δεν επιτρέπει τη χρήση των ειδικών χαρακτήρων (/, \, <, >, ", :, *, ?, |).

Εν συνεχεία, θα πρέπει να πατήσει στο κουμπί «Επιλογή Αφαιρούμενου Δίσκου», ώστε στο αναδυόμενο παράθυρο να επιλέξει, σε πιο αποθηκευτικό μέσο επιθυμεί να δημιουργηθεί ο ανωτέρω φάκελος (πιο συγκεκριμένα θα πρέπει να επιλέξει το φάκελο με το όνομα «Windows Forensics» που περιλαμβάνει όλα τα βοηθητικά εργαλεία και το λογισμικό μας, τα οποία βρίσκονται στον σκληρό δίσκο αυτό). Το χαρακτηριστικό αναγνωριστικό (γράμμα που δίνουν τα windows), του αποθηκευτικού μέσου που επιλέχθηκε, θα χρησιμοποιηθεί αυτόματα σε όλες τις εντολές κονσόλας που θα εκτελέσει το λογισμικό που αναπτύξαμε, κατά την συλλογή και αποθήκευση των ψηφιακών πειστηρίων.

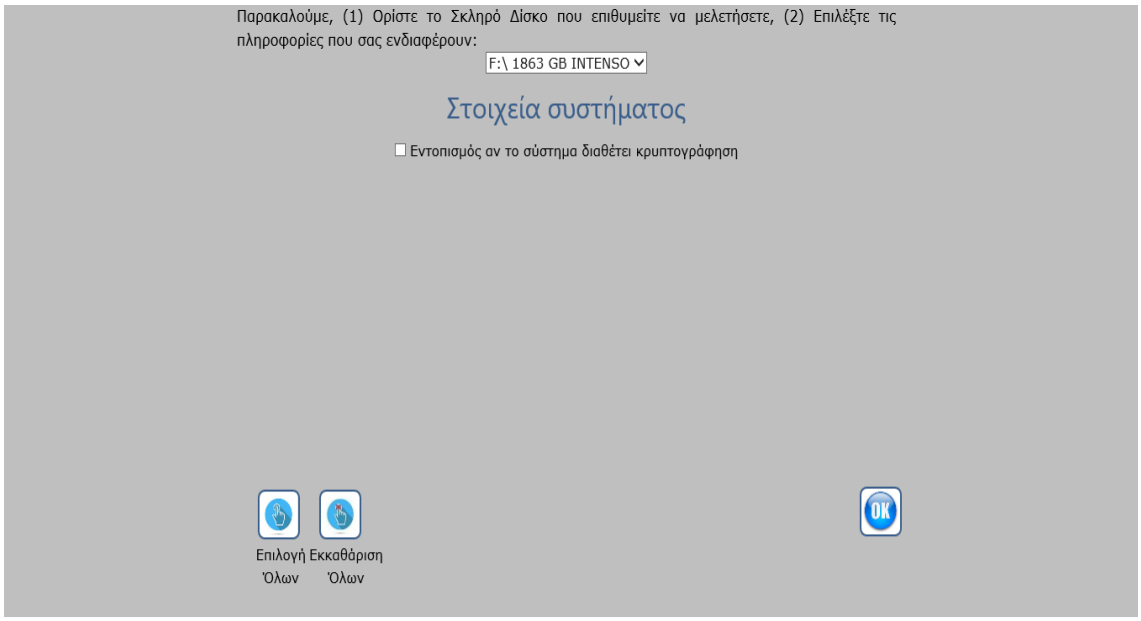
Στο σημείο αυτό, ο ερευνητής, έχει την δυνατότητα να επιλέξει τη συλλογή συγκεκριμένης κατηγορίας πληροφοριών, πατώντας σε ένα από τα παρακάτω κουμπιά:

- Γενικές Πληροφορίες Συστήματος
- Πληροφορίες Δικτύου & Περιηγητών Ιστού (Network – Email - Browsers)
- Αντίγραφο Πρωτεύων Σκληρού Δίσκου (Hdd) και Μητρώου (Registry)
- Αντίγραφο Δίσκου (Hdd / Usb Flash Disk)
- Χρονοδιάγραμμα Ενεργειών (Timeline)

Θα αναλύσουμε δε, το κάθε ένα από αυτά, στα επόμενα υποκεφάλαια.

3.3.1 Συλλογή Γενικών Πληροφοριών Συστήματος

Εάν ο χρήστης, πατήσει στο κουμπί «Γενικές Πληροφορίες Συστήματος», τότε, ανοίγει μία νέα σελίδα στον περιηγητή του (Εικόνα 3.3.1.1), στην οποία καλείται αρχικά να επιλέξει (από την αναδιπλούμενη λίστα), ποιόν από τους σκληρούς δίσκους που βρέθηκαν συνδεδεμένοι στο σύστημα του ερευνητή, επιθυμεί να μελετήσει. Στο σημείο αυτό, οφείλουμε να αναφέρουμε ότι, εάν δεν βρεθεί άλλος δίσκος πέραν του πρωτεύοντος σκληρού δίσκου του συστήματος του ερευνητή, τότε η σελίδα θα περιέχει μόνο ένα μήνυμα, το οποίο θα αναγράφει «Δεν βρέθηκαν δίσκοι».



Εικόνα 3.3.1.1: Επιλογή Γενικών Πληροφοριών Συστήματος

Αφού λοιπόν επιλεγεί ο επιθυμητός δίσκος, τότε, η μόνη πληροφορία που μπορεί να συλλεχθεί είναι, εάν στον υπό μελέτη δίσκο υπάρχει ή όχι κρυπτογραφημένα αρχεία. Έτσι, πατώντας στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την έκφραση «Εντοπισμός εάν το σύστημα διαθέτει κρυπτογράφηση», αυτόματα, ξεκινάει η διαδικασία μελέτης του συστήματος τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα encryption_on_systme.txt ([15]Microsoft Technet):

```
Cipher /y /c γραμμα δισκου > όνομα δίσκου\collected_information\General_information\encryption_on_system.txt
```

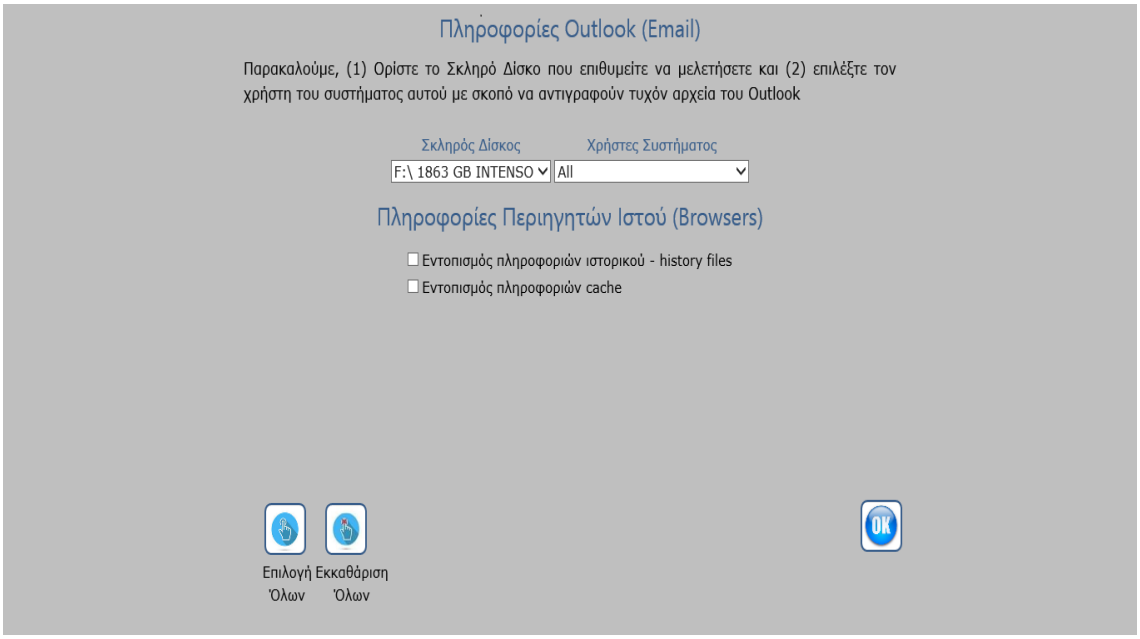
Ο χρήστης πατώντας στο κουμπί «OK» επιστρέφει στη σελίδα της εικόνας 3.3.1.

3.3.2 Συλλογή Πληροφοριών Δικτύου & Περιηγητών Ιστού (Email - Browsers)

Η δεύτερη δυνατότητα, που δίνεται στην περίπτωση του απενεργοποιημένου συστήματος, είναι η συλλογή πληροφοριών σχετικές με το δίκτυο και τους περιηγητές Ιστού, του υπό μελέτη συστήματος.

Πατώντας πάνω στο κουμπί «Πληροφορίες Δικτύου & Περιηγητών Ιστού (Email - Browsers)», τότε, ανοίγει μία νέα σελίδα (Εικόνα 3.3.2.1) στην οποία γίνεται διαχωρισμός των πληροφοριών σε δύο βασικές κατηγορίες:

- Πληροφορίες Outlook (Email)
- Πληροφορίες Περιηγητών Ιστού (Browsers)



Εικόνα 3.3.2.1: Επιλογή Πληροφοριών Δικτύου & Περιηγητών Ιστού

Θα πρέπει λοιπόν ο χρήστης, να επιλέξει τον δίσκο που θα ερευνήσει και στη συνέχεια να ορίσει ακριβώς ποιού χρήστη, του υπό μελέτη συστήματος, επιθυμεί να μελετήσει τις κινήσεις του, στο διαδίκτυο. Φυσικά, δεν πρέπει να παραλείψουμε να αναφέρουμε ότι, εάν δεν βρεθεί σκληρός δίσκος προσαρτημένος στο σύστημα του ερευνητή, τότε, θα εμφανιστεί μήνυμα περί μη εύρεσης σχετικού δίσκου και δεν θα εμφανιστεί η σελίδα της εικόνας 3.3.2.1.

Στην περίπτωση που ο ερευνητής έχει ορίσει τα παραπάνω δύο, τότε, αυτόματα, λαμβάνονται αντίγραφα τυχόν αντιγράφων ασφάλειας (αρχεία back up) που έχει λάβει ο χρήστης μέσω της δυνατότητας/επιλογής που προσφέρει, τόσο το λογισμικό «Outlok», όσο και το «Outlook Express» της εταιρείας Microsft. Τα αρχεία αυτά, ανάλογα την έκδοση της σουίτας προγραμμάτων «Office», της Microsoft, μπορούν να έχουν τις καταλήξεις: (α) .pst, (β) .pab, (γ) .pff, (δ) .ost και (ε) .off. Τα αποτελέσματα της παραπάνω αναζήτησης αποθηκεύονται, αυτόματα, σε υποφάκελο με το όνομα του χρήστη, ο οποίο θα βρίσκεται μέσα στο φάκελο email ([48]Forensicswiki, 2016):

```
Copy c:\users\όνομα συνδεδεμένου χρήστη\AppData\Local\Microsoft\ Outlook\*.κατάληξη αρχείου  όνομα δίσκου\collected_information\Email\Ονομα συνδεδεμένου χρήστη \Ονομα αρχειου
```

Το λογισμικό μας, στο σημείο αυτό, παρέχει στον ερευνητή, τη δυνατότητα συλλογής πληροφοριών σχετικές με το ιστορικό επισκεψιμότητας ιστοσελίδων, από τον περιηγητή ιστού (internet explorer). Μάλιστα, εάν στο προηγούμενο βήμα, ο ερευνητής είχε επιλέξει την επιλογή «All» στους χρήστες του συστήματος, τότε η παρακάτω εντολή κονσόλας θα εκτελεστεί επαναληπτικά, για κάθε έναν από τους χρήστες αυτού:

```
Copy ονομα δισκου:\users\Ονομα χρηστη\AppData\Local\Microsoft\Windows\ History\History.IE5 όνομα δίσκου\collected_information\Browsers\Ονομα χρηστη\
```

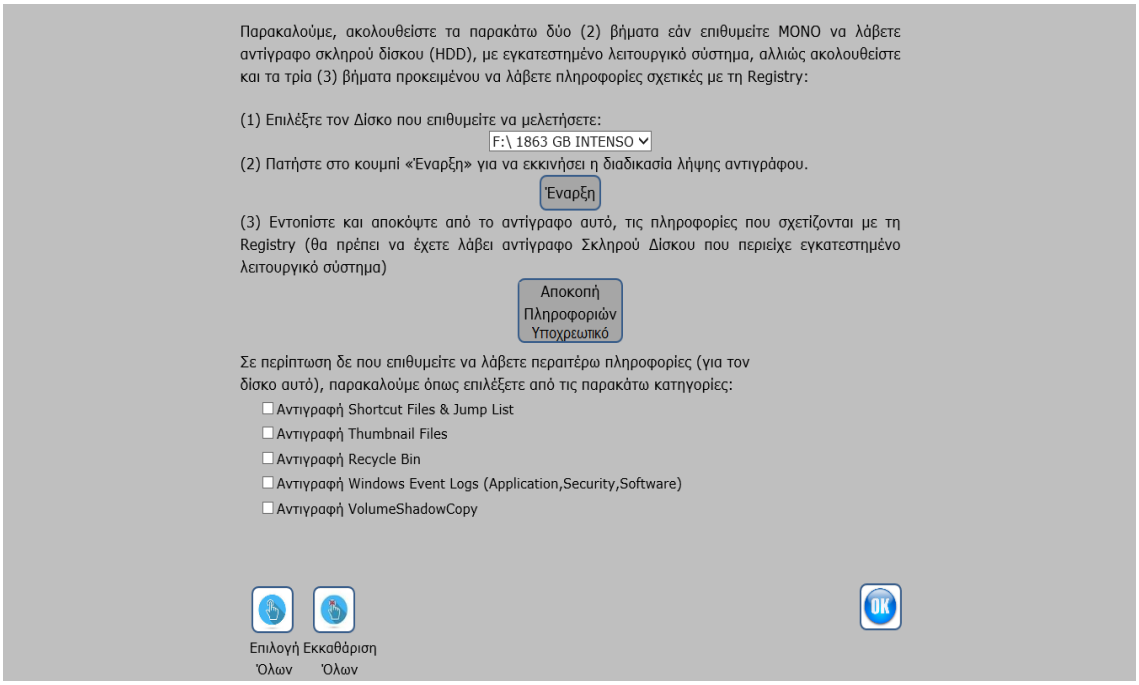
Copy ονομα δισκου:\users\Ονομα χρηστη\AppData\Local\Microsoft\Windows\ History\Low\History.IE5 όνομα δίσκου\collected_information\Browsers\Ονομα_χρηστη\
Copy ονομα δισκου:\users\Ονομα χρηστη\AppData\Local\Microsoft\Windows\ Webcache\webcacheV*.dat όνομα δίσκου\ collected_information\Browsers\Ονομα χρηστη\

Τέλος, ο ερευνητής, εάν επιλέξει τον εντοπισμό πληροφοριών cache του περιγητή ιστού (internet explorer), τότε, αυτόματα, τρέχει η παρακάτω εντολή κονσόλας για τον χρήστη που έχει επιλεγεί στο πεδίο «Χρήστες Συστήματος», όπως αναφέραμε πιο πάνω (η εντολή μπορεί να τρέξει επαναληπτικά και για όλους τους χρήστες, στην περίπτωση που έχει επιλογή το «All»):

Copy ονομα δισκου:\users\Ονομα χρηστη\AppData\Local\Microsoft\Windows\ Temporary Internet Files\content.IE5 όνομα δίσκου\collected_information\ Browsers\Ονομα_χρηστη\
Copy ονομα δισκου:\users\Ονομα χρηστη\AppData\Local\Microsoft\Windows\ Temporary Internet Files\low\content.IE5 όνομα δίσκου\collected_information\ Browsers\Ονομα_χρηστη\
Copy ονομα δισκου:\users\Ονομα χρηστη\AppData\Local\Microsoft\Windows\ Temporary Internet Files όνομα δίσκου\collected_information\Browsers\Ονομα_χρηστη\

3.3.3 Συλλογή Αντιγράφου Πρωτεύων Σκληρού Δίσκου (Hdd) και Μητρώου Συστήματος (Registry)

Πατώντας, πάνω στο κουμπί «Συλλογή Αντιγράφου Πρωτεύων Σκληρού Δίσκου(Hdd) και Μητρώου Συστήματος(Registry)», ανοίγει η νέα σελίδα (Εικόνα 3.3.3.1) στην οποία ο ερευνητής έχει την δυνατότητα να ακολουθήσει δύο (2) βασικά βήματα για να λάβει αντίγραφο, μόνο του πρωτεύοντος σκληρού δίσκου (Hdd), του υπό μελέτη συστήματος ή να ακολουθήσει και ένα τρίτο βήμα, με σκοπό να λάβει και αντίγραφο του Μητρώου (Registry), του υπό μελέτη συστήματος.



Εικόνα 3.3.3.1: Λήψη Αντίγραφου Πρωτεύοντος Σκληρού Δίσκου (HDD) & Μητρώου (Registry)

Αρχικά λοιπόν, ο ερευνητής, θα πρέπει να επιλέξει από τη λίστα, έναν σκληρό δίσκο ο οποίος να περιέχει εγκατεστημένο λειτουργικό σύστημα των windows και ο οποίος να έχει προσαρτηθεί στο σύστημά του, ως εξωτερικός σκληρός δίσκος (ο πρωτεύων δίσκος του κατασχεθέντος εκθέματος, το χαρακτηριστικό -physicaldrive**νούμερο**- του οποίου θα χρησιμοποιηθεί στην παρακάτω εντολή κονσόλας). Στη συνέχεια, θα πρέπει να πατήσει στο πλήκτρο «Έναρξη», με σκοπό να τρέξει η παρακάτω εντολή κονσόλας, η οποία θα εκκινήσει την διαδικασία λήψης πλήρους αντιγράφου του επιλεχθέντος σκληρού δίσκου([18]Crysocome, 2010):

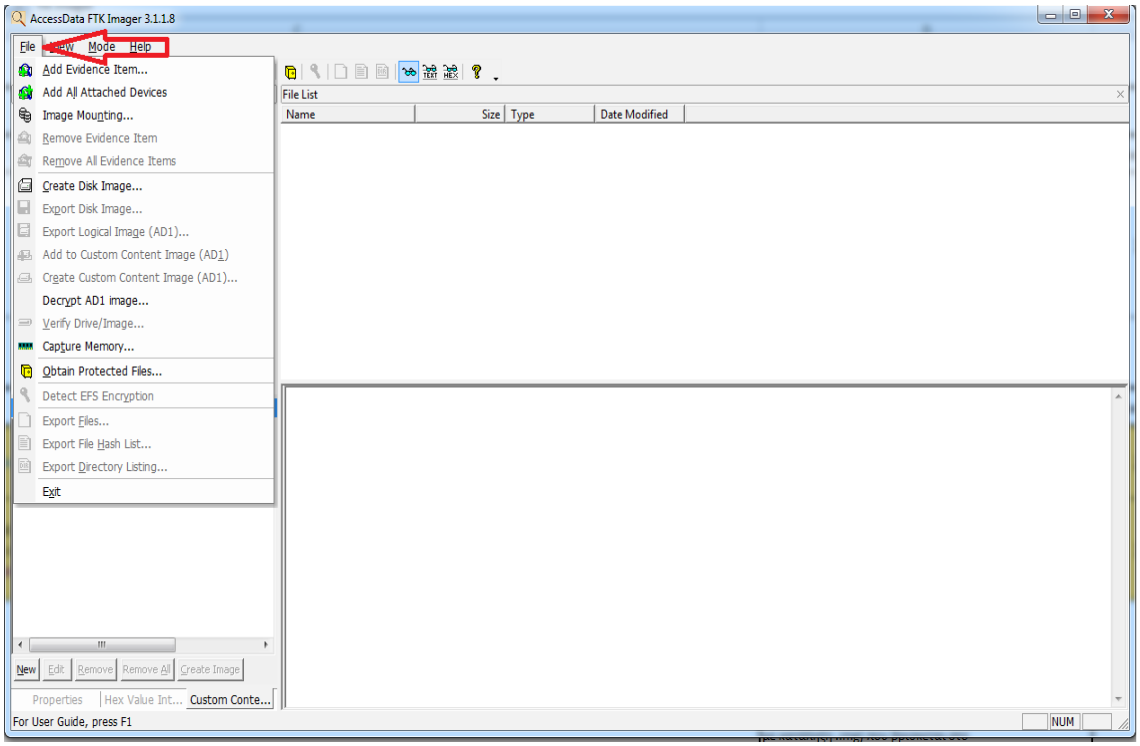
DD if=\\.\physicaldrive**νουμερο** of=όνομα δίσκου\collected_information\HDD\OFF\hdd_image.dd bs=1440k

Η εντολή αυτή, θα δημιουργήσει ένα αρχείο με το όνομα hdd_image.dd, το οποίο θα αποθηκευτεί μέσα στον υποφακέλο «OFF», ο οποίος θα δημιουργηθεί και αυτός αυτόματα και το όνομα, του οποίου μας καθορίζει ότι, το υπό μελέτη σύστημα βρέθηκε απενεργοποιημένο κατά την χρονική στιγμή της κατάσχεσής του.

Στην περίπτωση που ο ερευνητής θέλει να συλλέξει και πληροφορίες σχετικά με τις βασικές κυψέλες (Hives) του μητρώου (registry), του υπό μελέτη συστήματος, θα πρέπει να πατήσει στο κουμπί «Αποκοπή Πληροφοριών» ([19]Access Data, 2016). Μάλιστα, για να επιστήσουμε την προσοχή του ερευνητή αναγράφουμε την λέξη «Υποχρεωτικό» πάνω στο κουμπί ώστε να κατανοήσει ότι οι συλλεχθείσες πληροφορίες, σχετικά με το μητρώο, του υπό μελέτη συστήματος, είναι άκρως απαραίτητες για την μετέπειτα ανάλυση, του κατασχεθέντος συστήματος και συνίσταται λοιπόν η συλλογή αυτών.

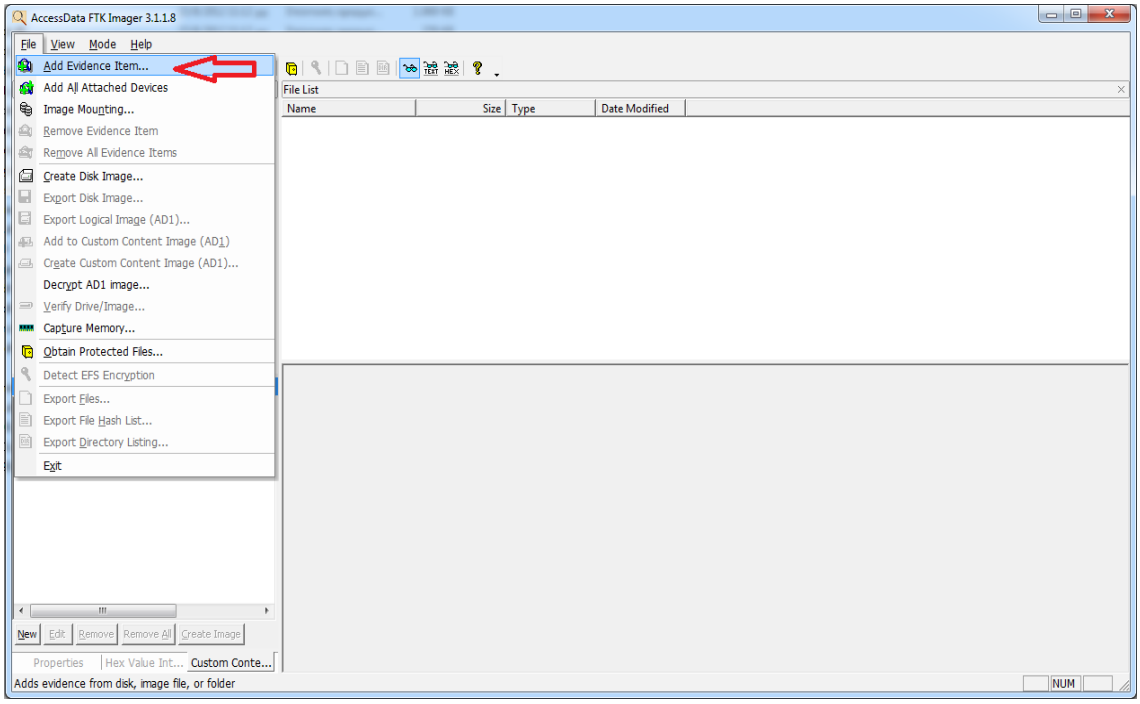
Πατώντας δε στο παραπάνω πλήκτρο, ανοίγει το βοηθητικό εργαλείο «FTK Imager Lite», το οποίο απαιτεί την συνδρομή του ερευνητή. Έτσι, θα πρέπει να ακολουθήσει τα εξής βήματα:

1) Επιλογή της κατηγορίας «File» (με μονό πάτημα του αριστερού πλήκτρου του ποντικιού) που βρίσκεται στην αριστερή πάνω γωνία (Εικόνα 3.3.3.2) με σκοπό να αναδιπλωθεί το παράθυρο επιλογών, καθόσον στο επόμενο βήμα θα επιλέξουμε μία εξ αυτών.



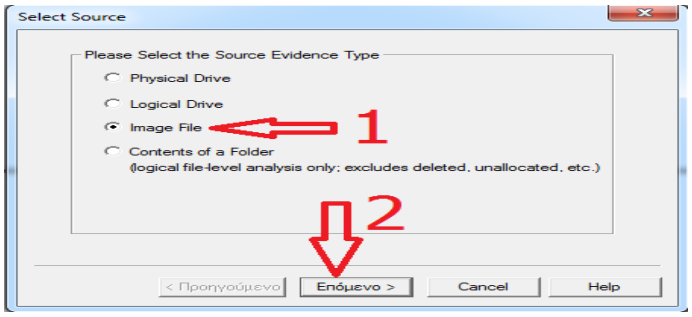
Εικόνα 3.3.3.2: FTK Imager Lite – Βήμα 1

2) Επιλογή της υποκατηγορίας «Add Evidence Item» (με μονό πάτημα του αριστερού πλήκτρου του ποντικιού) (Εικόνα 3.3.3.3) με σκοπό να εμφανιστεί το νέο παράθυρο επιλογών.



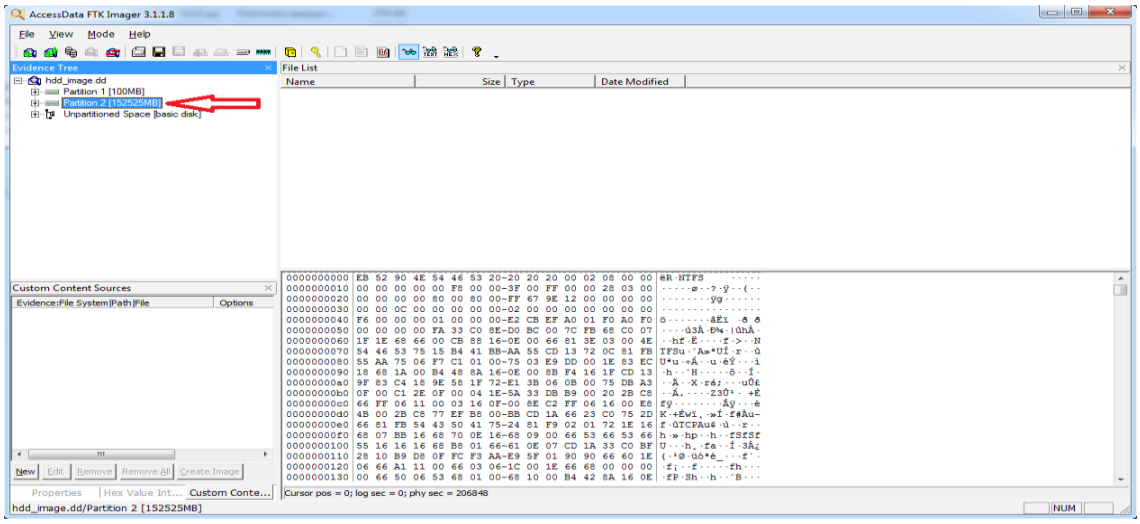
Εικόνα 3.3.3.3: FTK Imager Lite – Βήμα 2

3) Επιλογή από το αναδυόμενο παράθυρο της τρίτης επιλογής που αναγράφει «Image File» και εν συνεχεία, πάτημα του κουμπιού «Επόμενο» (Εικόνα 3.3.3.4).



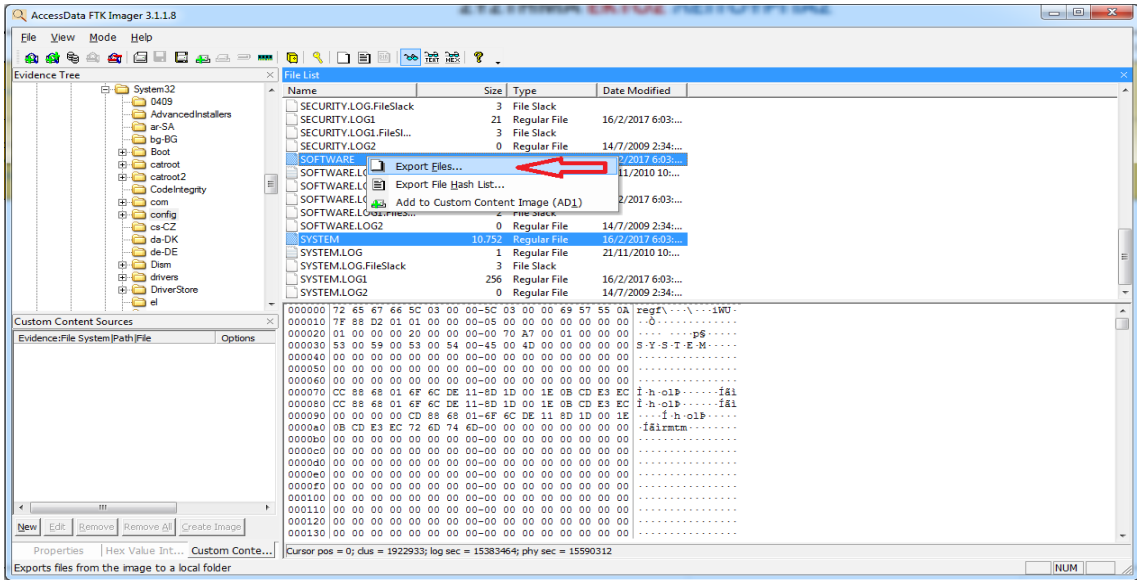
Εικόνα 3.3.3.4: FTK Imager Lite – Βήμα 3

4) Πάτημα του κουμπιού «Browse» και επιλογή του αντιγράφου πρωτεύοντος δίσκου που λάβαμε νωρίτερα (είναι το αρχείο hdd_image.dd και βρίσκεται μέσα στο φάκελο collected_information\hdd\off). Αφού εντοπίσουμε το αρχείο, πατάμε στο κουμπί «Άνοιγμα» και εν συνεχεία, πατάμε στο κουμπί «Finish».
5) Αφού φορτωθεί στο FTK Imager Lite, το αντίγραφο του πρωτεύοντος σκληρού δίσκου, του υπό μελέτη συστήματος, τότε, επιλέγουμε από την αριστερή στήλη, το αρχείο με το όνομα hdd_image.dd με σκοπό να αναδιπλωθεί η λίστα και εν συνεχεία, ο ερευνητής, να επιλέξει τον σκληρό δίσκο, εκείνο με την μεγαλύτερη χωρητικότητα (Εικόνα 3.3.3.5 – στον σκληρό δίσκο που εγκαθίστανται το λειτουργικό σύστημα των windows, δημιουργείται αυτόματα και δεύτερο τμήμα του δίσκου –partition 1- στο οποίο αποθηκεύονται όλα τα βασικά αρχεία των windows σε συμπιεσμένη μορφή και συνήθως έχει χωρητικότητα 100MB).



Εικόνα 3.3.3.5: FTK Imager Lite – Βήμα 5

6) Αφού ο ερευνητής πατήσει στο δίσκο αυτό, επιλέγει το τμήμα αυτού που αναγράφει «NONAME(NTFS)», με σκοπό την εμφάνιση των περιεχομένων του. Έτσι, στην αριστερή στήλη εμφανίζεται ο φάκελος με το όνομα «root», τον οποίο και οφείλει να επιλέξει για να εμφανιστούν τα περιεχόμενά του. Στη συνέχεια, πρέπει να ανοίξει το φάκελο με το όνομα «windows», ώστε να ανοίξει εν συνεχεία, τον φάκελο «system32», που βρίσκεται μέσα σε αυτόν. Σκοπός είναι να εμφανιστεί ο φάκελος με το όνομα «Config», τον οποίο πρέπει να επιλέξει με μονό αριστερό κλικ, ώστε στη δεξιά στήλη να εμφανιστούν τα περιεχόμενα αυτού.
7) Στο σημείο αυτό, θα πρέπει ο ερυενητής, με πατημένο το πλήκτρο «Ctrl» να επιλέξει τα αρχεία default,system,sam,security,software (αυτά που δεν έχουν κατάληξη) με σκοπό, στην συνέχεια, να λάβει αντίγραφα αυτών.
8) Έχοντας επιλεγμένα τα παραπάνω πέντε (5) αρχεία, αρκεί ο χρήστης να πατήσει μονό δεξί κλικ, πάνω σε ένα από αυτά και στην αναδιπλούμενη λίστα που θα εμφανιστεί να επιλέξει το «Export Files» (Εικόνα 3.3.3.6)



Εικόνα 3.3.3.6: FTK Imager Lite – Βήμα 8

9) Τέλος, θα πρέπει να επιλεγεί, από την αναδιπλούμενη λίστα, ο φάκελος στον οποίο θα εισαχθούν αυτές οι πληροφορίες (προτείνεται ο φάκελος collected_information\Registry), ενώ πατώντας στο πλήκτρο «OK», ξεκινάει η λήψη των ψηφιακών πειστηρίων από το Μητρώο (Regsitry), του υπό μελέτη συστήματος.

Βέβαια, όπως παρατηρούμε στην εικόνα 3.3.3.1, το λογισμικό μας, δίνει την δυνατότητα στον ερευνητή να συλλέξει επιπλέον πληροφορίες που σχετίζονται με τον πρωτεύων σκληρό δίσκο (HDD) του κατασχεθέντος εκθέματος. Έτσι, πατώντας στο αντίστοιχο κουτί επιλογής (check box) που βρίσκεται μπροστά από κάθε περιγραφή, μπορούν να συλλεχθούν οι εξής πληροφορίες:

1. Αντιγραφή αρχείου συντομεύσεων και παραπομπών (Shortcut files & Jump lists) στο οποίο διατηρούνται πληροφορίες σχετικές με τα αρχεία και τις εφαρμογές, του υπό μελέτη συστήματος ([30]WikiHow to do anything, 2017):

```
Xcopy όνομα δίσκου\users\ονομα συνδεδεμένου χρηστη\appdata\roaming\microsoft\ windows\ recent\*  όνομα δίσκου\collected_information\hdd\users\ονομα χρηστη\ recent_files /e /i /h
```

2. Αντιγραφή αρχείου μικρογραφιών εικόνων (Thumbnail files) που εμπλουτίζεται κάθε φορά που ο χρήστης ανοίγει μία εικόνα μέσα από το λειτουργικό σύστημα των windows ([30]WikiHow to do anything, 2017):

```
Xcopy όνομα δίσκου\users\ονομα χρηστη\appdata\local\microsoft\ windows\explorer\ thumb*.db όνομα δίσκου\collected_information\hdd\users\ονομα χρηστη\thumbnail_files /e /i /h
```

3. Αντιγραφή των περιεχομένων του κάδου ανακύκλωσης (Recycle Bin) του λειτουργικού συστήματος των windows :

```
Xcopy όνομα δίσκου\$recycle.bin\*.* όνομα δίσκου\collected_information\ hdd\recycle_bin /e /i /h
```

4. Αντιγραφή όλων των αρχείων καταγραφής γεγονότων (Event Logs – Application,Security, Software) του λειτουργικού συστήματος των windows και αποθήκευσής τους με τα ονόματα application_logs.evt, security_logs.evt και system_logs.evt αντίστοιχα ([37]Windows Command Line) - ([55]Microsoft Technet, 2017):

```
Copy γραμμα δισκου\windows\system32/winevt/logs/application.evtx όνομα δίσκου\ collected_information\hdd\application.evtx /v
Wevtutil epl όνομα δίσκου\collected_information\hdd\application.evtx όνομα δίσκου\collected_information\hdd\application_logs.evt /lf:true

Copy γραμμα δισκου\windows\system32/winevt/logs/security.evtx όνομα δίσκου\collected_information\hdd\security.evtx
Wevtutil epl όνομα δίσκου\collected_information\hdd\security.evtx όνομα δίσκου\collected_information\hdd\security_logs.evt /lf:true

Copy γραμμα δισκου\windows\system32/winevt/logs/system.evtx όνομα δίσκου\collected_information\hdd\system.evtx
Wevtutil epl όνομα δίσκου\collected_information\hdd\system.evtx όνομα δίσκου\collected_information\hdd\system_logs.evt /lf:true
```

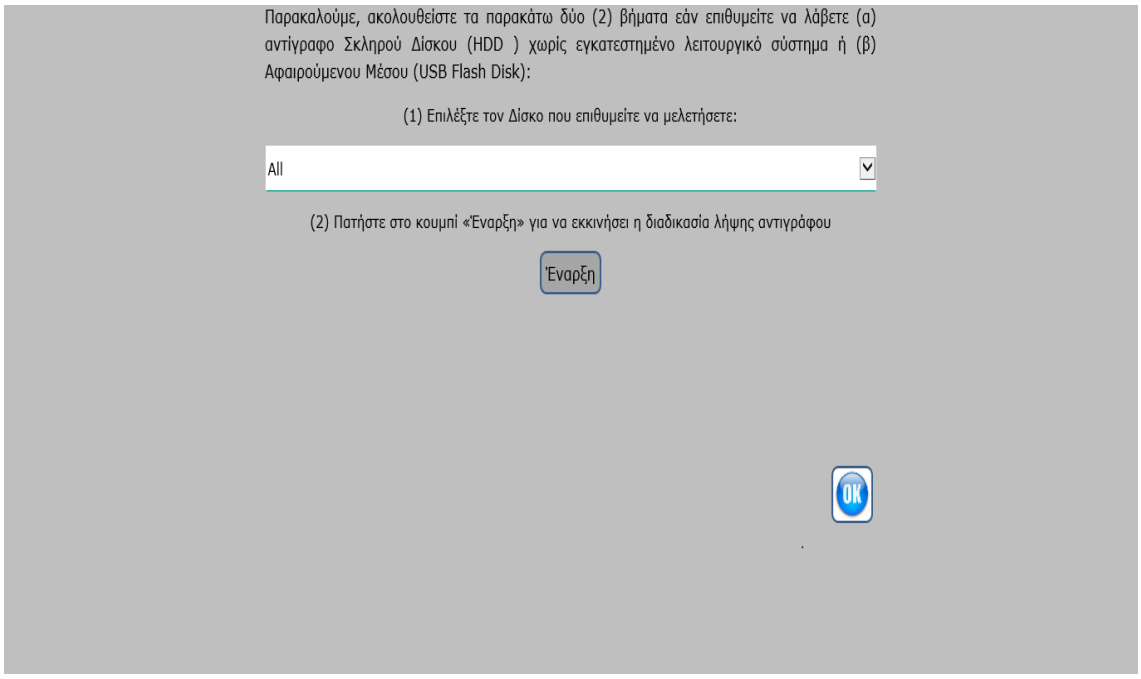
5. Αντιγραφή όλων των αντιγράφων ασφάλειας (Volume Snapshot Service, Volume Shadow Copy Services, VSS) που λήφθηκαν αυτόματα από την εν λόγω δυνατότητα/λογισμικό του λειτουργικού συστήματος των windows και αποθήκευσή τους στο αρχείο volumeshadowcopy.txt ([39]Microsoft TechNet, 2017):

```
Vssadmin list shadows /for=όνομα δίσκου: > όνομα δίσκου\collected_information\hdd\ VolumeShadowCopy.txt
```

3.3.4 Συλλογή Πληροφοριών από αποθηκευτικά μέσα (Hdd – Usb Flash Disks)

Ο ερευνητής, μπορεί κατά την χρονική στιγμή της κατάσχεσης του εκθέματος, να εντοπίσει και τυχόν εξωτερισκούς σκληρούς δίσκους ή κάποια εξωτερικά αποθηκευτικά μέσα (Usb Flash Disks). Επίσης, μπορεί κατά την αποσυναρμολόγηση του εκθέματος, να εντοπίσει περισσότερους από έναν σκληρό δίσκο (Hdd) εγκατεστημένους, οι οποίοι να αποτελούν όμως απλά αποθηκευτικό μέσο.

Σε κάθε μία από τις παραπάνω περιπτώσεις, ο ερευνητής, αρχικά, θα πρέπει να συνδέσει στον ηλεκτρονικό του υπολογιστή ή στο σύστημα που τρέχει την εφαρμογή μας, τα εξωτερικά αυτά αποθηκευτικά μέσα, μέσω «usb» σύνδεσης και στη συνέχεια, να πατήσει στο κουμπί «Αντίγραφο Δίσκου (Hdd/Usb Flash Disk)», προκειμένου τη λήψη αντιγράφων αυτών. Πατώντας δε στο κουμπί, αυτόματα, θα ανοίξει η κάτωθι σελίδα (Εικόνα 3.3.4.1):



Εικόνα 3.3.4.1: Λήψη Αντίγραφου Δίσκου (HDD/USB Flash Disk)

Στο σημείο αυτό, ο ερευνητής, θα πρέπει να επιλέξει από τη λίστα, το αποθηκευτικό μέσο, του οποίου επιθυμεί να λάβει αντίγραφο. Η λίστα αυτή δημιουργείται αυτόματα, εξαιρώντας τον πρωτεύων σκληρό δίσκο του συστήματος, του ερευνητή και τα τυχόν εγκατεστημένα οπτικά μέσα αυτού, τρέχοντας την κάτωθι εντολή κονσόλας ([27]NirSoft, 2011-2016):

```
Driveletterview /stext όνομα δίσκου\collected_information\hdd\usb.txt
```

Τα αποθηκευτικά μέσα (Usb flash Disks), συνήθως είναι διαμορφωμένα ως «FAT32» και όχι ως «NTFS» για το λόγο αυτό, όταν ο ερευνητής επιλέξει από τη λίστα μία τέτοια συσκευή και πατήσει στο κουμπί «Έναρξη», αυτόματα, θα τρέξει η εντολή κονσόλας (για την σύνταξη της οποίας χρησιμοποιούμε το περιεχόμενο του πεδίου **Drive Name** από το αρχείο usb.txt) ([18]Crysocome, 2010):

```
DD if=\\.\γραμμα  usb flash disk: of=όνομα δίσκου\collected_information\USB\drive name _image.dd bs=1440k
```

Αν όμως, η επιλεχθείσα συσκευή, είναι ένας σκληρός δίσκος (Hdd) χωρίς εγκατεστημένο λειτουργικό σύστημα (άρα είναι διαμορφωμένος ως NTFS), τότε, δεν τρέχει η προηγούμενη

εντολή κονσόλας, αλλά εκτελείται η εξής εντολή (για τη δε σύνταξη αυτή και πάλι χρησιμοποιούμε το περιεχόμενο του πεδίου **Drive Name** από το αρχείο usb.txt) ([18]Crysocome, 2010):

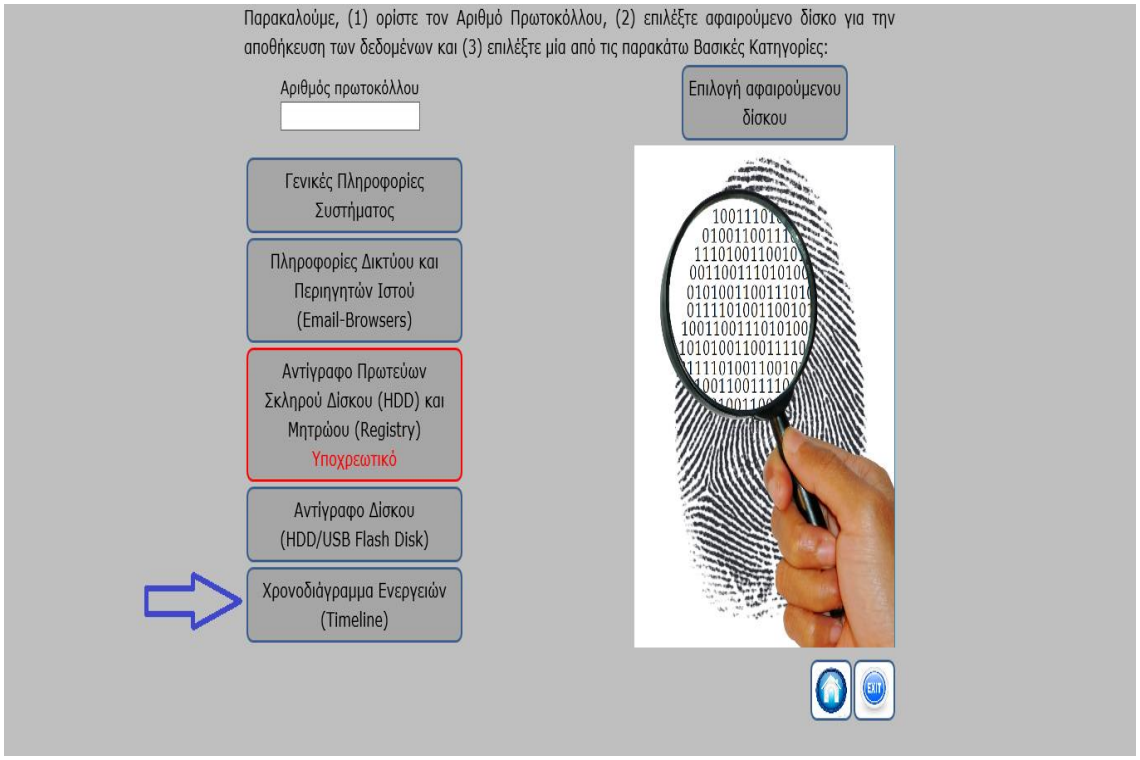
```
DD if=\\.\γραμμα δισκου: of=όνομα δίσκου\collected_information\hdd\OFF\hdd_image.dd
bs=1440k
```

Παρατηρούμε δε ότι, το αντίγραφο των εξωτερικών αποθηκευτικών μέσων (Usb Flash Disks) αποθηκεύνται μέσα στο φάκελο «USB», ενώ το αντίγραφο ενός σκληρού δίσκου, αποθηκεύεται στο φάκελο «Hdd\OFF». Τέλος, δεν πρέπει να παραλείψουμε να αναφέρουμε ότι, εάν τα μέσα αυτά που επιθυμεί ο ερευνητής να λάβει αντίγραφό τους, είναι περισσότερα του ενός, τότε θα πρέπει να επαναλάβει την ανωτέρω διαδικασία για κάθε ένα από αυτά, ξεχωριστά.

3.3.5 Συλλογή Χρονοδιαγράμματος Ενεργειών (TimeLine)

Όταν ο ερευνητής, πατήσει στο κουμπί «Χρονοδιάγραμμα Ενεργειών (Timeline)», (Εικόνα 3.3.5.1), τότε, αυτόματα, γίνεται ένας έλεγχος εάν έχει ληφθεί πλήρες αντίγραφο του Πρωτεύοντος Σκληρού Δίσκου(HDD) και του Μητρώου (Registry) ή όχι. Ο λόγος που δεν βάλαμε το λογισμικό μας, να λάβει αντίγραφο του χρονοδιαγράμματος αυτού, αυτόματα, είναι διότι, η διαδικασία αυτή διαρκεί πάρα πολύ. Οπότε, κατά την ανάλυση του Χρονοδιαγράμματος Ενεργειών (παράγραφος 4.3.7) θα παρατηρήσουμε ότι γίνεται ταυτόχρονα η συλλογή και η ανάλυση του χρονοδιαγράμματος αυτού (εξοικονόμηση χρόνου).

Εάν στο υπό μελέτη σύστημα, έχει ληφθεί αντίγραφο Πρωτεύοντος Σκληρού Δίσκου (άρα έχει δημιουργηθεί το αρχείο hdd.vhdx ή hdd.vpc μέσα στο φάκελο hdd\off), θα εμφανιστεί μήνυμα στην οθόνη που θα αναγράφει ότι δεν απαιτούνται περαιτέρω ενέργειες. Ενώ, εάν δεν έχει ληφθεί το σχετικό αντίγραφο, τότε, το μήνυμα θα διαφέρει και θα παραπέμπει τον ερευνητή στη λήψη του αντιγράφου αυτού (βλέπε υποκεφάλαιο 3.3.3).



Εικόνα 3.3.5.1: Συλλογή Χρονοδιαγράμματος Ενεργειών (TimeLine)

Στο σημείο αυτό, ολοκληρώνεται η διαδιακασία λήψης ψηφιακών πειστηρίων από ένα απενεργοποιημένο σύστημα και αρκεί ο ερευνητής να πατήσει, είτε στο κουμπί «Home», είτε στο κουμπί «Exit». Και στις δύο (2) περιπτώσεις, θα ελέγχονται οι διεργασίες του συστήματος με σκοπό να βρεθεί εάν εκκρεμεί κάποια διεργασία σχετιζόμενη με τις εντολές κονσόλας (command lines), εμφανίζοντας σχετικό μήνυμα περί μη ολοκλήρωσης των διαδικασιών που ζητήθηκαν.

Μετά το πέρας αυτών των διεργασιών, αυτόματα, η εφαρμογή δημιουργεί και συμπληρώνει τμήμα της αναφορικής έκθεσης (που θα περιγραφεί στο κεφάλαιο 5).

3.4 Ανασκόπηση Κεφαλαίου 3

Το κεφάλαιο 3, περιέχει την πλήρη περιγραφή των μεθόδων που πρέπει να ακολουθήσει ο τεχνικός εγκληματολογικής έρευνας, προκειμένου την συλλογή ψηφιακών πειστηρίων, τόσο από ενεργοποιημένο σύστημα, όσο και από απενεργοποιημένο σύστημα.

Διαχωρίστηκαν δε αυτές οι δύο (2) καταστάσεις, καθόσον οι πληροφοριές που μπορούν να συλλεχθούν από ένα απενεργοποιημένο έκθεμα είναι σαφώς πολύ λιγότερες σε πλήθος, από εκείνες που θα συλλεχθούν εάν το σύστημα είχε βρεθεί ενεργοποημένο. Σε κάθε περίπτωση όμως, δεν αρκεί μόνο η συλλογή αυτών, αλλά απαιτείται και η διεξοδική ανάλυσή τους, προκειμένου την εξαγωγή ασφαλών συμπερασμάτων περί τέλεσης ή μη αξιόποινης πράξης.

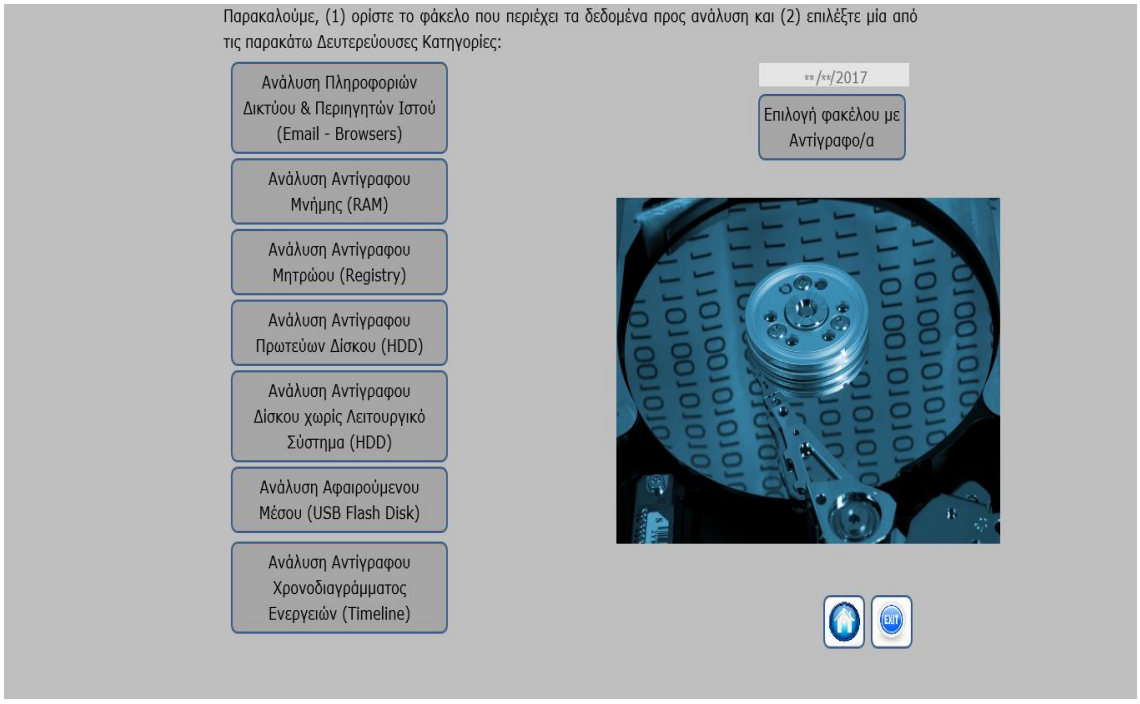
Έτσι, ακολουθεί η ανάλυση των συλλεχθέντων πληροφοριών σε κάθε μία, από τις δύο (2) προαναφερθείσες περιπτώσεις.

ΚΕΦΑΛΑΙΟ 4 – ΑΝΑΛΥΣΗ ΣΥΛΛΕΧΘΕΝΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

4.1 Εισαγωγή

Στο κεφάλαιο αυτό, θα περιγράψουμε τον τρόπο με τον οποίο αναλύονται οι συλλεχθείσες πληροφορίες, είτε το υπό μελέτη σύστημα βρέθηκε ενεργοποιημένο, είτε βρέθηκε απενεργοποιημένο, κατά τη χρονική στιγμή της κατάσχεσής του.

Ξεκινώντας την διαδικασία, ο τεχνικός της ψηφιακής εγκληματολογικής έρευνας θα πρέπει να πατήσει, στην αρχική σελίδα, το κουμπί «Ανάλυση Πληροφοριών», με σκοπό να ανοίξει η παρακάτω σελίδα (Εικόνα 4.1.1):



Εικόνα 4.1.1: Ανάλυση Συλλεχθέντων Πληροφοριών

Στο σημείο αυτό, ο χρήστης του λογισμικού καλείται να επιλέξει το φάκελο στον οποίο έχουν αποθηκευτεί τα στοιχεία που έλαβε. Πατώντας, πάνω στο κουμπί «Επιλογή φακέλου με Αντίγραφο/α», ανοίγει μια αναδιπλούμενη λίστα από την οποία θα πρέπει να ορίσει το σκληρό δίσκο που περιέχει τα συλλεχθέντα δεδομένα και εν συνεχεία, να ορίσει, με βάση τον αριθμό πρωτοκόλλου, το φάκελο που περιέχει τα ψηφιακά πειστήρια της συγκεκριμένης υπόθεσης που θα αναλύσει (ο φάκελος αυτός βρίσκεται μέσα στη διαδρομή «όνομα δίσκου\Windows Forensics\Protocols»).

Τέλος, καλείται να επιλέξει το είδος των πληροφοριών που επιθυμεί να αναλύσει, πατώντας σε ένα από τα κουμπιά. Μετά το πέρας της διαδιακασίας ανάλυσης, ο χρήστης μπορεί, είτε να επιστρέψει στην αρχική σελίδα πατώντας στο κουμπί «Home», είτε να τερματίσει την εφαρμογή μας, πατώντας στο κουμπί «Exit». Σε κάθε περίπτωση, θα συμπληρωθούν αυτόματα τα αντίστοιχα πεδία του πίνακα, ο οποίος και θα εισαχθεί στην τελική αναφορική έκθεση ψηφιακών πειστηρίων (περιγράφεται στο κεφάλαιο 5), κάποια πεδία (Εικόνα 3.1.2) τα οποία θα εισαχθούν αργότερα (αυτόματα) στην αναφορική έκθεση (Κεφάλαιο 5).

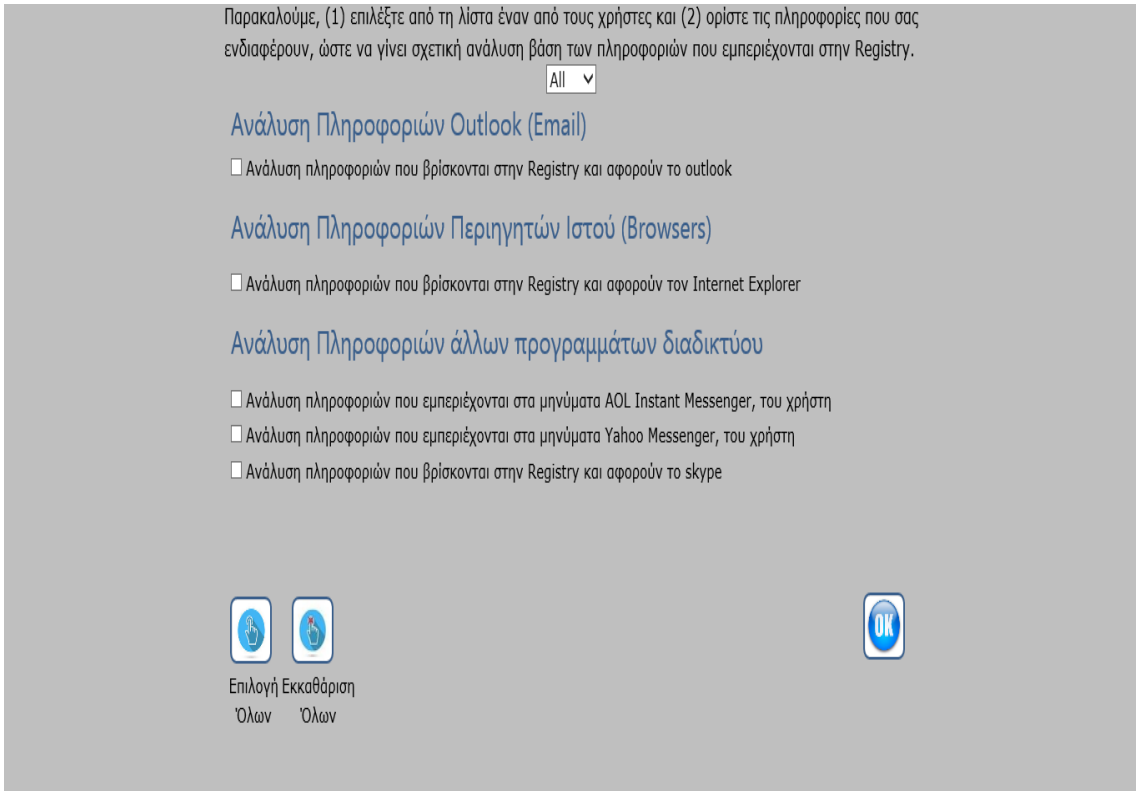
4.2 Ανάλυση Πληροφοριών από Ενεργοποιημένο Σύστημα

Μόλις ο αναλυτής πατήσει σε κάποιο από τα κουμπιά, με σκοπό την ανάλυση των αντίστοιχων πληροφοριών, η εφαρμογή, αυτόματα, αναζητάει στο φάκελο που όρισε ο αναλυτής (παράγραφος 4.1), εάν υπάρχει ο υποφάκελος με το όνομα «ON», μέσα στο φάκελο με το όνομα «HDD», των αντίστοιχων συλλεχθέντων πληροφοριών.

Σε περίπτωση που υπάρχει, τότε, αναζητάει στο εσωτερικό αυτού, με σκοπό να βρεί εάν υπάρχει περιεχόμενο αρχείο. Εάν υπάρχει, αυτό συνεπάγεται ότι τα δεδομένα που έχουν συλλεχθεί, είναι από ένα σύστημα που βρέθηκε ενεργοποιημένο κατά την κατάσχεσή του. Κατά συνέπεια, ο αναλυτής, κάθε φορά που θα πατάει σε ένα από τα κουμπιά που θα περιγράψουμε παρακάτω στις παραγράφους 4.2.1 έως και 4.2.7, θα αφορούν ενεργοποιημένο σύστημα. Σε διαφορετική περίπτωση (Παράγραφος 4.3), θα αφορούν απενεργοποιημένο σύστημα και θα δίνονται διαφορετικές δυνατότητες ανάλυσης (περιγράφονται στις παραγράφους 4.3.1 έως και 4.3.6) στον τεχνικό ψηφιακών πειστηρίων.

4.2.1 Ανάλυση Πληροφοριών Δικτύου & Περιηγητών Ιστού (Email - Browsers)

Η πρώτη δυνατότητα που δίνεται, είναι η ανάλυση των πληροφοριών που συλλέχθηκαν και έχουν σχέση, είτε με το δίκτυο, είτε με τους Περιηγητές Ιστού που χρησιμοποιούσε ο χρήστης, του υπό μελέτη συστήματος. Έτσι, πατώντας στο κουμπί «Ανάλυση Πληροφοριών Δικτύου & Περιηγητών Ιστού (Email - Browsers)», ανοίγει η κάτωθι σελίδα (Εικόνα 4.2.1.1).



Εικόνα 4.2.1.1: Ανάλυση Πληροφοριών Δικτύου & Περιηγητών Ιστού (Ενεργοποιημένο Σύστημα)

Με το άνοιγμα της σελίδας αυτής, γίνοται ταυτόχρονα δύο (2) ενέργειες:

α) Αντιγράφει όλα τα περιεχόμενα των υποφακέλων collected_information\Browsers και collected_information\Email, στους αντίστοιχους υποφακέλους μέσα στο φάκελο annalized_information, εκτελώντας την κάτωθι εντολή κονσόλας:

```
Copy όνομα δίσκου\collected_information\Browsers\*.* όνομα δίσκου\analyzed_information\ Browsers

Copy όνομα δίσκου \collected_information\Email\*.* όνομα δίσκου\analyzed_information\ Email
```

και (β) ελέγχει εάν υπάρχει περιεχόμενο αρχείο, στο φάκελο με το όνομα «Registry», διότι, για την ανάλυση των πληροφοριών που δίνονται στην κατηγορία αυτή, απαιτείται πρωταρχικά να έχει ληφθεί σχετικό αντίγραφο του Μητρώου (Registry). Στην περίπτωση που δεν έχει ληφθεί, εμφανίζεται σχετικό μήνυμα που παραπέμπει τον αναλυτή, στην αντίστοιχη ενέργεια.

Επειδή, σε ένα ενργοποιημένο σύστημα, συνήθως υπάρχουν περισσότεροι, του ενός, εγκατεστημένοι χρήστες, γι' αυτό, ο αναλυτής καλείται να επιλέξει αρχικά ποιος χρήστης, του υπό μελέτη συστήματος, τον ενδιαφέρει. Στην αναδιπλούμενη λίστα, δίνεται η δυνατότητα επιλογής, όχι μόνο ενός συγκεκριμένου χρήστη, αλλά επιλέγοντας την κατηγορία «ALL», μπορεί ταυτόχρονα να μελετήσει όλους τους χρήστες, του συστήματος αυτού.

Στην συνέχεια, θα πρέπει να επιλέξει τις επιμέρους πληροφορίες που τον ενδιαφέρουν κάνοντας μονό αριστερό κλικ, στο αντίστοιχο κουτί επιλογής (check box) που βρίσκεται μπροστά από κάθε περιγραφή. Οι πληροφορίες αφορούν, αρχικά τα ηλεκτρονικά μηνύματα (email) του χρήστη/χρηστών, του υπό μελέτη συστήματος. Έτσι, πατώντας στο κουτί επιλογής (check box), που βρίσκεται μπροστά από την έκφραση «Ανάλυση πληροφοριών που βρίσκονται στην Registry και αφορούν το outlook», αυτόματα, ξεκινάει η αντίστοιχη διαδικασία τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα outlook_registry_analysis.txt ([20] RegRipper, 2015):

```
Copy όνομα δισκου:\collected_information\Email\*.* όνομα δίσκου\analyzed_information\ Email

Rip –r όνομα δισκου:\collected_information\Registry\software –p outlook > όνομα δίσκου\analyzed_information\ Email\outlook_registry_analysis.txt
```

Σε περίπτωση που ο αναλυτής επιλέξει την «Ανάλυση πληροφοριών που βρίσκονται στην Registry και αφορούν τον Internet Explorer» τότε, τρέχει η παρακάτω εντολή κονσόλας και αποθηκεύονται τα αποτελέσματα στα αρχεία με τα ονόματα registry_analysis_internet_explorer.txt και registry_analysis_internet_settings.txt ([20] RegRipper, 2015):

```
Rip –r όνομα δισκου:\collected_information\Registry\Users\όνομα χρήστη\ntuser.dat –p internet_explorer_cu > όνομα δίσκου\analyzed_information\Browsers\ όνομα χρήστη\registry_analysis_internet_explorer.txt

Rip –r όνομα δισκου:\collected_information\Registry\Users\όνομα χρήστη\ntuser.dat –p internet_settings_cu > όνομα δίσκου\analyzed_information\Browsers\ όνομα χρήστη\registry_analysis_internet_settings.txt
```

Φυσικά, ο αναλυτής μπορεί να αναλύσει, εάν επιθυμεί και τις πληροφορίες που σχετίζονται με άλλα προγράμματα του διαδικτύου (internet), όπως το Skype, το Yahoo Messenger και το AOL Instant Messenger, που χρησιμοποιεί ο χρήστης, του υπό μελέτη συστήματος, προκειμένου να επικοινωνήσει με άλλους χρήστες του διαδικτύου (σχετικά με το πρόγραμμα Facebook και Viber γίνεται αναφορά στην παράγραφο 6.2). Έτσι, πιο συγκεκριμένα, εάν ο αναλυτής επιλέξει την «Ανάλυση πληροφοριών που βρίσκονται στην Registry και αφορούν το Skype», τότε, τρέχει η παρακάτω εντολή κονσόλας και αποθηκεύονται τα αποτελέσματα στο αρχείο με το όνομα skype_registry_analysis.txt ([20] RegRipper, 2015):

```
Copy όνομα δισκου:\collected_information\Browsers\skype_history.txt όνομα δίσκου\ analyzed_information\Browsers

Rip –r όνομα δισκου:\collected_information\Registry\Users\όνομα χρήστη\ntuser.dat –p skype > όνομα δίσκου\analyzed_information\ Browsers\όνομα χρήστη\ skype_registry_analysis.txt
```

Αν επιλέξει, την «Ανάλυση πληροφοριών που εμπεριέχονται στα μηνύματα AOL INSTANT Messenger, του χρήστη», τότε, τρέχει η παρακάτω εντολή κονσόλας και αποθηκεύονται τα αποτελέσματα στο αρχείο με το όνομα aol_instant_messenger.txt ([20] RegRipper, 2015):

```
Rip –r όνομα δισκου:\collected_information\Registry\Users\όνομα χρήστη\ntuser.dat –p aim > όνομα δίσκου\analyzed_information\ Browsers\όνομα χρήστη\ aol_instant_messenger.txt
```

Ενώ, αν επιλέξει, την «Ανάλυση πληροφοριών που εμπεριέχονται στα μηνύματα Yahoo Messenger, του χρήστη», τότε, τρέχει η παρακάτω εντολή κονσόλας και αποθηκεύονται τα αποτελέσματα στα αρχεία με τα ονόματα yahoo_cu.txt, yahoo_lm.txt και yahoo_messenger.txt ([20] RegRipper, 2015):

```
Rip –r όνομα δισκου:\collected_information\Registry\Users\όνομα χρήστη\ntuser.dat –p yahoo_cu > όνομα δίσκου\analyzed_information\Browsers\όνομα χρήστη\ yahoo_cu.txt

Rip –r όνομα δισκου:\collected_information\Registry\Users\όνομα χρήστη\ntuser.dat –p yahoo_lm > όνομα δίσκου\analyzed_information\Browsers\όνομα χρήστη\ yahoo_lm.txt

Copy όνομα δισκου:\collected_information\Registry\όνομα χρήστη\yahoo_cu.txt + όνομα δισκου:\collected_information\Registry\όνομα χρήστη\yahoo_lm.txt όνομα δίσκου\analyzed_
information\Browsers\όνομα χρήστη\ yahoo_messenger.txt
```

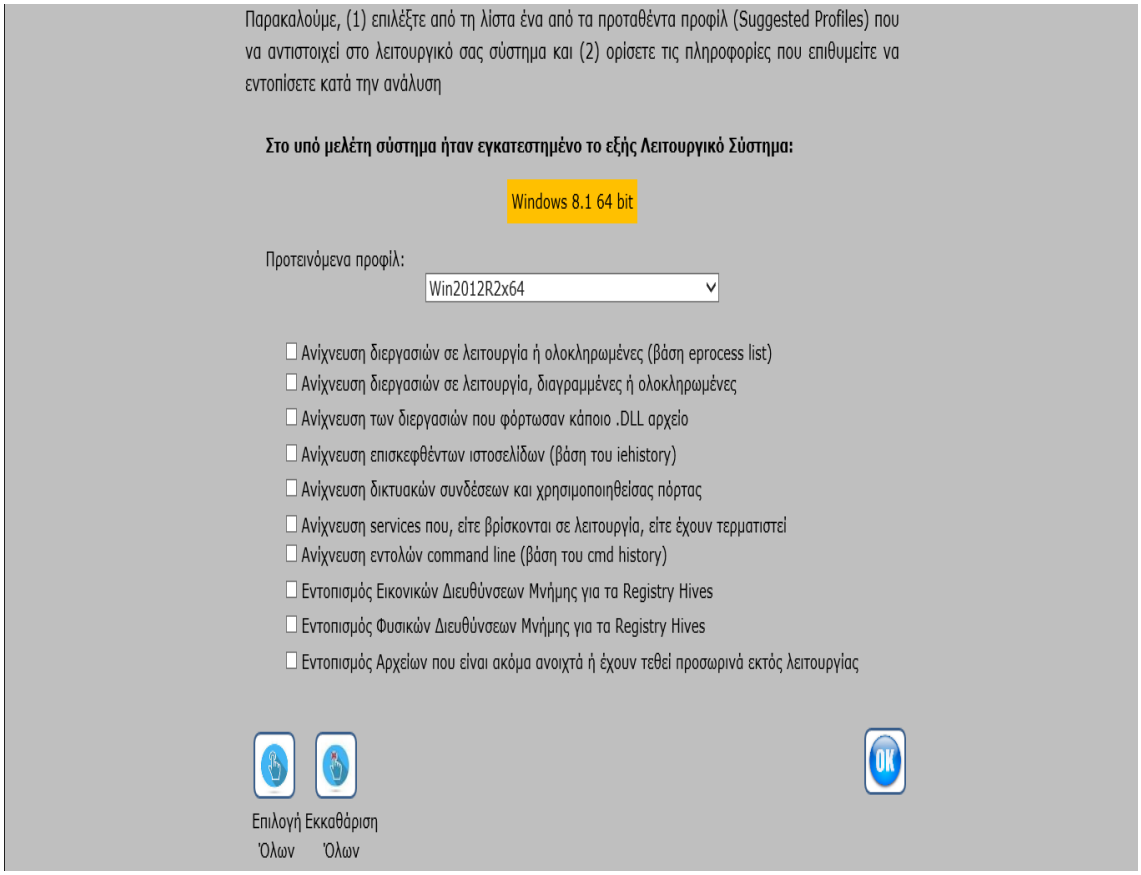
Τέλος, σε περίπτωση που ο αναλυτής επιθυμεί να λάβει γνώση για όλα τα αναγραφόμενα, τότε, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων», που βρίσκεται στο κάτω μέρος της οθόνης. Μάλιστα, στην περίπτωση που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών αυτών και θέλει μόνο την ανάλυση ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν.

Σε κάθε περίπτωση όμως, μετά το πέρας των παραπάνω ενεργειών, αρκεί να πατήσει στο κουμπί «OK», με σκοπό την έξοδό του, από την κατηγορία αυτή. Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη των αντίστοιχων εντολών κονσόλας (command line) που εκτελούνται και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτών.

4.2.2 Ανάλυση Αντίγραφου Μνήμης (Ram)

Η επόμενη δυνατότητα που δίνεται στον τεχνικό ψηφιακών πειστηρίων, είναι η ανάλυση του αντιγράφου του μνήμης, που λήφθηκε όταν το υπο κατάσχεση σύστημα βρέθηκε ενεργοποιημένο.

Θα πρέπει λοιπόν ο τεχνικός να πατήσει στο κουμπί «Ανάλυση Αντιγράφου Μνήμης (RAM)» με σκοπό να του ανοίξει η επόμενη σελίδα (Εικόνα 4.2.2.1).



Εικόνα 4.2.2.1: Ανάλυση Αντιγράφου Μνήμης (RAM) από Ενεργοποιημένο Σύστημα

Με το άνοιγμα της σελίδας αυτής, καλείται ο αναλυτής να επιλέξει από την αναδυόμενη λίστα το λειτουργικό σύστημα των Windows, που ήταν εγκατεστημένο, στο υπό μελέτη σύστημα. Τα προφίλ (Suggested Profiles) που εμφανίζονται στην λίστα αυτή, είναι προτεινόμενα (αρχείο με το όνομα analyzed_information\ram\profiles.dmp) με βάση τις πληροφορίες που προκύπτουν από την εκτέλεση της κάτωθι εντολής κονσόλας ([53]Volatility-GitHub, 2017):

```
Volatility imageinfo όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp > όνομα δίσκου\analyzed_information\Ram\ volatility_profile.txt
```

Για την αποφυγή λανθασμένης επιλογής, από τον αναλυτή, εκτελούμε τις κάτωθι εντολές κονσόλας (command line) με σκοπό να παρουσιάσουμε στο πεδίο «Εγκατεστημένο Λειτουργικό Σύστημα» την ακριβής έκδοση του Λειτουργικού Συστήματος των Windows (που ήταν εγκατεστημένο, στο υπό μελέτη σύστημα, κατά τη χρονική στιγμή συλλογής των ψηφιακών πειστηριών), την οποία και θα πρέπει να συμβουλευτεί ο αναλυτής, με σκοπό την ορθή επιλογή ([20] RegRipper, 2015) :

```
Rip -r όνομα δισκου:\collected_information\Registry\software -p winnt_cv > όνομα δισκου\analyzed\ονομα αρχειου.txt

Type όνομα δισκου\analyzed\ονομα αρχειου.txt | findstr "ProductName" > όνομα δισκου\analyzed\ονομα αρχειου.txt & Type όνομα δισκου\analyzed\ονομα αρχειου.txt | findstr "BuildLabEx" >> όνομα δισκου\windows_version.txt
```

Στη συνέχεια, θα πρέπει να επιλέξει, πατώντας μονό αριστερό κλικ, στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την εκάστοτε έκφραση, με σκοπό να ανιχνευθούν και να αναλυθούν οι πληροφορίες που σχετίζονται με όσα αναγράφονται σε κάθε επιλογή. Πατώντας στην «Ανίχνευση διεργασιών σε λειτουργία ή ολοκληρωμένες (βάση eprocess list)», αυτόματα, ξεκινάει η αντίστοιχη διαδικασία, τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα pslist.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ pslist > όνομα δίσκου\analyzed_information\Ram\pslist.txt
```

Επιλέγοντας την «Ανίχνευση διεργασιών σε λειτουργία,διεγραμμένες ή ολοκληρωμένες», τρέχει, η αντίστοιχη εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο psscan.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ psscan > όνομα δίσκου\analyzed_information\Ram\psscan.txt
```

Πατώντας στο «Ανίχνευση διεργασιών που φόρτωσαν κάποιο .DLL αρχείο» ξεκινάει η διαδικασία, αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα dlllist.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ dlllist > όνομα δίσκου\analyzed_information\Ram\dlllist.txt
```

Αντίστοιχα, για την «Ανίχνευση επισκεφθέντων ιστοσελίδων (βάση του iehistory)» τα αποτελέσματα αποθηκεύονται στο iehistory.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ iehistory > όνομα δίσκου\analyzed_information\Ram\iehistory.txt
```

Επιλέγοντας την «Ανίχνευση δικτυακών συνδέσεων και χρησιμοποιηθείσας πόρτας» τα αποτελέσματα θα αποθηκευτούν στο αρχείο με το όνομα netscan.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ netscan > όνομα δίσκου\analyzed_information\Ram\netscan.txt
```

Πατώντας στην επιλογή «Ανίχνευση services που, είτε βρίσκονται σε λειτουργία, είτε έχουν τερματιστεί», τρέχει η παρακάτω εντολή κονσόλας και τα αποτελέσματα αποθηκεύονται στο αρχείο με το όνομα svcscan.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ svcscan > όνομα δίσκου\analyzed_information\Ram\svcscan.txt
```

Αντίστοιχα, για την «Ανίχνευση εντολών command line (βάση cmd history)» τα αποτελέσματα θα αποθηκευτούν στο αρχείο με το όνομα cmdscan.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ cmdscan > όνομα δίσκου\analyzed_information\Ram\cmdscan.txt
```

Από την επιλογή «Εντοπισμός Εικονικών Διευθύνσεων Μνήμης και Registry Hives» μπορούν να ληφθούν εξίσου σημαντικές πληροφορίες οι οποίες θα αποθηκευτούν στο αρχείο hivelist.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ hivelist > όνομα δίσκου\analyzed_information\Ram\hivelist.txt
```

Ενώ, από την επιλογή «Εντοπισμός Φυσικών Διευθύνσεων Μνήμης και Registry Hives» τα αποτελέσματα θα αποθηκευτούν στο αρχείο με το όνομα hivescan.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ hivescan > όνομα δίσκου\analyzed_information\Ram\hivescan.txt
```

Τέλος, επειδή το σύστημα είχε βρεθεί ενεργοποιημένο, μπορούν να ανιχνευθούν και πληροφορίες με αρχεία που ήταν ανοικτά ή προσωρινά εκτός λειτουργίας, κατά την χρονική στιγμή κατάσχεσης του συστήματος. Αρκεί λοιπόν να πατήσει στην επιλογή «Εντοπισμός Αρχείων που είναι ακόμα ανοικτά ή έχουν τεθεί προσωρινά εκτός λειτουργίας» και τα αποτελέσματα της ενέργειας αυτής θα αποθηκευτούν στο αρχείο με το όνομα filescan.txt ([53]Volatility-GitHub, 2017):

```
Volatility -f όνομα δισκου:\collected_information\Ram\όνομα αρχείου.dmp –profile=επιλεχθέν προφίλ filescan > όνομα δίσκου\analyzed_information\Ram\filescan.txt
```

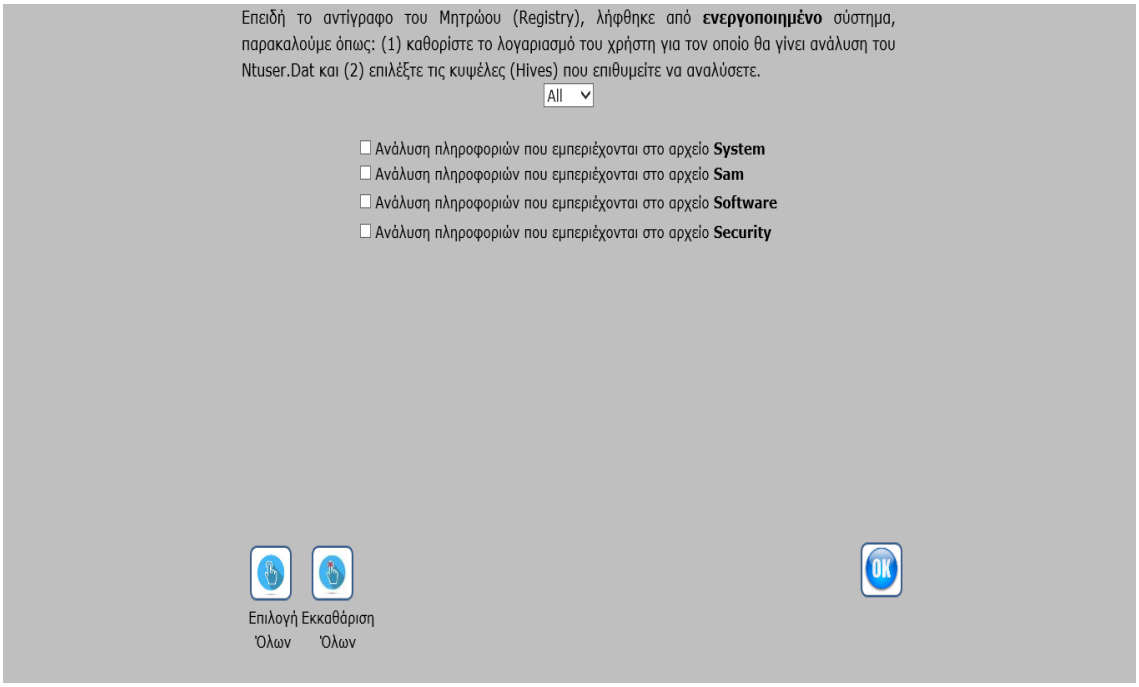
Μάλιστα, σε περίπτωση που ο αναλυτής επιθυμεί να λάβει γνώση για όλα τα παραπάνω, τότε, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων», που βρίσκεται στο κάτω μέρος της οθόνης. Σε περίπτωση δε που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών αυτών και θέλει μόνο την ανάλυση ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν.

Σε κάθε περίπτωση όμως, μετά το πέρας των παραπάνω ενεργειών, αρκεί να πατήσει στο κουμπί «OK», με σκοπό την έξοδό του, από την κατηγορία αυτή. Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη των αντίστοιχων εντολών κονσόλας (command line) που εκτελούνται και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτών.

4.2.3 Ανάλυση Αντίγραφου Μητρώου Συστήματος (Registry)

Το λογισμικό μας, στο σημείο αυτό, παρέχει τη δυνατότητα στον τεχνικό ψηφιακών πειστηρίων, να αναλύσει το αντίγραφο του Μητρώου (Registry) του λειτουργικού συστήματος, που ήταν εγκατεστημένο στο κατασχεθέν ηλεκτρονικό υπολογιστή. Φυσικά, η ανάλυση αυτή, στηρίζεται εξ ολοκλήρου στο αντίγραφο που λήφθηκε και όχι στο αντίγραφο του πρωτεύοντος δίσκου, στο οποίο όπως θα αναφέρουμε πιο κάτω, στηρίζεται η ανάλυση του μητρώου, σε περίπτωση που το υπό μελέτη σύστημα, βρέθηκε απενεργοποιημένο, κατά την χρονική στιγμή της κατάσχεσής του.

Πατώντας, στο κουμπί «Ανάλυση Αντιγράφου Μητρώου (Registry)», ανοίγει η επόμενη σελίδα (Εικόνα 4.2.3.1), στην οποία αρχικά ο αναλυτής θα πρέπει να επιλέξει από την αναδυόμενη λίστα, τον χρήστη που επιθυμεί να μελετήσει. Μάλιστα, στην περίπτωση που επιθυμεί να αναλύσει τα δεδομένα όλων των χρηστών, που χρησιμοποιούσαν το υπό μελέτη σύστημα, τότε, αρκεί να επιλέξει την κατηγορία «ALL».



Εικόνα 4.2.3.1: Ανάλυση Αντιγράφου Μητρώου (Registry) από Ενεργοποιημένο Σύστημα

Επόμενο βήμα, είναι η επιλογή των συγκεκριμένων πληροφοριών που τον ενδιαφέρουν από τις κυψέλες (Hives) του Μητρώου (Registry). Πατώντας μονό αριστερό κλικ, στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την εκάστοτε έκφραση, ανιχνεύονται και αναλύονται οι αντίστοιχες πληροφορίες. Αν, για παράδειγμα, επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **System**», αυτόματα, ξεκινάει η αντίστοιχη διαδικασία τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα system_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\sysem –f system > όνομα δίσκου\analyzed_information\Registry\system_analysis.txt
```

Στην περίπτωση που επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Sam**», τότε, αυτόματα, θα εκκινήσει η αντίστοιχη διαδικασία εκτελώντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα sam_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\sam –f sam > όνομα δίσκου\analyzed_information\Registry\sam_analysis.txt
```

Κατά αντίστοιχο τρόπο, εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Software»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας και θα αποθηκευτούν τα αποτελέσματα στο αρχείο με το όνομα software_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\software –f software > όνομα δίσκου\analyzed_information\Registry\software_analysis.txt
```

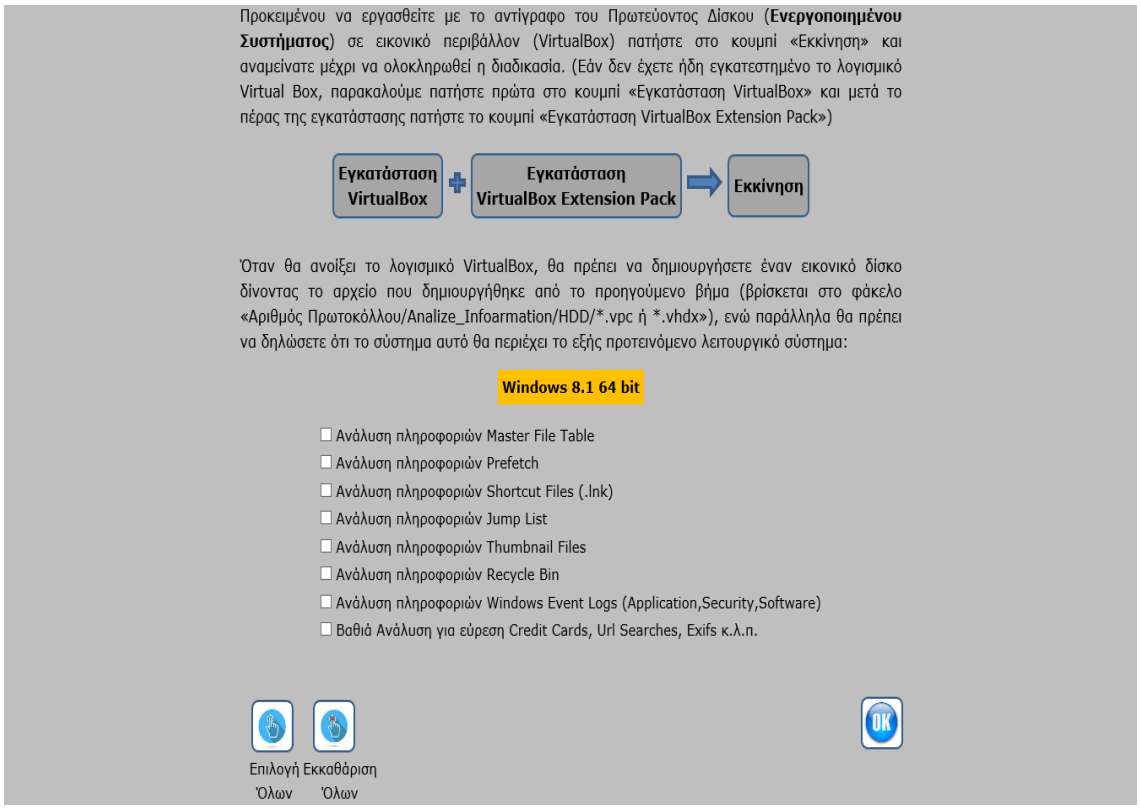
Ενώ, τέλος, εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Security»**, τότε, αυτόματα, θα εκτελεστεί η αντίστοιχη εντολή κονσόλας και θα αποθηκευτούν τα αποτελέσματα στο αρχείο με το όνομα security_analysis.txt ([20] RegRipper, 2015) :

Rip –r όνομα δισκου:\collected_information\Registry\security –f security > όνομα δίσκου\analyzed_information\Registry\security_analysis.txt

Σε κάθε περίπτωση, εάν ο αναλυτής επιθυμεί να λάβει γνώση όλων των παραπάνω, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων», που βρίσκεται στο κάτω μέρος της οθόνης. Σε περίπτωση δε, που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών αυτών και θέλει μόνο την ανάλυση ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν. Μετά το πέρας των παραπάνω ενεργειών, οφείλει να πατήσει στο κουμπί «OK», με σκοπό την έξοδό του από την κατηγορία αυτή. Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη των αντίστοιχων εντολών κονσόλας (command line), που εκτελούνται και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτών.

4.2.4 Ανάλυση Αντίγραφου Πρωτεύων Δίσκου (Hdd)

Επόμενη δυνατότητα είναι η ανάλυση του αντιγράφου του πρωτεύοντος δίσκου (HDD), του υπο μελέτη συστήματος. Αν λοιπόν ο αναλυτής πατήσει στο κουμπί «Ανάλυση Αντιγράφου Πρωτεύον Δίσκου (HDD)», αυτόματα ανοίγει η επόμενη σελίδα (Εικόνα 4.2.4.1).



Εικόνα 4.2.4.1: Ανάλυση Αντιγράφου Πρωτεύων Δίσκου (HDD) από Ενεργοποιημένο Σύστημα

Αρχικά, ο αναλυτής θα πρέπει να πατήσει στο κουμπί «Εκκίνηση», με σκοπό να εκτελεστεί το λογισμικό «Virtual Box», της εταιρείας Oracle. Επειδή ο αναλυτής μπορεί να μην έχει εγκατεστημένο το εν λόγω λογισμικό στον υπολογιστή του, γι'αυτό γίνεται ο απαραίτητος έλεγχος και αν δεν είναι εγκατεστημένο, τότε, με κατάλληλο μήνυμα το παραπέμπει να ακολουθήσει δύο (2) επιπλέον βήματα. Δηλαδή, θα πρέπει να πατήσει πρώτα στο κουμπί «Εγκατάσταση Virtual Box» και στη συνέχεια θα πρέπει να πατήσει στο κουμπί «Εγκατάσταση

Virtual Box Extension Pack». Με τον τρόπο αυτό εγκαθίστανται το απαιραίτητο λογισμικό, με όλες του, τις λειτουργίες, ενεργοποιημένες.

Ανοίγει λοιπόν το λογισμικό Virtual Box και καλείται ο αναλυτής να δημιουργήσει έναν εικονικό δίσκο, επιλέγοντας το αντίγραφο του δίσκου που έχει ήδη ληφθεί (αρχείο με το όνομα hdd.vpc ή hdd.vhdx που βρίσκεται μέσα στο φάκελο αριθμός_πρωτοκόλλου/analyzed_information\hdd). Κατά την δημιουργία αυτού του εικονικού δίσκου, ο αναλυτής, θα κληθεί να ορίσει το είδος του λειτουργικού συστήματος (windows), που ήταν εγκατεστημένο στον ηλεκτρονικό υπολογιστή, από τον οποίο και λήφθηκε το εν λόγω αντίγραφο. Για το λόγο αυτό, στο χρωματιστό πλαίσιο της εικόνας 4.2.4.1, ορίζεται το είδος και η έκδοση του λειτουργικού (Windows) που ήταν εγκατεστημένο στο υπό μελέτη σύστημα. Αυτή η ενέργεια επιτυγχάνεται εκτελώντας τις παρακάτω εντολές κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα final_hdd_image_letter.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\software –p winnt_cv > όνομα δίσκου\analyzed_information\hdd\image_letter.txt

Type όνομα δίσκου:\analyzed_information\hdd\image_letter.txt | findstr “ProductName” > όνομα δίσκου:\analyzed_information\hdd\final_hdd_image_letter.txt & type όνομα δίσκου:\ analyzed_information\hdd\image_letter.txt | “BuildLabEx” >> όνομα δίσκου:\ analyzed_information\hdd\final_hdd_image_letter.txt
```

Μετά το πέρας των παραπάνω βημάτων, δημιουργείται και ενεργοποιείται ένας εικονικός δίσκος, που δεν είναι άλλος, παρά ένα πλήρες αντίγραφο του δίσκου, του υπο μελέτη συστήματος. Δηλαδή, ο αναλυτής έχει μπροστά του, ως εικονικό περιβάλλον, το ίδιο, το υπο μελέτη σύστημα. Μπορεί λοιπόν, να περιηγηθεί στα περιεχόμενα, του δίσκου αυτού και να εμβαθύνει την ανάλυσή του, με σκοπό την εξαγωγή ακόμα περισσοτέρων συμπερασμάτων. Φυσικά, στην περίπτωση που θέλει να αναλύσει συγκεκριμένες πληροφορίες από το αντίγραφο του πρωτεύοντος δίσκου (HDD), του υπο μελέτη συστήματος, μπορεί εάν θέλει να το επιτύχει μέσα από το λογισμικό μας, αρκεί να επιλέξει μία από τις δυνάτοτητες που του δίνονται.

Δηλαδή, εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών Master File Table», πατώντας μονό αριστερό κλικ στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την έκφραση, τότε, αυτόματα, θα εκκινήσει η αντίστοιχη διαδικασία εκτελώντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα analyzed_mft.csv ([28]Dkovar/AnalyzeMFT, 2017 και [29]Py2EXE, 2014) :

```
AnalyzeMFT -f όνομα δισκου:\collected_information\hdd\$mft –o όνομα δίσκου\ analyzed_information\hdd\analyzed_mft.csv
```

Κατά αντίστοιχο τρόπο εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών Prefetch**»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας και θα αποθηκευτούν τα αποτελέσματα στο αρχείο με το όνομα prefetch.xml :

```
Xcopy όνομα δισκου:\collected_information\hdd\prefetch.xml όνομα δίσκου\ analyzed_information\ hdd\prefetch.xml
```

Εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών Shortcut Files (.lnk)**»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα, θα αποθηκευτούν στο αρχείο με το όνομα analyzed_recent_files.txt ([31]lnkParser, 2012) :

```
lnk_parser_cmd όνομα δισκου:\collected_information\hdd\users\όνομα χρήστη\recent_files > όνομα δίσκου\analyzed_information\hdd\users\όνομα χρήστη\recent_files\ analyzed_recent _files.txt
```

Αντίστοιχα, εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών Jump List**»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας (για κάθε έναν από τους χρήστες, του

υπό μελέτη συστήματος) και τα αποτελέσματα, θα αποθηκευτούν στο αρχείο με το όνομα analyzed_jump_lists.txt ([32]JumpListsView, 2013-2016) :

```
Jumplixtview /recentfolder  όνομα δισκου:\collected_information\hdd\users\όνομα χρήστη\
recent_files /sxml όνομα δίσκου\analyzed_information\hdd\users\όνομα χρήστη\jumkp_lists\
analyzed_jump_lists.xls
```

Αν ο αναλυτής επιλέξει την κατηγορία «Ανάλυση πληροφοριών Thumbnail Files**»**, τότε, εκτελείται η ακόλουθη εντολή κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα αποθηκεύονται σε αρχεία με την εξής μορφή ονόματος analyzed_thumbcache_όνομα.txt ([33]Thumbcache Viewer, 2016):

```
Thumbcache_viewer_cmd  όνομα δισκου:\collected_information\hdd\users\όνομα χρήστη\
thumbnail_files\thumbcache_όνομα.db > όνομα δίσκου\analyzed_information\hdd\users\
όνομα χρήστη\thumbnail_files/analyzed_thumbcache_όνομα.txt
```

Επόμενη πληροφορία που μπορεί να αναλυθεί είναι σχετικά με τον κάδο ανακύκλωσης. Έτσι, εάν ο αναλυτής επιλέξει την κατηγορία «Ανάλυση πληροφοριών Recycle Bin**»**, τότε, εκτελούνται οι παρακάτω εντολές κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα αποθηκεύονται ως αρχεία, εντός του υποφακέλου με το όνομα recycle_bin ([34]Abelecheung/Rifiuti2, 2017), [35]Show Hidden Files Using Attrib Command, 2017 και ([51]Rifiuti2/Readme, 2017)):

```
Attrib –s –h –r /s /d

Dir /b > όνομα δίσκου:\analyzed_information\hdd\username_recycle_bin.txt

Rifiuti-vista –x –z –o όνομα δίσκου\analyzed_information\hdd\users\όνομα
χρήστη\recycle_bin\analyzed_recycle_bin.xml όνομα δίσκου:\collected_information\hdd\
recycle_bin\όνομα χρήστη
```

Στο σημείο αυτό, ο αναλυτής, εάν επιθυμεί μπορεί να επιλέξει την κατηγορία «Ανάλυση πληροφοριών Windows Event Logs (Application,Security,Software)**»**, αλλά απαιτείται να είναι ήδη εγκατεστημένο στον υπολογιστή του, το λογισμικό Log Parser. Ελέγχεται λοιπόν, εάν είναι ήδη εγκατεστημένο και αν δεν είναι, τότε, τον παραπέμπει να πατήσει στο κουμπί με το όνομα «Εγκατάσταση Log Parser» και να ακολουθήσει τα παραίτητα βήματα, όπως αυτά υποδεικνύονται. Στη συνέχεια, εκτελούνται οι παρακάτω εντολές κονσόλας, ενώ, τα αποτελέσματα αποθηκεύονται στα αντίστοιχα αρχεία με τα ονόματα analyzed_application_logs.xml, analyzed_security_logs.xml και analyzed_system_logs.xml ([38]LogParser 2.2, 2017):

```
Logparser “SELECT Timegenerated, SourceName, EventCategoryName, EventId, Message
into όνομα δισκου:\analyzed_information\hdd\analyzed_Application_logs.xml FROM όνομα
δίσκου\collected_information\hdd\Application_logs_evt” –i:evt –o:xml

Logparser “SELECT Timegenerated, SourceName, EventCategoryName, EventId, Message
into όνομα δισκου:\analyzed_information\hdd\analyzed_Security_logs.xml FROM όνομα
δίσκου\collected_information\hdd\Security_logs_evt” –i:evt –o:xml

Logparser “SELECT Timegenerated, SourceName, EventCategoryName, EventId, Message
into όνομα δισκου:\analyzed_information\hdd\analyzed_System_logs.xml FROM όνομα
δίσκου\collected_information\hdd\System_logs_evt” –i:evt –o:xml
```

Η τελευταία δυνατότητα ανάλυσης που δίνεται στον αναλυτή, είναι να επιλέξει την κατηγορία «Βαθιά Ανάλυση για εύρεση Credit Cards,Url Searches, Exifs κλπ**»**, όπου, αυτόματα,

θα εκτελεστεί η επόμενη εντολή κονσόλας και τα αποτελέσματα θα αποθηκευτούν σε υποφάκελο με το όνομα Deep_HDD_Image_Analysis ([41]Bulk Extractor, 2015):

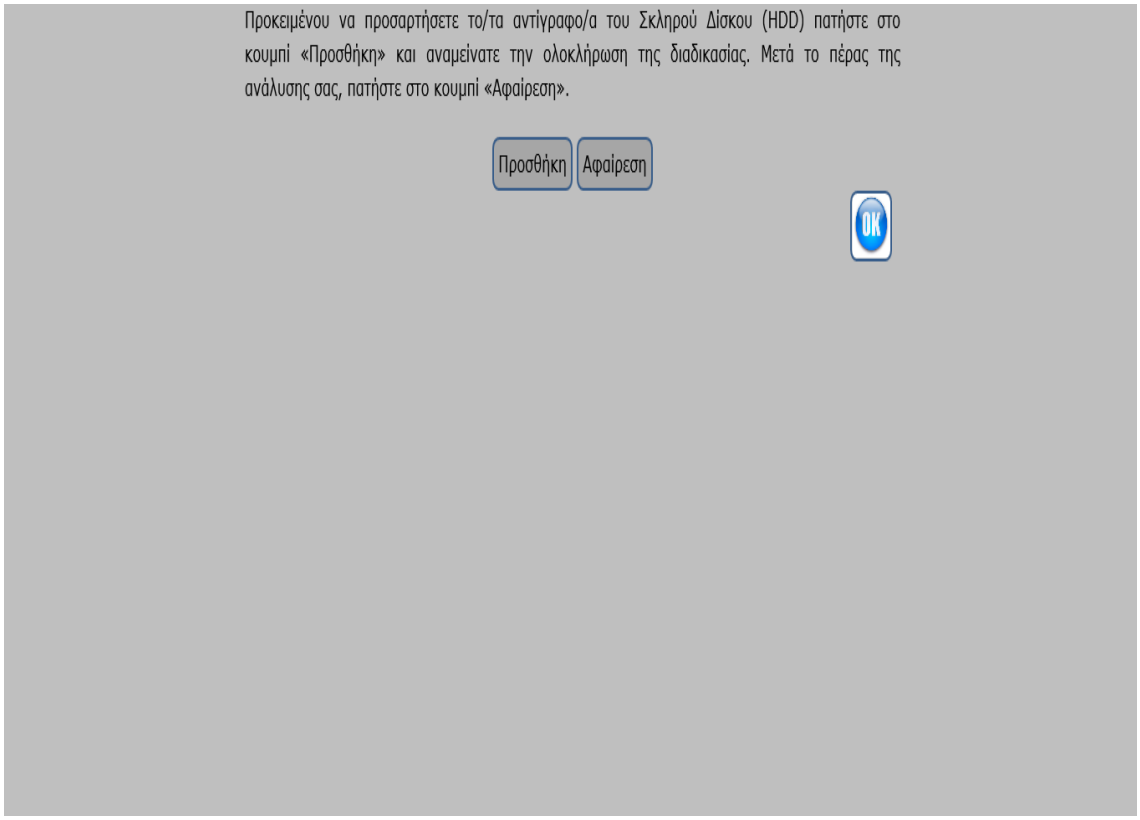
```
Bulk_Extractor32 –ο όνομα δίσκου\analyzed_information\hdd\Deep_HDD_Image_Analysis
όνομα δίσκου:\collected_information\hdd\ON\hdd_image.dd
```

Σε κάθε περίπτωση, εάν ο αναλυτής επιθυμεί να λάβει γνώση όλων των παραπάνω, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων» που βρίσκεται στο κάτω μέρος της οθόνης. Σε περίπτωση δε που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών αυτών και θέλει μόνο την ανάλυση ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν. Μετά το πέρας των παραπάνω ενεργειών, οφείλει να πατήσει στο κουμπί «OK» με σκοπό την έξοδό του από την κατηγορία αυτή. Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη των αντίστοιχων εντολών κονσόλας (command line) που εκτελούνται και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτών.

4.2.5 Ανάλυση Αντίγραφου Δίσκου χωρίς Λειτουργικό Σύστημα (Hdd)

Επειδή, κατά τη συλλογή των πληροροφιών μπορεί να βρεθεί ένας σκληρός δίσκος (HDD) εγκατεστημένος στο κατασχεθέν σύστημα, αλλά, χωρίς να φέρει εγκατεστημένο λειτουργικό, γι'αυτό το λόγο, το λογισμικό μας, προσφέρει στον αναλυτή των ψηφιακών πειστηρίων, την δυνατότητα να αναλύσει ακόμα και τα περιεχόμενα αυτού του δίσκου.

Έτσι, εάν πατήσει στο κουμπί «Ανάλυση Αντιγράφου Δίσκου χωρίς Λειτουργικό Σύστημα (HDD)», αυτόματα, ανοίγει η επόμενη σελίδα (Εικόνα 4.2.5.1).



Εικόνα 4.2.5.1: Ανάλυση Αντιγράφου Δίσκου χωρίς Λειτουργικό Σύστημα (HDD) από Ενεργοποιημένο Σύστημα

Στο σημείο αυτό, θα πρέπει να πατήσει στο κουμπί «Προσθήκη», με σκοπό να προσαρτηθεί στον υπολογιστή του, ως εικονικός εξωτερικός σκληρός δίσκος, το αντίγραφο που είχε λάβει από τον εν λόγω σκληρό δίσκο. Μάλιστα, στην περίπτωση που είχαν βρεθεί περισσότεροι του ενός, σκληροί δίσκοι, κατά την χρονική στίγμη της κατάσχεσης (άρα έχουν ληφθεί αντίγραφα από όλους αυτούς τους δίσκους), τότε, πατώντας στο κουμπί αυτό, αυτόματα, θα προσαρτηθούν όλα τα αντίγραφα ως εξωτερικοί σκληροί δίσκοι, του συστήματος του αναλυτή. Για να επιτευχθεί η ενέργεια αυτή, εκτελούνται οι κάτωθι εντολές κονσόλας ([24]Qemu-img for Windows, 2016-2017 και [26]Mounting VHDs in Windows 7 from a Command-Line Script , 2012):

```
Qemu-img convert όνομα δίσκου:\collected_information\hdd\ON\hdd_image.dd –O vhdx όνομα δίσκου:\analyzed_information\hdd\VMDisk.vhdx

Diskpart
Sel vdisk file=”όνομα δίσκου:\analyzed_information\hdd\VMDisk.vhdx”
Attach vdisk
```

Ο αναλυτής, μπορεί πλέον να μελετήσει τα δεδομένα που εμπεριέχονται σε αυτούς τους εικονικούς δίσκους, εξάγοντας με ασφάλεια επιμέρους συμπεράσματα. Μετά το πέρας της ανάλυσής του αυτής, οφείλει να αφαιρέσει από το σύστημά του, τους εικονικούς αυτούς δίσκους. Για να το επιτύχει αυτό, αρκεί να πατήσει στο κουμπί «Αφαίρεση». Με το πάτημα του κουμπιού αυτού, αυτόματα εκτελούνται οι παρακάτω εντολές:

```
Diskpart
Sel vdisk file=”όνομα δίσκου:\analyzed_information\hdd\VMDisk.vhdx”
Detach vdisk
```

Μετά την παραπάνω ενέργεια και πατώντας στο κουμπί «OK», ο αναλυτής εξέρχεται από την κατηγορία αυτή και επιστρέφει στη σελίδα που μπορεί να επιλέξει οποιαδήποτε άλλη πληροφορία προς ανάλυση.

4.2.6 Ανάλυση Αφαιρούμενου Μέσου (Usb Flash Disk)

Όπως αναφέραμε και στο προηγούμενο υποκεφάλαιο, υπάρχει περίπτωση κατά την κατάσχεση ενός εκθέματος, να βρεθούν, πλησίον του, εξωτερικά αποθηκευτικά μέσα, όπως σκληροί δίσκοι (HDD), ή αφαιρούμενα αποθηκευτικά μέσα μικρής χωρητικότητας (Usb Flash Disks).

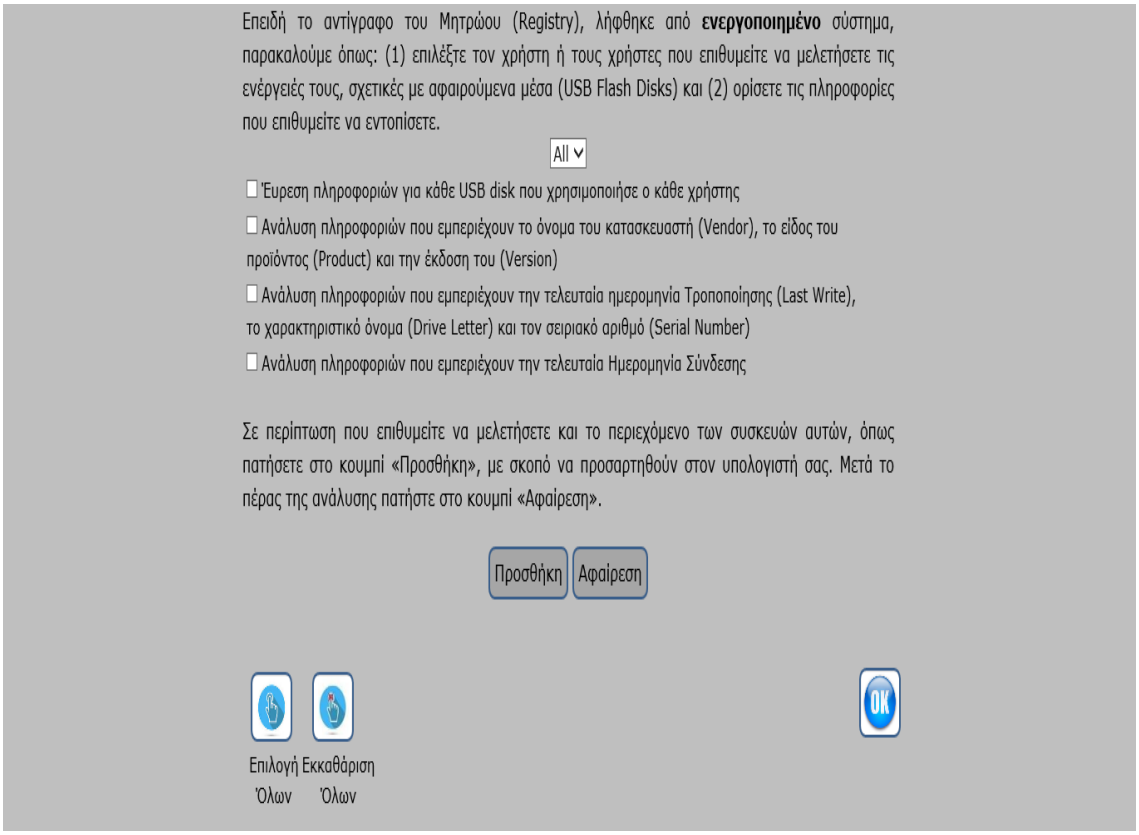
Και στις δυο αυτές περιπτώσεις, ο αναλυτής, θα πρέπει να τα θεωρεί ως ιδίου τύπου αποθηκευτικές συσκευές, δηλαδή, ως «Αφαιρούμενα Μέσα». Μάλιστα, επειδή μπορεί σε οποιαδήποτε χρονική στιγμή, πριν την κατάσχεση, να έχουν συνδεθεί οι συσκευές αυτές στον ηλεκτρονικό υπολογιστή που μας ενδιαφέρει, γι’ αυτό είναι ορθό, να ληφθούν αντίγραφα και από αυτά, καθόσον μπορεί να περιέχουν σημαντικές πληροφορίες.

Μάλιστα, ο αναλυτής, μπορεί να εξάγει σημαντικά συμπεράσματα, όχι μόνο από την ανάλυση του αντιγράφου αυτών των συσκευών, αλλά και από τις πληροφορίες που αποθηκεύτηκαν κατά την σύνδεση των συσκευών αυτών, στον εν λόγω ηλεκτρονικό υπολογιστή. Οι πληροφορίες αυτές αποθηκεύονται στο Μητρώο του λειτουργικού συστήματος (Registry) και απαιτούν ιδιαίτερο χειρισμό για να μπορέσουμε να τις αντλήσουμε.

Σε κάθε περίπτωση δε, ο ερευνητής, εάν επιθυμεί την ανάλυση των ανωτέρω συσκευών, οφείλει να πατήσει στο κουμπί «Ανάλυση Αφαιρούμενου Μέσου (USB Flash Disk)», με σκοπό να του ανοίξει η παρακάτω σελίδα (Εικόνα 4.2.6.1), στην οποία έχουμε διαχωρίσει τις πληροφορίες που μπορούν να μελετηθούν, σε κάθε μια από τις δύο (2) περιπτώσεις, που προαναφέραμε.

Μόλις ανοίξει η σελίδα, ο αναλυτής, θα πρέπει να επιλέξει από την αναδυόμενη λίστα, τον χρήστη, του υπό μελέτη συστήματος, του οποίου θέλει να μελετήσει τις ενέργειες και οι οποίες σχετίζονται με εξωτερικά αποθηκευτικά μέσα. Εάν δεν ενδιαφέρεται για συγκεκριμένο χρήστη,

αλλά, θέλει να μελετήσει όλους του χρήστες του συστήματος αυτού, αρκεί να επιλέξει την κατηγορία «ALL».



Εικόνα 4.2.6.1: Ανάλυση Αφαιρούμενου Μέσου (USB Flash Disk) από Ενεργοποιημένο Σύστημα

Εν συνεχεία, πατώντας μονό αριστερό κλικ, στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την εκάστοτε έκφραση, ανιχνεύονται οι απαραίτητες πληροφορίες από το αντίγραφο του Μητρώου (Registry) και αναλύονται. Αν λοιπόν, για παράδειγμα, επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχουν το όνομα του κατασκευαστή (Vendor), το είδος του προϊόντος (Product) και την έκδοση του (Version)», αυτόματα, ξεκινάει, η αντίστοιχη διαδικασία τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα USB_Vendor+Product_Name+Version.txt ([21]Type, 2017):

```
Type όνομα δίσκου:\collected_information\Registry\system_analysis.txt | find “USBSTOR#” > όνομα δίσκου\analyzed_information\USB\ USB_Vendor+Product_Name+Version.txt
```

Στην περίπτωση που επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχουν την τελευταία ημερομηνία Τροποποίησης (Last Write), το χαρακτηριστικό όνομα (Drive Letter) και τον σειριακό αριθμό (Serial Number)», τότε, εκτελείται η παρακάτω εντολή κονσόλας και τα αποτελέσματα αποθηκεύονται στο αρχείο με το όνομα USB_Serial+Last_Write+Drive_Letter.txt ([20] RegRipper, 2015):

```
Rip –r όνομα δίσκου:\collected_information\Registry\software –p removdev > όνομα δίσκου\analyzed_information\USB\ USB_Serial+Last_Write+Drive_Letter.txt
```

Ενώ, εάν επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχουν την τελευταία ημερομηνία Σύνδεσης»,τότε, εκτελείται η παρακάτω εντολή κονσόλας και τα αποτελέσματα θα

αποθηκευτούν στο αρχείο με το όνομα USB_Last_Time_Connection.txt ([20] RegRipper, 2015):

```
Rip –r όνομα δίσκου:\collected_information\Registry\system –p devclass > όνομα δίσκου\analyzed_information\USB\ USB_Last_Time_Connection.txt
```

Στο σημείο αυτό, έχει ολοκληρωθεί η ανάλυση των πληροφοριών που σχετίζονται με τα εξωτερικά αποθηκευτικά μέσα και οι οποίες βρίσκονταν στο Μητρώο (Registry), του υπό μελέτη συστήματος. Αν ο ερευνητής επιθυμεί να εμβαθύνει την ανάλυσή του, τότε, οφείλει να μελετήσει και τα περιεχόμενα των συσκευών αυτών.

Πατώντας πάνω στο κουμπί «Προσθήκη», προσαρτάται στον υπολογιστή του, ως εικονικό εξωτερικό αποθηκευτικό μέσο, το αντίγραφο που είχε λάβει από την εν λόγω συσκευή (USB Flash Disk). Μάλιστα, στην περίπτωση που είχαν βρεθεί περισσότερες από μία τέτοιου είδους συσκευές, κατά την χρονική στίγμη της κατάσχεσης (άρα έχουν ληφθεί αντίγραφα από όλες αυτές), τότε, πατώντας στο κουμπί αυτό, αυτόματα, θα προσαρτηθούν όλα τα αντίγραφα, ως εξωτερικά αποθηκευτικά μέσα, του συστήματος του αναλυτή. Για να επιτευχθεί η ενέργεια αυτή εκτελούνται οι κάτωθι εντολές κονσόλας ([24]Qemu-img for Windows, 2016-2017 και [26]Mounting VHDs in Windows 7 from a Command-Line Script , 2012):

```
Qemu-img convert όνομα δίσκου:\collected_information\USB\όνομα usb δίσκου_image.dd –O vhdx όνομα δίσκου:\analyzed_information\USB\όνομα usb δίσκου.vhdx

Diskpart
Sel vdisk file=”όνομα δίσκου:\analyzed_information\USB\όνομα usb δίσκου.vhdx”
Attach vdisk
```

Ο αναλυτής μπορεί πλέον να μελετήσει τα δεδομένα που εμπεριέχονται σε αυτά τα εικονικά εξωτερικά αποθηκευτικά μέσα, εξάγοντας με ασφάλεια επιμέρους συμπεράσματα. Μετά το πέρας της ανάλυσης του αυτής, οφείλει να αφαιρέσει από το σύστημά του, αυτά τα εικονικά μέσα. Για να το επιτύχει αυτό, αρκεί να πατήσει στο κουμπί «Αφαίρεση». Με το πάτημα του κουμπιού αυτού, αυτόματα εκτελούνται οι παρακάτω εντολές:

```
Diskpart
Sel vdisk file=”όνομα δίσκου:\analyzed_information\ USB\όνομα usb δίσκου.vhdx”
Detach vdisk
```

Μετά την παραπάνω ενέργεια και πατώντας στο κουμπί «OK», ο αναλυτής, εξέρχεται από την κατηγορία αυτή. Σε περίπτωση όμως που κάποιες ή κάποια από τις παραπάνω εντολές κονσόλας δεν έχουν τερματίσει, τότε, αυτόματα, θα εμφανιστεί μήνυμα σχετικά με την μη ολοκλήρωσή τους και η έξοδος θα πραγματοποιηθεί μετά το πέρας τους.

4.2.7 Ανάλυση Αντίγραφου Χρονοδιαγράμματος Ενεργειών (Timeline)

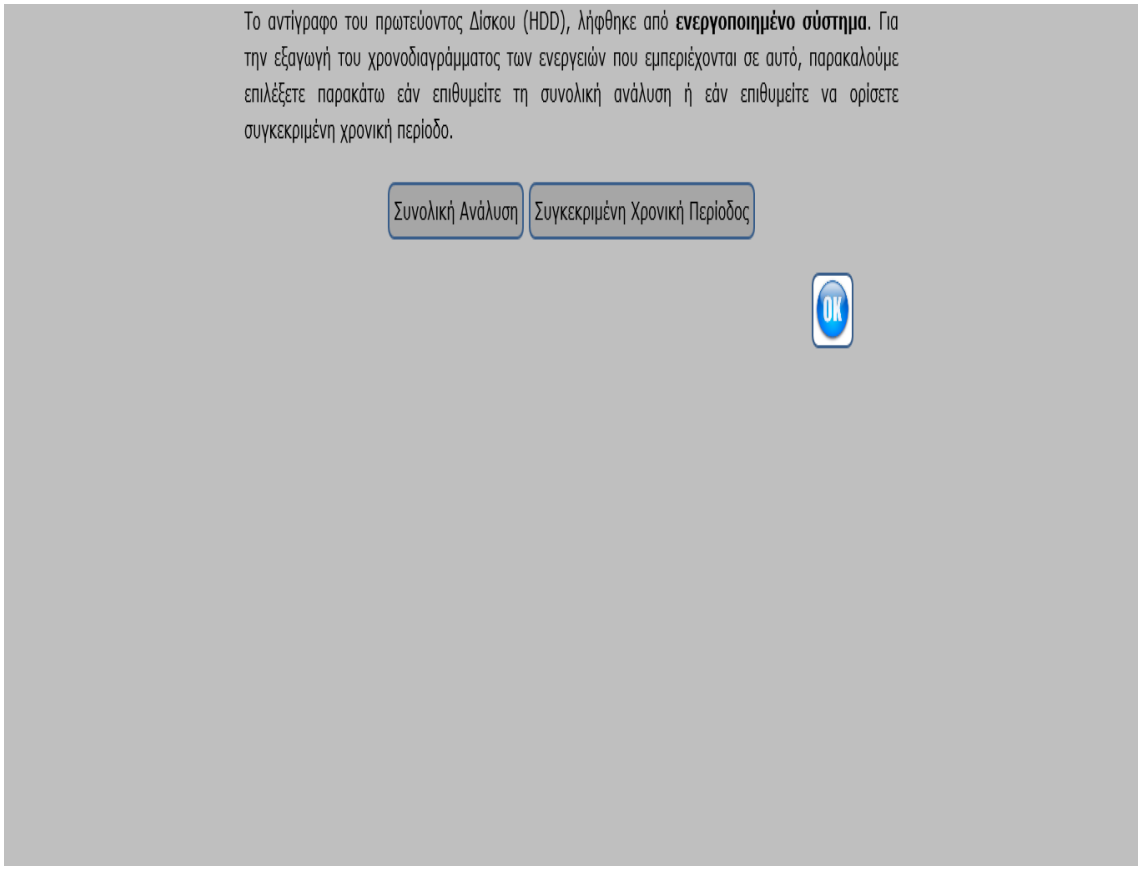
Κατά τη συλλογή πληροφοριών που σχετίζονται με το χρονοδιάγραμμα των ενεργειών (TimeLine) που εκτελέστηκαν σε έναν ηλεκτρονικό υπολογιστή, αναφέραμε ότι η διαδικασία αυτή είναι χρονοβόρα. Για το λόγο αυτό, κατά την συλλογή του χρονοδιαγράμματος αυτού, η εφαρμογή μας, αν και λάμβανε ένα υποτυπώδες αντίγραφο των ενεργειών, του υπό μελέτη συστήματος, παρ’όλα αυτά, η κύρια ενέργεια που γινόταν, ήταν ο έλεγχος εάν έχει ληφθεί ή όχι αντίγραφο του Πρωτεύων Δίσκου (HDD).

Ο σκοπός του ελέγχου αυτού, ήταν ότι, όταν ο ερευνητής επιθυμούσε να αναλύσει τα πεπραγμένα γεγονότα, τότε και μόνο τότε, να δημιουργούσαμε το κατάλληλο αρχείο που θα περιελάμβανε όλες τις εκτελεσθείσες ενέργειες, στο υπό μελέτη σύστημα. Όπως καταλαβαίνουμε, επειδή σε έναν ηλεκτρονικό υπολογιστή μπορεί να έχει παρέλθει μεγάλο χρονικό διάστημα από την χρονική στιγμή που εγκαταστάθηκε σε αυτό, το λειτουργικό σύστημα

των Windows, για το λόγο αυτό δίνουμε την δυνατότητα στον αναλυτή, είτε να επιλέξει την ανάλυση του χρονοδιαγράμματος αυτού, εντός συγκεκριμένου χρονικού διαστήματος, είτε γενικότερα από την ημερομηνία εγκατάστασης του λειτουργικού συστήματος των Windows, μέχρι και την ημερομηνία της κατάσχεσής του (δεν προτείνεται λόγω μεγάλου όγκου πληροφοριών).

Έτσι, λοιπόν, αν ο αναλυτής πατήσει στο κουμπί «Ανάλυση Αντιγράφου Χρονοδιαγράμματος Ενεργειών (TimeLine)» ταυτόχρονα εκτελούνται δύο (2) ενέργειες:

1) Ξεκινάει η διαδικασία λήψης του Αντιγράφου του Χρονοδιαγράμματος Ενεργειών, του υπό μελέτη συστήματος.
2) Εμφανίζει σχετικό μήνυμα, περί έναρξης της διαδικασίας αυτής και παροτρύνει τον αναλυτή να αναμένει μέχρι την ολοκλήρωση της.
3) Μετά την ολοκλήρωση της λήψης του Αντιγράφου του Χρονοδιαγράμματος Ενεργειών, ανοίγει η παρακάτω σελίδα (Εικόνα 4.2.7.1)



Εικόνα 4.2.7.1 : Ανάλυση Αντιγράφου Χρονοδιαγράμματος Ενεργειών (TimeLine) από Απενεργοποιημένο Σύστημα

Επειδή το αρχείο που δημιουργείται είναι πολύ μεγάλο, γι' αυτό, δεν το αποθηκεύουμε απευθείας στον εξωτερικό σκληρό δίσκο με τα ψηφιακά πειστήρια, του υπό μελέτη συστήματος, καθόσον παρατηρήσαμε κολλήματα στον ελεγκτή (controller) του δίσκου αυτού. Αποθηκεύουμε λοιπόν τα αποτελέσματα στο φάκελο των προσωρινών αρχείων (Temp) του λειτουργικού συστήματος του αναλυτή και στη συνέχεια, το αντιγράφουμε στον δίσκο με τα ψηφιακά πειστήρια. Για να επιτευχθεί η όλη διαδικασία αυτή, εκτελούμε τις παρακάτω εντολές κονσόλας και αποθηκεύουμε τα αποτελέσματα στο εξής αρχείο Timeline.dump ([42]Using Log2TimeLine, 2017 και ([44]Technet/Move, 2017)):

```
Echo %username% > όνομα δίσκου\analyzed_information\timeline\analist_Username.txt
```

```
Log2timeline - -partiotion all - -vss_store all c:\users\analist_Username\AppData \Local\Temp\TimeLine.dump όνομα δίσκου:\collected_information\HDD\ON\hhd_image.dd

Move c:\users\analist_Username\AppData\Local\Temp\TimeLine.dump όνομα δίσκου:\collected_information\TimeLine
```

Αφού λοιπόν έχει ολοκληρωθεί η διαδικασία δημιουργίας του απαραίτητου αρχείου, ο αναλυτής, καλείται να επιλέξει, εάν επιθυμεί την ανάλυση ολόκληρού του χρονοδιαγράμματος ενεργειών ή μόνο ενός συγκεκριμένου χρονικού διαστήματος αυτού. Αν λοιπόν πατήσει στο κουμπί «Συνολική Ανάλυση», τότε, εκτελείται η παρακάτω εντολή κονσόλας και τα αποτελέσματα αποθηκεύονται στο αρχείο με το όνομα Timeline.xlsx ([43]Plaso - Google & Timelines, 2014):

```
Psort –o xlsx –w όνομα δίσκου:\analyzed_information\Timeline\timeline.xlsx - -debug όνομα δίσκου\collected information\TimeLine\Timeline.dump
```

Ενώ, στην περίπτωση που επιθυμούσε την ανάλυση μόνο συγκεκριμένου χρονικού διαστήματος, τότε, θα έπρεπε να πατήσει στο κουμπί «Συγκεκριμένη Χρονική Περίοδο», με σκοπό να του εμφανιστούν τα πεδία στα οποία θα ορίσει την ημερομηνία εκκίνησης και την ημερομηνία λήξης (ημέρα/μήνας/έτος). Με το πάτημα του κουμπιού αυτού, εκτελείται η παρακάτω εντολή κονσόλας και τα αποτελέσματα αποθηκεύονται στο αρχείο με το όνομα Timeline.xlsx ([43]Plaso - Google & Timelines, 2014):

```
Psort –o xlsx –w όνομα δίσκου:\analyzed_information\Timeline\timeline.xlsx - -debug όνομα δίσκου\collected information\TimeLine\Timeline.dump “date > ‘ημερομηνια απο’ AND date < ‘ημερομηνια εως’ ”
```

Μετά το πέρας των παραπάνω ενεργειών, οφείλει να πατήσει στο κουμπί «OK», με σκοπό την έξοδό του, από την κατηγορία αυτή.

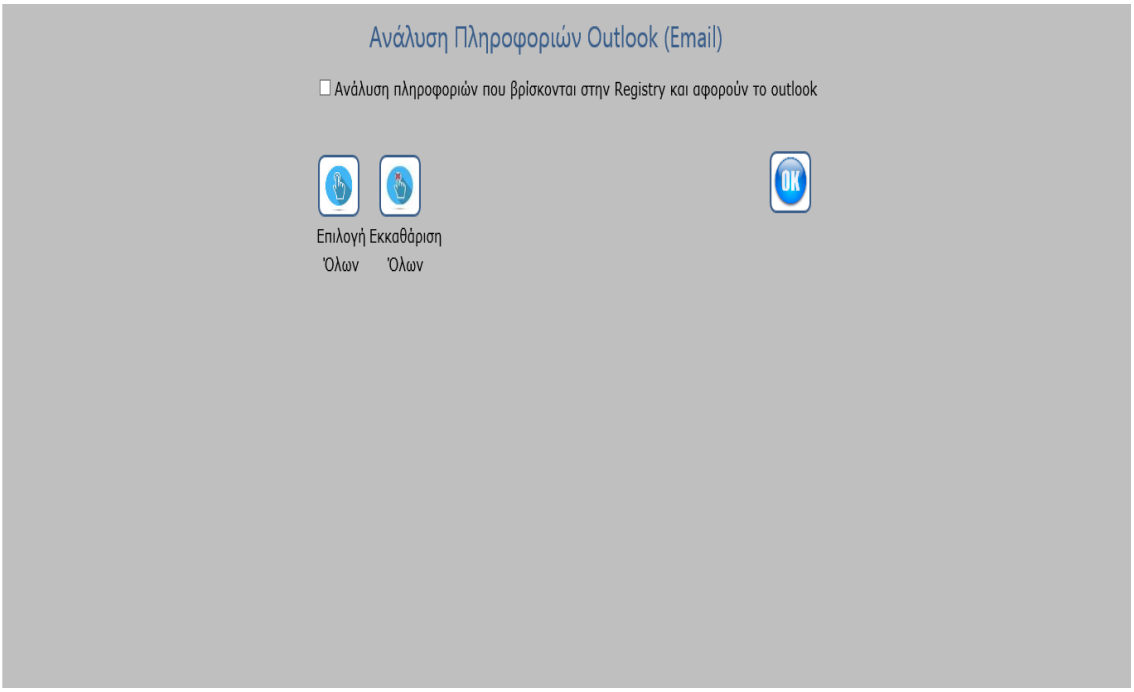
4.3 Ανάλυση Πληροφοριών από Απενεργοποιημένο Σύστημα

Όπως αναφέραμε και στην παράγραφο 4.2, μόλις ο αναλυτής πατήσει σε κάποιο από τα κουμπιά, με σκοπό την ανάλυση των αντίστοιχων πληροφοριών, η εφαρμογή αυτόματα αναζητάει στο φάκελο που όρισε ο αναλυτής (παράγραφος 4.1), εάν υπάρχει ο υποφάκελος με το όνομα «OFF», μέσα στο φάκελο με το όνομα «HDD», των αντίστοιχων συλλεχθέντων πληροφοριών.

Σε περίπτωση που υπάρχει, τότε, αναζητάει στο εσωτερικό αυτού, με σκοπό να βρεί εάν υπάρχει περιεχόμενο αρχείο. Εάν υπάρχει, αυτό συνεπάγεται ότι τα δεδομένα που έχουν συλλεχθεί, είναι από ένα σύστημα που βρέθηκε απενεργοποιημένο κατά την κατάσχεσή του. Κατά συνέπεια, ο αναλυτής κάθε φορά που θα πατάει σε ένα από τα κουμπιά που θα περιγράψουμε παρακάτω στις παραγράφους 4.3.1 έως και 4.3.6, θα αφορούν απενεργοποιημένο σύστημα.

4.3.1 Ανάλυση Πληροφοριών Δικτύου & Περιηγητών Ιστού (Email - Browsers)

Η πρώτη δυνατότητα που δίνεται για απενεργοποιημένο σύστημα είναι η ανάλυση των πληροφοριών που συλλέχθησαν και έχουν σχέση, είτε με το δίκτυο, είτε με τους Περιηγητές Ιστού που χρησιμοποιούσε ο χρήστης, του υπό μελέτη συστήματος. Έτσι πατώντας στο κουμπί «Ανάλυση Πληροφοριών Δικτύου & Περιηγητών Ιστού (Email - Browsers)», ανοίγει η κάτωθι σελίδα (Εικόνα 4.3.1.1)



Εικόνα 4.3.1.1 : Ανάλυση Πληροφοριών Δικτύου & Περιηγητών Ιστού (Email-Browsers) από Απενεργοποιημένο Σύστημα)

Με το άνοιγμα της σελίδας αυτής, γίνοται ταυτόχρονα δύο (2) ενέργειες:

α) Αντιγράφει όλα τα περιεχόμενα των υποφακέλων collected_information\Browsers και collected_information\Email, στους αντίστοιχους υποφακέλους μέσα στο φάκελο annalized_information, εκτελώντας την κάτωθι εντολή κονσόλας:

```
Copy όνομα δίσκου\collected_information\Browsers\*.* όνομα δίσκου\analyzed_information\ Browsers

Copy όνομα δίσκου \collected_information\Email\*.* όνομα δίσκου\analyzed_information\ Email
```

και (β) ελέγχει εάν υπάρχει περιεχόμενο αρχείο στο φάκελο με το όνομα «Registry», διότι για την ανάλυση των πληροφοριών που δίνονται στην κατηγορία αυτή απαιτείται πρωταρχικά να έχει ληφθεί σχετικό αντίγραφο του Μητρώου (Registry). Στην περίπτωση που δεν έχει ληφθεί, εμφανίζεται σχετικό μήνυμα που παραπέμπει τον αναλυτή στην αντίστοιχη ενέργεια.

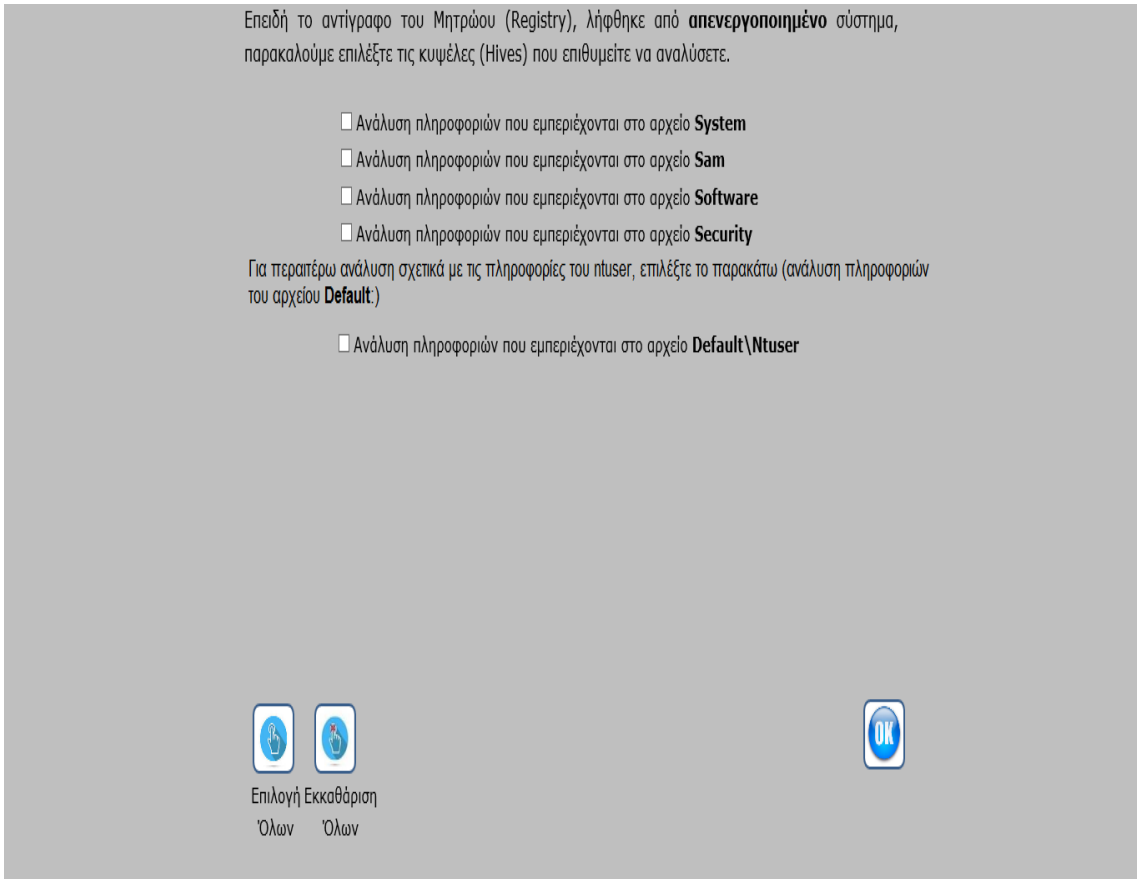
Επειδή σε ένα απενεργοποιημένο σύστημα, δεν υπάρχουν πολλές δυνατότητες, γι'αυτό ο αναλυτής μπορεί να λάβει γνώση μόνο των πληροφοριών εκείνων που σχετίζονται με τα ηλεκτρονικά μηνύματα (email) του χρήστη/χρηστών, του υπό μελέτη συστήματος. Έτσι, πατώντας στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την έκφραση «Ανάλυση πληροφοριών που βρίσκονται στην Registry και αφορούν το outlook», αυτόματα, ξεκινάει η αντίστοιχη διαδικασία τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα outlook_registry_analysis.txt ([20] RegRipper, 2015):

```
Copy γραμμα δισκου:\collected_information\Email\*.* όνομα δίσκου\analyzed_information\ Email

Rip –r γραμμα δισκου:\collected_information\Registry\software –p outlook > όνομα δίσκου\analyzed_information\ Email\outlook_registry_analysis.txt
```

Τέλος, για την έξοδό του, από την κατηγορία αυτή, αρκεί να πατήσει στο κουμπί «OK». Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη της παραπάνω εντολής κονσόλας (command line) και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτής.

4.3.2 Ανάλυση Αντίγραφου Μητρώου Συστήματος (Registry)

Η επόμενη δυνατότητα που δίνεται για απενεργοποιημένο σύστημα, είναι η ανάλυση των πληροφοριών που συλλέχθησαν και έχουν σχέση με το Μητρώο (Registry) του λειτουργικού συστήματος που ήταν εγκατεστημένο, στο υπό μελέτη σύστημα. Έτσι, πατώντας στο κουμπί «Ανάλυση Αντιγράφου Μητρώου (Registry)» ανοίγει η κάτωθι σελίδα (Εικόνα 4.3.2.1).



Εικόνα 4.3.2.1: Ανάλυση Αντιγράφου Μητρώου (Registry) από Απενεργοποιημένο Σύστημα

Θα πρέπει σε αυτήν τη σελίδα, ο αναλυτής, να επιλέξει συγκεκριμένες πληροφορίες που τον ενδιαφέρουν να αναλυθούν και σχετίζονται με τις κυψέλες (Hives) του Μητρώου (Registry). Πατώντας λοιπόν, μονό αριστερό κλικ, στο κουτί επιλογής (check box) που βρίσκεται μπροστά από την εκάστοτε έκφραση, ανιχνεύονται και αναλύονται οι αντίστοιχες πληροφορίες. Αν, για παράδειγμα, επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **System**», αυτόματα, ξεκινάει η αντίστοιχη διαδικασία τρέχοντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα system_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\sysem –f system > όνομα δίσκου\analyzed_information\Registry\system_analysis.txt
```

Στην περίπτωση που επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Sam**», τότε, αυτόματα, θα εκκινήσει η αντίστοιχη διαδικασία εκτελώντας την παρακάτω εντολή κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα sam_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\sam –f sam > όνομα δίσκου\analyzed_information\Registry\sam_analysis.txt
```

Κατά αντίστοιχο τρόπο, εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Software»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας και θα αποθηκευτούν τα αποτελέσματα στο αρχείο με το όνομα software_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\software –f software > όνομα δίσκου\analyzed_information\Registry\software_analysis.txt
```

Εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Security»**, τότε, αυτόματα, θα εκτελεστεί η αντίστοιχη εντολή κονσόλας και θα αποθηκευτούν τα αποτελέσματα στο αρχείο με το όνομα security_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\security–f security > όνομα δίσκου\analyzed_information\Registry\security_analysis.txt
```

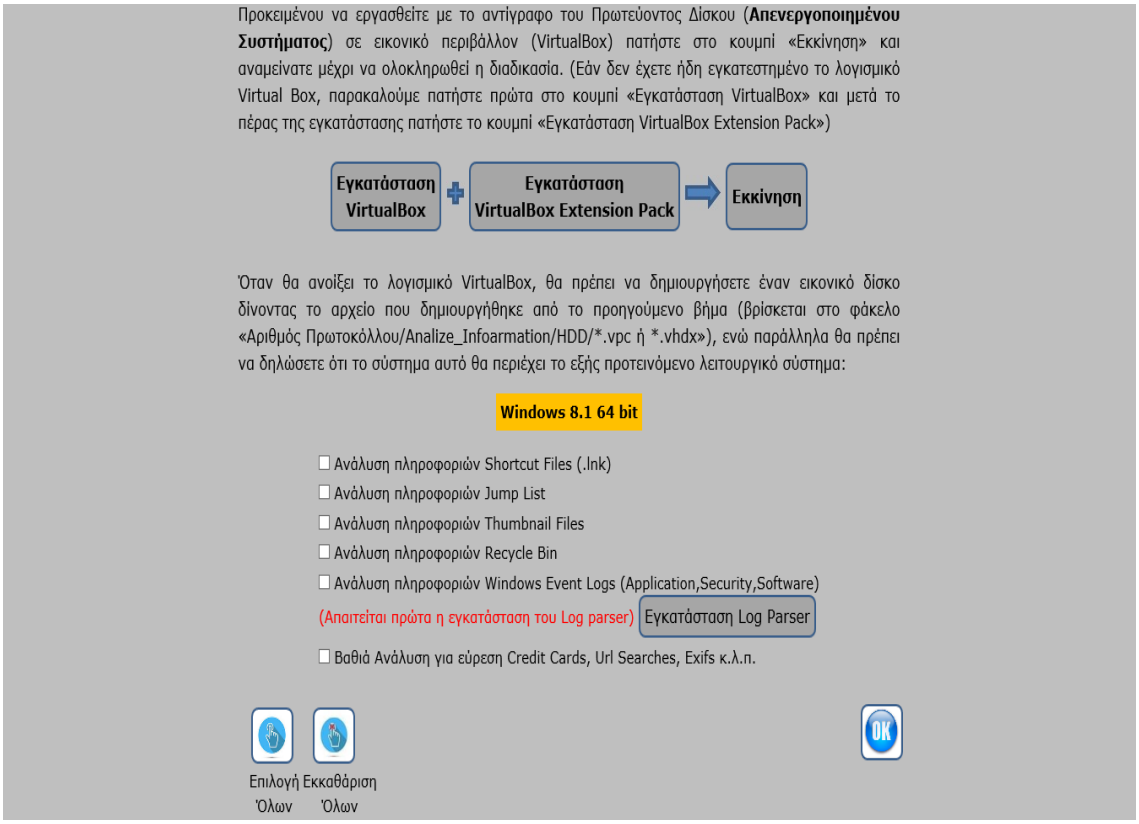
Τέλος, εάν ο αναλυτής επιθυμεί να εμβαθύνει ακόμα περισσότερο την ανάλυσή του, τότε το λογισμικό μας, του δίνει την δυνατότητα επιλογή της κατηγορίας «Ανάλυση πληροφοριών που εμπεριέχονται στο αρχείο **Default\Ntuser»**, εκτελώντας την παρακάτω εντολή κονσόλας και θα αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα ntuser_analysis.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\default –f ntuser > όνομα δίσκου\analyzed_information\Registry\ntuser_analysis.txt
```

Σε κάθε περίπτωση, εάν ο αναλυτής επιθυμεί να λάβει γνώση όλων των παραπάνω, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων», που βρίσκεται στο κάτω μέρος της οθόνης. Σε περίπτωση δε που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών αυτών και θέλει μόνο την ανάλυση ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν. Μετά το πέρας των παραπάνω ενεργειών, οφείλει να πατήσει στο κουμπί «OK», με σκοπό την έξοδό του, από την κατηγορία αυτή. Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη των αντίστοιχων εντολών κονσόλας (command line), που εκτελούνται και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτών.

4.3.3 Ανάλυση Αντίγραφου Πρωτεύων Δίσκου (Hdd)

Στο σημείο αυτό, ο αναλυτής, έχει τη δυνατότητα να αναλύσει το αντίγραφο του πρωτεύοντος δίσκου (HDD), που είχε λάβει από το υπό μελέτη σύστημα, έστω και αν αυτό βρέθηκε απενεργοποιημένο κατά την κατάσχεσή του. Αν λοιπόν, ο αναλυτής, πατήσει στο κουμπί «Ανάλυση Αντιγράφου Πρωτεύων Δίσκου (HDD)», αυτόματα, ανοίγει η επόμενη σελίδα (Εικόνα 4.3.3.1).



Εικόνα 4.3.3.1: Ανάλυση Αντιγράφου Πρωτεύων Δίσκου (HDD) από Απενεργοποιημένο Σύστημα

Αρχικά, ο αναλυτής, θα πρέπει να πατήσει στο κουμπί «Εκκίνηση», με σκοπό να εκτελεστεί το λογισμικό «Virtual Box», της εταιρείας Oracle. Επειδή ο αναλυτής μπορεί να μην έχει εγκατεστημένο το εν λόγω λογισμικό στον υπολογιστή του, γι'αυτό γίνεται ο απαραίτητος έλεγχος και αν δεν είναι εγκατεστημένο, τότε, με κατάλληλο μήνυμα τον παραπέμπει να ακολουθήσει δύο (2) επιπλέον βήματα. Δηλαδή, θα πρέπει να πατήσει πρώτα στο κουμπί «Εγκατάσταση Virtual Box» και στη συνέχεια θα πρέπει να πατήσει στο κουμπί «Εγκατάσταση Virtual Box Extension Pack». Με τον τρόπο αυτό εγκαθίστανται το απαιραίτητο λογισμικό με όλες του τις λειτουργίες ενεργοποιημένες.

Ανοίγει λοιπόν το λογισμικό Virtual Box και καλείται ο αναλυτής να δημιουργήσει έναν εικονικό δίσκο, επιλέγοντας το αντίγραφο του δίσκου που έχει ήδη ληφθεί (αρχείο με το όνομα hdd.vpc ή hdd.vhdx που βρίσκεται μέσα στο φάκελο αριθμός_πρωτοκόλλου/analyzed_information\hdd). Κατά την δημιουργία αυτού του εικονικού δίσκου, ο αναλυτής, θα κληθεί να ορίσει το είδος του λειτουργικού συστήματος (windows), που ήταν εγκατεστημένο στον ηλεκτρονικό υπολογιστή, από τον οποίο και λήφθηκε το εν λόγω αντίγραφο. Για το λόγο αυτό, στο χρωματιστό πλαίσιο της εικόνας 4.3.3.1, ορίζεται το είδος και η έκδοση του λειτουργικού (Windows) που ήταν εγκατεστημένο, στο υπό μελέτη σύστημα. Αυτή η ενέργεια επιτυγχάνεται εκτελώντας τις παρακάτω εντολές κονσόλας και αποθηκεύοντας τα αποτελέσματα στο αρχείο με το όνομα final_hdd_image_letter.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δισκου:\collected_information\Registry\software –p winnt_cv > όνομα δίσκου\analyzed_information\hdd\image_letter.txt

Type όνομα δίσκου:\analyzed_information\hdd\image_letter.txt | findstr “ProductName” > όνομα δίσκου:\analyzed_information\hdd\final_hdd_image_letter.txt & type όνομα δίσκου:\ analyzed_information\hdd\image_letter.txt | “BuildLabEx” >> όνομα δίσκου:\ analyzed_information\hdd\final_hdd_image_letter.txt
```

Μετά το πέρας των παραπάνω βημάτων, δημιουργείται και ενεργοποιείται ένας εικονικός δίσκος, που δεν είναι άλλος παρά ένα πλήρες αντίγραφο του δίσκου, του υπο μελέτη συστήματος. Δηλαδή, ο αναλυτής, έχει μπροστά του, ως εικονικό περιβάλλον, το ίδιο, το υπο μελέτη σύστημα. Μπορεί λοιπόν, να περιηγηθεί στα περιεχόμενα του δίσκου αυτού και να εμβαθύνει την ανάλυσή του, με σκοπό την εξαγωγή ακόμα περισσοτέρων συμπερασμάτων. Φυσικά, στην περίπτωση που θέλει να αναλύσει συγκεκριμένες πληροφορίες από το αντίγραφο του πρωτεύοντος δίσκου (HDD), του υπο μελέτη συστήματος, μπορεί εάν θέλει να το επιτύχει μέσα από το λογισμικό μας, αρκεί να επιλέξει μία από τις δυνάτοτητες που του δίνονται.

Δηλαδή, εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών Shortcut Files (.lnk)**»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα, θα αποθηκευτούν στο αρχείο με το όνομα analyzed_recent_files.txt ([31]lnkParser, 2012) :

```
lnk_parser_cmd όνομα δισκου:\collected_information\hdd\users\όνομα χρήστη\recent_files > όνομα δίσκου\analyzed_information\hdd\users\όνομα χρήστη\recent_files\ analyzed_recent _files.txt
```

Κατά αντίστοιχο τρόπο εάν επιλέξει την κατηγορία «Ανάλυση πληροφοριών Jump List**»**, τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα, θα αποθηκευτούν στο αρχείο με το όνομα analyzed_jump_lists.txt ([32]JumpListsView, 2013-2016) :

```
Jumplixtview /recentfolder όνομα δισκου:\collected_information\hdd\users\όνομα χρήστη\ recent_files /sxml όνομα δίσκου\analyzed_information\hdd\users\όνομα χρήστη\jumkp_lists\ analyzed_jump_lists.xls
```

Αν ο αναλυτής επιλέξει την κατηγορία «Ανάλυση πληροφοριών Thumbnail Files**»**, τότε, εκτελείται η ακόλουθη εντολή κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα αποθηκεύονται σε αρχεία με την εξής μορφή ονόματος analyzed_thumbcache_όνομα.txt ([33]Thumbcache Viewer, 2016):

```
Thumbcache_viewer_cmd όνομα δισκου:\collected_information\hdd\users\όνομα χρήστη\ thumbnail_files\thumbcache_όνομα.db > όνομα δίσκου\analyzed_information\hdd\users\ όνομα χρήστη\thumbnail_files/analyzed_thumbcache_όνομα.txt
```

Επόμενη πληροφορία που μπορεί να αναλυθεί είναι σχετικά με τον κάδο ανακύκλωσης. Έτσι, εάν ο αναλυτής επιλέξει την κατηγορία «Ανάλυση πληροφοριών Recycle Bin**»**, τότε, εκτελούνται οι παρακάτω εντολές κονσόλας (για κάθε έναν από τους χρήστες, του υπό μελέτη συστήματος) και τα αποτελέσματα αποθηκεύονται ως αρχεία εντός του υποφακέλου με το όνομα recycle_bin ([34]Abelecheung/Rifiuti2, 2017) και [35]Show Hidden Files Using Attrib Command, 2017):

```
Attrib –s –h –r /s /d

Dir /b > όνομα δίσκου:\analyzed_information\hdd\username_recycle_bin.txt

Rifiuti-vista –x –z –o όνομα δίσκου\analyzed_information\hdd\users\όνομα χρήστη\recycle_bin\analyzed_recycle_bin.xml όνομα δίσκου:\collected_information\hdd\ recycle_bin\όνομα χρήστη
```

Στο σημείο αυτό, ο αναλυτής, εάν επιθυμεί μπορεί να επιλέξει την κατηγορία «Ανάλυση πληροφοριών Windows Event Logs (Application,Security,Software)**»**, αλλά απαιτείται να είναι ήδη εγκατεστημένο στον υπολογιστή του, το λογισμικό Log Parser. Ελέγχεται λοιπόν εάν είναι ήδη εγκατεστημένο και αν δεν είναι, τότε, τον παραπέμπει να πατήσει στο κουμπί με το όνομα «Εγκατάσταση Log Parser» και να ακολουθήσει τα παραίτητα βήματα, όπως αυτά υποδεικνύονται. Στη συνέχεια, εκτελούνται οι παρακάτω εντολές κονσόλας, ενώ τα

αποτελέσματα αποθηκεύονται στα αντίστοιχα αρχεία με τα ονόματα analyzed_application_logs.xml, analyzed_security_logs.xml και analyzed_system_logs.xml ([38]LogParser 2.2, 2017):

```
Logparser “SELECT Timegenerated, SourceName, EventCategoryName, EventId, Message into όνομα δισκου:\analyzed_information\hdd\analyzed_Application_logs.xml FROM όνομα δίσκου\collected_information\hdd\Application_logs_evt” –i:evt –o:xml

Logparser “SELECT Timegenerated, SourceName, EventCategoryName, EventId, Message into όνομα δισκου:\analyzed_information\hdd\analyzed_Security_logs.xml FROM όνομα δίσκου\collected_information\hdd\Security_logs_evt” –i:evt –o:xml

Logparser “SELECT Timegenerated, SourceName, EventCategoryName, EventId, Message into όνομα δισκου:\analyzed_information\hdd\analyzed_System_logs.xml FROM όνομα δίσκου\collected_information\hdd\System_logs_evt” –i:evt –o:xml
```

Η τελευταία δυνατότητα ανάλυσης που δίνεται στον αναλυτή, είναι να επιλέξει την κατηγορία «Βαθιά Ανάλυση για εύρεση Credit Cards,Url Searches, Exifs κλπ», όπου αυτόματα θα εκτελεστεί η επόμενη εντολή κονσόλας και τα αποτελέσματα θα αποθηκευτούν σε υποφάκελο με το όνομα Deep_HDD_Image_Analysis ([41]Bulk Extractor, 2015):

```
Bulk_Extractor32 –o όνομα δίσκου\analyzed_information\hdd\Deep_HDD_Image_Analysis όνομα δίσκου:\collected_information\hdd\OFF\hdd_image.dd
```

Σε κάθε περίπτωση, εάν ο αναλυτής επιθυμεί να λάβει γνώση όλων των παραπάνω, αρκεί να πατήσει στο κουμπί «Επιλογή Όλων», που βρίσκεται στο κάτω μέρος της οθόνης. Σε περίπτωση δε που μετάνοιωσε να λάβει γνώση όλων των πληροφοριών αυτών και θέλει μόνο την ανάλυση ορισμένων εξ αυτών, τότε, του δίνεται η δυνατότητα να πατήσει στο κουμπί «Εκκαθάριση Όλων», ώστε να επιλέξει εξ αρχής μόνο εκείνες που τον ενδιαφέρουν. Μετά το πέρας των παραπάνω ενεργειών, οφείλει να πατήσει στο κουμπί «OK», με σκοπό την έξοδό του από την κατηγορία αυτή. Αυτόματα δε, θα εμφανιστεί μήνυμα σχετικά με την ολοκλήρωση ή μη των αντίστοιχων εντολών κονσόλας (command line), που εκτελούνται και η έξοδος θα πραγματοποιηθεί μετά το πέρας αυτών.

4.3.4 Ανάλυση Αντίγραφου Δίσκου χωρίς Λειτουργικό Σύστημα (HDD)

Ανεξάρτητα με το γεγονός εάν, το υπό μελέτη σύστημα, βρέθηκε ενεργοποιημένο ή απενεργοποιημένο κατά τη χρονική στιγμή της κατάσχεσής του, τα βήματα για την ανάλυση των επιμέρους προσαρτημένων σκληρών δίσκων, χωρίς εγκατεστημένο Λειτουργικό σύστημα, είναι ακριβώς ίδια.

Κατά συνέπεια, μπορείτε να ανατρέξετε στην παράγραφο 4.2.5, προκειμένου να ακολουθήσετε τα απαραίτητα βήμα, για την ανάλυση των πληροροφοριών που εμπεριέχονται σε έναν τέτοιο σκληρό δίσκο (HDD).

4.3.5 Ανάλυση Αφαιρούμενου Μέσου (Usb Flash Disk)

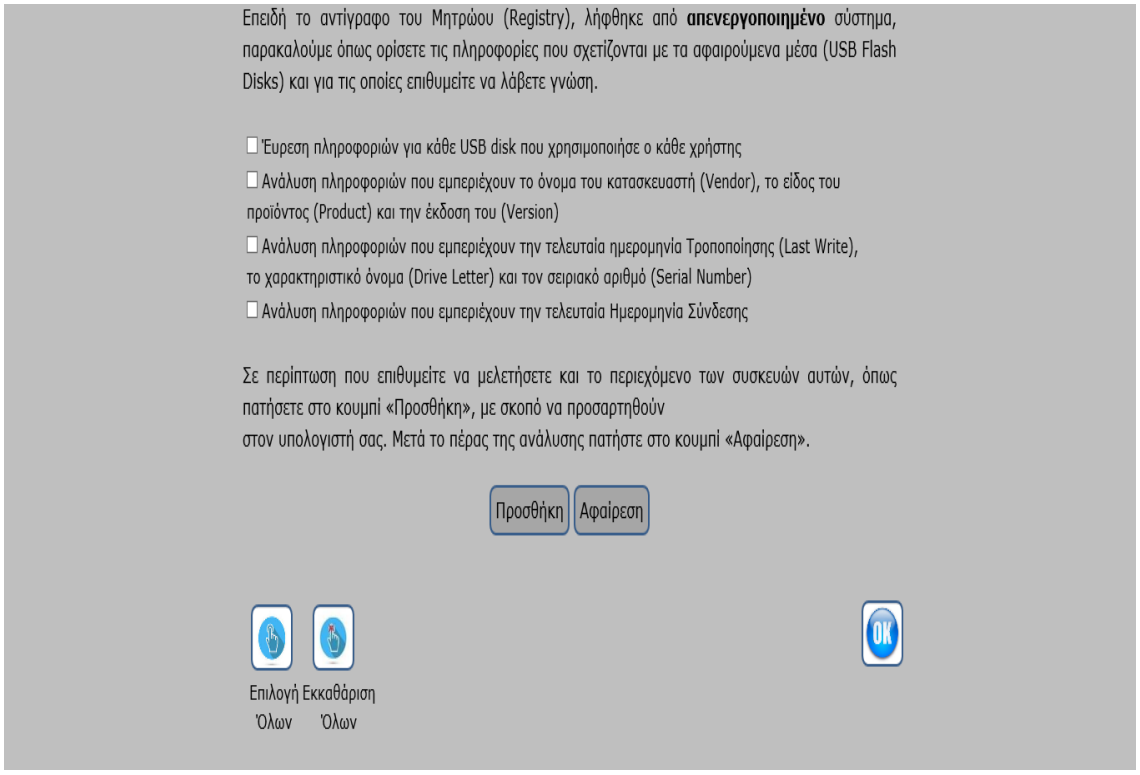
Όπως αναφέραμε και στο υποκεφάλαιο 4.2.6, υπάρχει περίπτωση κατά την κατάσχεση ενός εκθέματος να βρεθούν, πλησίον του, εξωτερικά αποθηκευτικά μέσα, όπως σκληροί δίσκοι (HDD), ή αφαιρούμενα αποθηκευτικά μέσα μικρής χωρητικότητας (Usb Flash Disks).

Και στις δυο αυτές περιπτώσεις, ο αναλυτής, θα πρέπει να τα θεωρεί ως ιδίου τύπου αποθηκευτικές συσκευές, δηλαδή ως «Αφαιρούμενα Μέσα». Μάλιστα, επειδή μπορεί σε

οποιαδήποτε χρονική στιγμή, πριν την κατάσχεση, να έχουν συνδεθεί οι συσκευές αυτές στον ηλεκτρονικό υπολογιστή που μας ενδιαφέρει, γι' αυτό, είναι ορθό να ληφθούν αντίγραφα και από αυτά, καθόσον μπορεί να περιέχουν σημαντικές πληροφορίες.

Μάλιστα, ο αναλυτής, μπορεί να εξάγει σημαντικά συμπεράσματα, όχι μόνο από την ανάλυση του αντιγράφου αυτών των συσκευών, αλλά και από τις πληροφορίες που αποθηκεύτηκαν κατά τη σύνδεση των συσκευών αυτών, στον εν λόγω ηλεκτρονικό υπολογιστή. Οι πληροφορίες αυτές αποθηκεύονται στο Μητρώο του λειτουργικού συστήματος (Registry) και απαιτούν ειδιαίτερο χειρισμό για να μπορέσουμε να τις αντλήσουμε.

Σε κάθε περίπτωση δε, ο ερευνητής, εάν επιθυμεί την ανάλυση των ανωτέρω συσκευών, οφείλει να πατήσει στο κουμπί «Ανάλυση Αφαιρούμενου Μέσου (USB Flash Disk)», με σκοπό να του ανοίξει η παρακάτω σελίδα (Εικόνα 4.3.5.1) στην οποία έχουμε διαχωρίσει τις πληροφορίες που μπορούν να μελετηθούν, σε κάθε μια από τις δύο (2) περιπτώσεις, που προαναφέραμε.



Εικόνα 4.3.5.1: Ανάλυση Αφαιρούμενου Μέσου (USB Flash Disk) από Απενεργοποιημένο Σύστημα

Μόλις ανοίξει η σελίδα, ο αναλυτής, θα πρέπει να πατήσει μονό αριστερό κλικ, στο αντίστοιχο κουτί επιλογής (check box) που βρίσκεται μπροστά από την εκάστοτε έκφραση, με σκοπό την ανίχνευση και την ανάλυση των απαραίτητων πληροφοριών που βρίσκονται στο αντίγραφο του Μητρώου (Registry). Αν λοιπόν επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχουν το όνομα του κατασκευαστή (Vendor), το είδος του προϊόντος (Product) και την έκδοση του (Version)», αυτόματα, θα ξεκινήσει η εκτέλεση της παρακάτω εντολής κονσόλας και τα αποτελέσματα θα αποθηκευτούν στο αρχείο με το όνομα USB_Vendor+Product_Name+Version.txt ([21]Type, 2017) :

```
Type όνομα δίσκου:\collected_information\Registry\system_analysis.txt | find "USBSTOR#" > όνομα δίσκου\analyzed_information\USB\ USB_Vendor+Product_Name+Version.txt
```

Αν όμως επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχουν την τελευταία ημερομηνία Τροποποίησης (Last Write), το χαρακτηριστικό όνομα (Drive Letter) και τον σειριακό αριθμό (Serial Number)», τότε, αυτόματα, θα εκτελεστεί η παρακάτω εντολή κονσόλας και τα

αποτελέσματα θα αποθηκευτούν στο αρχείο με το όνομα USB_Serial+Last_Write+Drive_Letter.txt ([20] RegRipper, 2015) :

```
Rip –r όνομα δίσκου:\collected_information\Registry\software –p removdev > όνομα δίσκου\analyzed_information\USB\ USB_Serial+Last_Write+Drive_Letter.txt
```

Ενώ, εάν επιλέξει την «Ανάλυση πληροφοριών που εμπεριέχουν την τελευταία ημερομηνία Σύνδεσης», τότε, εκτελείται η παρακάτω εντολή κονσόλας και τα αποτελέσματα θα αποθηκευτούν στο αρχείο με το όνομα USB_Last_Time_Connection.txt ([20] RegRipper, 2015):

```
Rip –r όνομα δίσκου:\collected_information\Registry\system –p devclass > όνομα δίσκου\analyzed_information\USB\ USB_Last_Time_Connection.txt
```

Στο σημείο αυτό, έχει ολοκληρωθεί η ανάλυση των πληροφοριών που σχετίζονται με τα εξωτερικά αποθηκευτικά μέσα και οι οποίες βρίσκονταν στο Μητρώο (Registry), του υπό μελέτη συστήματος. Αν ο ερευνητής επιθυμεί να εμβαθύνει την ανάλυσή του, τότε, οφείλει να μελετήσει και τα περιεχόμενα των συσκευών αυτών.

Πατώντας πάνω στο κουμπί «Προσθήκη», προσαρτάται στον υπολογιστή του, ως εικονικό εξωτερικό αποθηκευτικό μέσο, το αντίγραφο που είχε λάβει από την εν λόγω συσκευή (USB Flash Disk). Μάλιστα, στην περίπτωση που είχαν βρεθεί περισσότερες από μία τέτοιου είδους συσκευές, κατά την χρονική στίγμη της κατάσχεσης (άρα έχουν ληφθεί αντίγραφα από όλες αυτές), τότε, πατώντας στο κουμπί αυτό, αυτόματα θα προσαρτηθούν όλα τα αντίγραφα, ως εξωτερικά αποθηκευτικά μέσα του συστήματος, του αναλυτή. Για να επιτευχθεί η ενέργεια αυτή εκτελούνται οι κάτωθι εντολές κονσόλας ([24]Qemu-img for Windows, 2016-2017 και [26]Mounting VHDs in Windows 7 from a Command-Line Script , 2012):

```
Qemu-img convert όνομα δίσκου:\collected_information\USB\όνομα usb δίσκου_image.dd –O vhdx όνομα δίσκου:\analyzed_information\USB\όνομα usb δίσκου.vhdx

Diskpart
Sel vdisk file=”όνομα δίσκου:\analyzed_information\USB\όνομα usb δίσκου.vhdx”
Attach vdisk
```

Ο αναλυτής, μπορεί πλέον να μελετήσει τα δεδομένα που εμπεριέχονται σε αυτά τα εικονικά εξωτερικά αποθηκευτικά μέσα, εξάγοντας με ασφάλεια επιμέρους συμπεράσματα. Μετά το πέρας της ανάλυσης του αυτής, οφείλει να αφαιρέσει από το σύστημά του, αυτά τα εικονικά μέσα. Για να το επιτύχει αυτό, αρκεί να πατήσει στο κουμπί «Αφαίρεση». Με το πάτημα του κουμπιού αυτού, αυτόματα εκτελούνται οι παρακάτω εντολές:

```
Diskpart
Sel vdisk file=”όνομα δίσκου:\analyzed_information\ USB\όνομα usb δίσκου.vhdx”
Detach vdisk
```

Μετά την παραπάνω ενέργεια και πατώντας στο κουμπί «OK», ο αναλυτής, εξέρχεται από την κατηγορία αυτή. Σε περίπτωση όμως που κάποιες ή κάποια από τις παραπάνω εντολές κονσόλας, δεν έχουν τερματίσει, τότε, αυτόματα, θα εμφανιστεί μήνυμα σχετικά με τη μη ολοκλήρωσή τους και η έξοδος θα πραγματοποιηθεί μετά το πέρας τους.

4.3.6 Ανάλυση Αντίγραφου Χρονοδιαγράμματος Ενεργειών (Timeline)

Όπως έχουμε αναφέρει και σε προγενέστερη παράγραφο, είτε το υπό μελέτη σύστημα, βρεθεί ενεργοποιημένο, είτε βρεθεί απενεργοποιημένο, κατά τη χρονική στιγμή της κατάσχεσής του, τα βήματα για την ανάλυση μπορεί να είναι ίδια. Έτσι και στην περίπτωση αυτή, η ανάλυση του

αντιγράφου του χρονοδιαγράμματος ενεργειών, είναι ίδια με εκείνη που περιγράψαμε στην παράγραφο 4.2.7.

Κατά συνέπεια, ο ερευνητής των ψηφιακών πειστηρίων, προκειμένου να συλλέξει το απαραίτητο αρχείο που περιέχει το χρονοδιάγραμμα όλων των πεπραγμένων γεγονότων του υπό μελέτη συστήματος, αλλά και την επιμέρους ανάλυση αυτού, οφείλει να ακολουθήσει τα βήματα της παραγράφου αυτής. Ολόκληρώνοντας την ανάλυση του θα πρέπει να πατήσει στο κουμπί «OK», προκειμένου να επιστρέψει στην αρχική σελίδα της παραγράφου 4.1, από όπου μπορεί, είτε να εξέλθει από την εφαρμογή μας, πατώντας στο κουμπί «Exit», είτε να επιστρέψει στην αρχική σελίδα της παραγράφου 3.1, πατώντας στο κουμπί «Home».

4.4 Ανασκόπηση του Κεφαλαίου 4

Στο κεφάλαιο 4, πραγματοποιήθηκε παρουσίαση των μεθόδων ανάλυσης των συλλεχθέντων πληροφοριών, τόσο από ενεργοποιημένο σύστημα, όσο και από απενεργοποιημένο σύστημα.

Κατόπιν της σχετικής ανάλυσης, δημιουργήθηκαν τα απαραίτητα αρχεία, τα οποία οφείλει να μελετήσει ο υπεύθυνος της εγκληματολογικής έρευνας, προκειμένου να εξάγει με ασφάλεια ένα συμπέρασμα περί την τέλεση ή μη, μιας εκούσιας ή ακούσιας εγκληματικής πράξης, σχετιζόμενης με τους ηλεκτρονικούς υπολογιστές.

Σε κάθε περίπτωση δε, τα συμπερασμάτα αυτά, θα πρέπει να αποδοθούν με πλήρη σαφήνεια και να συμπεριληφθούν στο αντίστοιχο πεδίο της αναφορικής του έκθεσης, που περιγράφεται στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 5 – ΣΥΜΠΛΗΡΩΣΗ ΚΑΙ ΥΠΟΒΟΛΗ ΑΝΑΦΟΡΙΚΗΣ ΕΚΘΕΣΗΣ

5.1 Αξία και Σκοπός Αναφορικής Έκθεσης

Στο συγκεκριμένο κεφάλαιο θα ασχοληθούμε με την αναφορική έκθεση, που οφείλει να συμπληρώσει ο τεχνικός της ψηφιακής εγκληματολογίας, μετά το πέρας της έρευνάς του.

Αρχικά, κατασχέθηκε το έκθεμα και ξεκίνησε η διαδιακασία λαμβάνοντας τα απαιραίτητα αντίγραφα (ψηφιακά πειστήρια). Είτε, το υπό μελέτη σύστημα βρέθηκε ενεργοποιημένο, είτε βρέθηκε απενεργοποιημένο, σε κάθε περίπτωση, το λογισμικό μας, παρείχε την δυνατότητα στο ερευνητή να συλλέξει με δωρεάν εργαλεία, όσο το δυνατόν περισσότερες πληροφορίες που θα τον βοηθούσαν στην έρευνά του. Μάλιστα, οι πληροφορίες αυτές, όχι μόνο αποθηκεύτηκαν σε αρχεία με κατάλληλη ονομασία, αλλά ταυτόχρονα, συμπληρώθηκαν αυτόματα αρκετά από τα πεδία του πίνακα που θα συμπεριληφθούν στην εν λόγω αναφορική έκθεση.

Κατά αντιστοιχία, όταν ο ερευνητής ανέλυσε τα δεδομένα αυτά, με σκοπό να εξάγει με ασφάλεια το συμπέρασμα εάν τελέστηκε ή όχι μια εγκληματική πράξη (που σχετίζεται με ηλεκτρονικούς υπολογιστές), η εφαρμογή μας και πάλι αποθήκευσε τα ανελυμένα δεδομένα και συμπλήρωσε τα αντίστοιχα πεδία του πίνακα αυτού.

Σε κάθε περίπτωση δηλαδή, αρκετά από τα πεδία του πίνακα, που θα αποτελεί το κύριο μέρος της αναφορικής έκθεσης, συμπληρώνονται αυτόματα από το λογισμικό μας, με σκοπό να απλουστεύσουμε το έργο του αναλυτή. Φυσικά, η μελέτη των ανελυμένων δεδομένων και η εξαγωγή του τελικού συμπεράσματος για την τέλεση ή μη μιάς αξιόποινης πράξης, είναι ενέργειες που απαιτούν την ανθρώπινη παρέμβαση.

Ο αναλυτής, οφείλει να μελετήσει με μεγάλη προσοχή, όλα τα δεδομένα που συνέλεξε και ανέλυσε, με σκοπό να αποτυπώσει στην έκθεση αυτή τα συμπεράσματά του. Σε αυτά, θα πρέπει να προσδιορίζεται η πράξη που τελέστηκε, η ημερομηνία τέλεσής της, η ταυτότητα του δράστη (όπου αυτό είναι δυνατό), τα εργαλεία (λογισμικά) που χρησιμοποιήσε για την επίτευξη αυτής της πράξης, οι πιθανές συνέπειες που προκλήθηκαν στο θύμα και τα οφέλη που κέρδισε ο δράστης από την εν λόγω ενέργειά του. Βέβαια, όπου είναι εφικτό, ο αναλυτής θα πρέπει να προσδιορίζει και τις τυχόν ενέργειες που οφείλει να ακολουθήσει το θύμα, με σκοπό την αποκατάσταση της ορθής λειτουργίας του συστήματός του.

Συνολικά, τόσο η αναφορική έκθεση, όσο και τα αντίστοιχα δεδομένα που συλλέχθηκαν και αναλύθηκαν, θα κατατεθούν στις αρμόδιες δικαστικές αρχές και θα αποτελούν αποδεικτικά στοιχεία, στην περίπτωση εκδίκασης, αυτής της αξιόποινης πράξης.

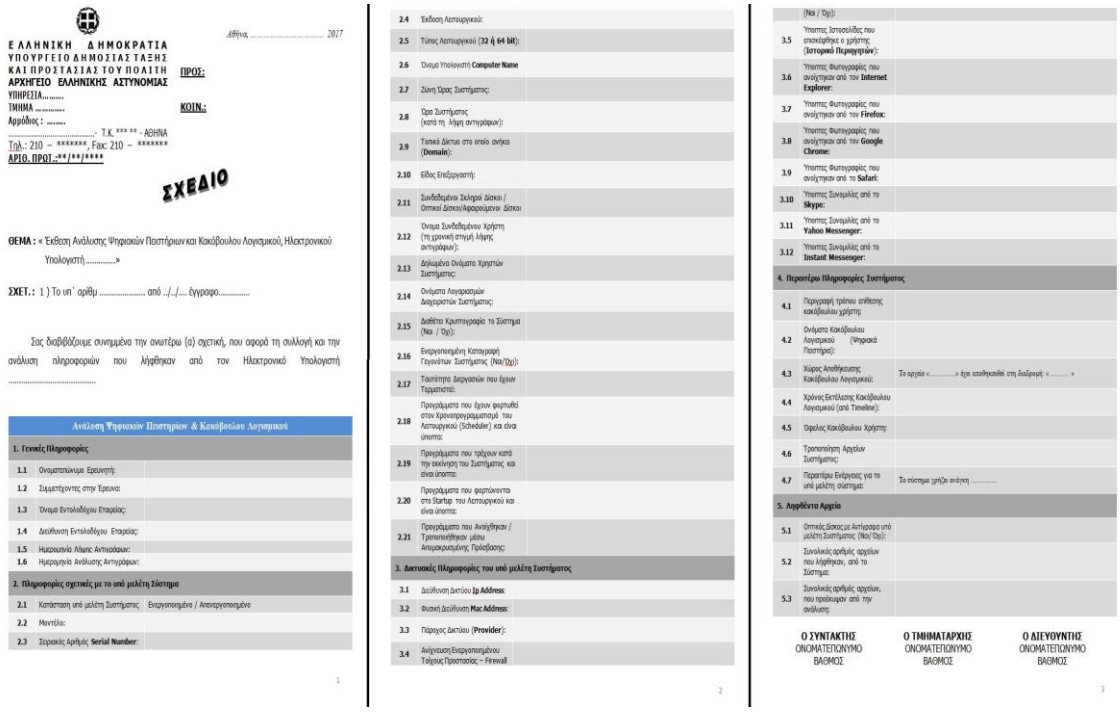
Όπως καταλαβαίνουμε, η έκθεση αυτή είναι πάρα πολύ σημαντική, καθόσον μπορεί να ενοχοποιήσει ή να αθωώσει ένα άτομο και για το λόγο αυτό θα πρέπει να συμπληρώνεται μετά από διεξοδική και μεθοδευμένη έρευνα και ανάλυση.

5.2 Συμπλήρωση Πίνακα Ψηφιακών Πειστηρίων

Κατά τη συλλογή των ψηφιακών πειστηρίων, αυτόματα, συμπληρώνονται κάποια από τα πεδία του πίνακα που θα συμπεριληφθούν στην αναφορική έκθεση (Εικόνα 5.2.1).

Πιο συγκεκριμένα τα πεδία της κατηγορίας 1 (1.1 έως και 1.6) συμπληρώνονται από την αντίστοιχη σελίδα της εφαρμογής μας, όπου ο ερευνητής καλείται να συμπληρώσει τα απαραίτητα πεδία (παράγραφος 3.1). Τα πεδία της κατηγορίας 2 (2.1 έως και 2.21) συμπληρώνονται, αυτόματα, όταν ο ερευνητής επέλεξε την κατηγορία «Γενικές Πληροφορίες» της «Συλλογής Πληροφοριών» (παράγραφος 3.2 ή 3.3.1). Της κατηγορίας 3, τα πεδία συμπληρώνονται από τις αντίστοιχες πληροφορίες της κατηγορίας «Πληροφορίες Δικτύου & Περιηγητών Ιστού (Network – Email- Browsers)» (παράγραφος 3.2.2 ή 3.3.2). Τα δε πεδία της

κατηγορίας 4 (4.1 εώς και 4.7) θα πρέπει να συμπληρώνονται από τον αναλυτή, αφού όμως πρώτα έχει αναλύσει σχολαστικά, όλα τα συλλεχθέντα ψηφιακά πειστήρια.



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΔΗΜΟΣΙΑΣ ΤΑΞΗΣ
ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ.....
ΤΜΗΜΑ .....
Αρμόδιος : .....
..... - Τ.Κ ***** - ΑΘΗΝΑ
Τηλ.: 210 – *******, Fax: 210 – *******
ΑΡΙΘ. ΠΡΩΤ.:**/**/****

Αθήνα, ... 2017

ΠΡΟΣ:

ΚΟΙΝ.:

ΣΧΕΔΙΟ

ΘΕΜΑ : « Έκθεση Ανάλυσης Ψηφιακών Πειστήριων και Κακόβουλου Λογισμικού, Ηλεκτρονικού Υπολογιστή.....»

ΣΧΕΤ.: 1.) Το υπ΄ αριθμ ..... από ../../..... έγγραφο.....

Σας διαβιβάζουμε συνημμένα την αναλυτέρω (α) σχετική, που αφορά τη συλλογή και την ανάλυση πληροφοριών που λήφθηκαν από τον Ηλεκτρονικό Υπολογιστή .....

Ανάλυση Ψηφιακών Πειστηρίων & Κακόβουλου Λογισμικού		
1. Γενικές Πληροφορίες		
1.1	Ονοματεπώνυμο Ερευνητή:	
1.2	Συμμετέχοντες στην Έρευνα:	
1.3	Όνομα Εντολοδόχου Εταιρίας:	
1.4	Διεύθυνση Εντολοδόχου Εταιρίας:	
1.5	Ημερομηνία Λήψης Αντιγράφων:	
1.6	Ημερομηνία Ανάλυσης Δεντγράφων:	
2. Πληροφορίες σχετικές με το υπό μελέτη Σύστημα		
2.1	Κατάσταση υπό μελέτη Συστήματος:	Ενεργοποιημένο / Απενεργοποιημένο
2.2	Μοντέλο:	
2.3	Σειριακός Αριθμός **Serial Number**:	

2.4	Έκδοση Λειτουργικού:	
2.5	Τύπος Λειτουργικού (**32 ή 64 bit**):	
2.6	Όνομα Υπολογιστή **Computer Name**	
2.7	Ζώνη Ώρας Συστήματος:	
2.8	Ώρα Συστήματος (κατά τη λήψη αντιγράφων):	
2.9	Τοπικό Δίκτυο στο οποίο ανήκει (**Domain**):	
2.10	Είδος Επεξεργαστή:	
2.11	Συνδεδεμένοι Σκληροί Δίσκοι / Οπτικοί Δίσκοι/Αφαιρούμενοι Δίσκοι	
2.12	Όνομα Συνδεδεμένου Χρήστη (τη χρονική στιγμή λήψης αντιγράφων):	
2.13	Δημιμένα Ονόματα Χρηστών Συστήματος:	
2.14	Ονόματα Λογαριασμών Διαχειριστών Συστήματος:	
2.15	Διαθέτει Κρυπτογράφηση το Σύστημα (Ναι / Όχι):	
2.16	Ενεργοποιημένη Κατηγορική Γεγονότων Συστήματος (Ναι/Όχι):	
2.17	Ταυτότητα Διεργασιών που έγιναν Τερματιστεί:	
2.18	Προγράμματα που έχουν φορτωθεί στον Χρονοπρογραμματιστή του Λειτουργικού (Scheduler) και είναι ύποπτα:	
2.19	Προγράμματα που τρέχουν κατά την εκκίνηση του Συστήματος και είναι ύποπτα:	
2.20	Προγράμματα που φορτώνονται στο Startup του Λειτουργικού και είναι ύποπτα:	
2.21	Προγράμματα που Ανοίχθηκαν / Τρεπαναίχθηκαν μέσω Απομακρυσμένης Πρόσβασης:	
3. Δικτυακές Πληροφορίες του υπό μελέτη Συστήματος		
3.1	Διεύθυνση Δικτύου **Ip Address**:	
3.2	Φυσική Διεύθυνση **Mac Address**:	
3.3	Πάροχος Δικτύου (**Provider**):	
3.4	Ανίχνευση Ενεργοποιημένου Τοίχους Προστασίας – Firewall	

	(Ναι / Όχι):	
3.5	Ύπαρτες Ιστοσελίδες που επισκεμθήκε ο χρήστης (**Ιστορικό Περιηγητών**):	
3.6	Ύπαρτες Φωτογραφίες που ανοίχτηκαν από τον **Internet Explorer**:	
3.7	Ύπαρτες Φωτογραφίες που ανοίχτηκαν από τον **Firefox**:	
3.8	Ύπαρτες Φωτογραφίες που ανοίχτηκαν από τον **Google Chrome**:	
3.9	Ύπαρτες Φωτογραφίες που ανοίχτηκαν από το **Safari**:	
3.10	Ύπαρτες Συνομιλίες από το **Skype**:	
3.11	Ύπαρτες Συνομιλίες από το **Yahoo Messenger**:	
3.12	Ύπαρτες Συνομιλίες από το **Instant Messenger**:	
4. Περαιτέρω Πληροφορίες Συστήματος		
4.1	Περιγραφή τρόπου απέθεσης κακόβουλου χρήστη:	
4.2	Ονόμαστο Κακόβουλου Λογισμικού (Ψηφιακά Πειστήρια):	
4.3	Χώρος Αποθήκευσης Κακόβουλου Λογισμικού:	Το αρχείο «.....» ήχη αποθηκεθεί στη διαδρομή: «..... »
4.4	Χρόνος Εκτέλεσης Κακόβουλου Λογισμικού (από Timeline):	
4.5	Όφελος Κακόβουλου Χρήστη:	
4.6	Τροποποίηση Αρχείων Συστήματος:	
4.7	Περαιτέρω Ενέργειες για το υπό μελέτη σύστημα:	Το σύστημα χρήζει ανάγκη .....
5. Αγνθέντα Αρχεία		
5.1	Οπτικός Δίσκος με Αντίγραφα υπό μελέτη Συστήματος (Ναι/Όχι):	
5.2	Συνολικός αριθμός αρχείων που λήφθηκαν, από το Σύστημα:	
5.3	Συνολικός αριθμός αρχείων, που προέκυψαν από την ανάλυση:	

Ο ΣΥΝΤΑΚΤΗΣ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ
ΒΑΘΜΟΣ

Ο ΤΜΗΜΑΤΑΡΧΗΣ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ
ΒΑΘΜΟΣ

Ο ΔΙΕΥΘΥΝΤΗΣ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ
ΒΑΘΜΟΣ

Εικόνα 5.2.1: Υπόδειγμα Αναφορικής Έκθεσης συμπεριλαμβανομένου του Πίνακα Δεδομένων

Τέλος, τα πεδία της κατηγορίας 5 (5.1 έως και 5.3) συμπληρώνονται υποχρεωτικά από την εφαρμογή με σκοπό να αναγράφεται στην αναφορική έκθεση, τόσο το πλήθος των αρχείων που περιλαμβάνουν τα ληφθέντα ψηφιακά πειστήρια, όσο και το πλήθος των αρχείων που περιλαμβάνουν τις αναλύσεις των δεδομένων αυτών. Τα πεδία της κατηγορίας αυτής διασφαλίζουν την ακεραιότητα και την διαθεσιμότητα, των ψηφιακών πειστηρίων αυτών ([56]Confidentiality-Intergrity-Availability CIA Triad, 1999-2017).

5.4 Ανασκόπηση του κεφαλαίου 5

Στο κεφάλαιο 5, προσδιορίσαμε την σημαντικότητα της αναφορικής έκθεσης που οφείλει να συμπληρώσει ο εκάστοτε τεχνικός της ψηφιακής εγκληματολογίας, στην περίπτωση που έχει επιφορτιστεί με την μελέτη ενός συστήματος, για την εξαγωγή του συμπεράσματος, εάν έχει τελεστεί ή όχι μια αξιόποινη πράξη που σχετίζεται με τους ηλεκτρονικούς υπολογιστές.

Όπως θα δούμε, στο επόμενο κεφάλαιο, τόσο οι πληροφορίες της αναφοράς αυτής μπορούν να εμπλουτιστούν, όσο και ολόκληρο το λογισμικό μας, μπορεί να εξελιχθεί-αναβαθμιστεί.

ΚΕΦΑΛΑΙΟ 6 – ΕΞΑΓΩΓΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ - ΠΡΟΤΑΣΕΙΣ ΠΕΡΑΙΤΕΡΩ ΕΠΕΚΤΑΣΕΩΝ

6.1 Συνολική ανασκόπηση της εργασίας και γενική συμπεράσματα

Στην παρούσα μεταπτυχιακή εργασία πραγματοποιήθηκαν τα κάτωθι:

- Βιβλιογραφική μελέτη των όρων «Εγκληματολογία», «Ψηφιακή Εγκληματολογία» και εντοπισμός των βημάτων μιας ψηφιακής εγκληματολογικής έρευνας.
- Διενεργήθηκε σχετική έρευνα στην παγκόσμια επιστημονική βιβλιοθήκη και στο διαδίκτυο, για τον εντοπισμό κατάλληλων δωρεάν εργαλείων για τη συλλογή και ανάλυση πληροφοριών, από ηλεκτρονικό υπολογιστή.
- Υλοποιήσαμε λογισμικό, το οποίο παρέχει την δυνατότητα συλλογής και ανάλυσης πληροφοριών, από σύστημα, στο οποίο έχει λάβει πρόσβαση μη εξουσιοδοτημένος χρήστης. Πιο συγκεκριμένα, κατά τη συλλογή, παρέχει την δυνατότητα λήψης πληροφοριών ανάλογα με το εάν, το υπό μελέτη σύστημα, βρέθηκε ενεργοποιημένο ή απενεργοποιημένο, κατά τη χρονική στιγμή της κατάσχεσής του. Ενώ, ως προς το δεύτερο σκέλος αυτού, ανάλογα την κατάσταση του συστήματος, κατά την λήψη των πληροφοριών, παρέχονται τα κατάλληλα εργαλεία ανάλυσης πληροφοριών και εξαγωγής ασφαλών συμπερασμάτων.
- Αναπτύξαμε κατάλληλη διαδικασία μέσω της οποίας δημιουργείται αυτόματα κατά την συλλογή πληροφοριών, αναφορική έκθεση η οποία περιλαμβάνει σημαντικές πληροφορίες σχετικές με τα ληφθέντα δεδομένα. Η έκθεση αυτή δε, ενημερώνεται αυτόματα κατά την ανάλυση των συλλεχθέντων πληροφοριών και η οποία θα κατατεθεί με το πέρας των εγκληματολογικών ερευνών στην υπηρεσία που διέταξε την εγκληματολογική έρευνα ή στην αντίστοιχη εντολοδόχο εταιρία.
- Παρουσιάσαμε τον τρόπο λειτουργίας του λογισμικού που υλοποιήσαμε και εξάγαμε συμπεράσματα σχετικά με τυχόν μελλοντικές βελτιώσεις ή επεκτάσεις αυτού.

6.2 Περαιτέρω επεκτάσεις

Η τρέχουσα μεταπτυχιακή εργασία, μπορεί, τόσο να βελτιωθεί, όσο και να επεκταθεί. Ως προς τις βελτιώσεις της, προτείνουμε τα εξής:

1. Εύρεση διαφορετικού λογισμικού, που να υποστηρίζει την ανάλυση της μνήμης ηλεκτρονικού υπολογιστή, στον οποίο έχει εγκατασταθεί το λειτουργικό σύστημα των Windows 10. Φυσικά, θα μπορεί να χρησιμοποιηθεί, όχι μόνο ένα νέο λογισμικό, αλλά και το ήδη υπάρχον (volatility) αρκεί να αντικατασταθεί η χρησιμοποιηθείσα έκδοση «2.5.win.standalone» με νεότερη, η οποία θα μπορεί να εντοπίσει το κατάλληλο προφίλ του λειτουργικού συστήματος των windows 10, το οποίο απαιτείται για την ανάλυση των δεδομένων της μνήμης.
2. Αντικατάσταση του λογισμικού «FTK Imager Lite» και πιο συγκεκριμένα της έκδοσης «Imager_Lite_3.1.1» με διαφορετικό λογισμικό, το οποίο θα χρησιμοποιεί εντολές κονσόλας (command line) και όχι οπτικό περιβάλλον (interface) για την συλλογή του μητρώου του λειτουργικού συστήματος των windows. Βέβαια, επειδή ήδη αναπτύσσονται οι εκδόσεις «command line versions of FTK Imager» και το «AccessData Triage» συνιστάται η χρήση αυτού, που θα υποστηρίζει τις εντολές κονσόλας και θα είναι δωρεάν.
3. Προσθήκη κατάλληλου λογισμικού στην κατηγορία «Συλλογή Πληροφοριών/ Πληροφορίες Δικτύου & Περιηγητών Ιστού», τόσο σε ενεργοποιημένο, όσο και σε

απενεργοποιημένο σύστημα, για την συγκέντρωση δεδομένων που σχετίζονται με την χρήση του λογισμικού «Facebook».

4. Προσθήκη κατάλληλου λογισμικού στην κατηγορία «Συλλογή Πληροφοριών/ Πληροφορίες Δικτύου & Περιηγητών Ιστού», τόσο σε ενεργοποιημένο, όσο και σε απενεργοποιημένο σύστημα, για την συγκέντρωση δεδομένων που σχετίζονται με τυχόν συνομιλίες του χρήστη, με την χρήση του λογισμικού «Viber».
5. Χρήση κατάλληλου βοηθητικού λογισμικού CSS, για τη βελτιστοποίηση των γραφικών, τόσο των σελίδων του λογισμικού, όσο και την αυτοματοποίηση του λογισμικού μας, για την παραμετροποίηση των γραφικών και των αναλύσεων, ανάλογα πάντα με τις εκάστοτε ρυθμίσεις των χρηστών.
6. Συγγραφή όλων των μηνυμάτων/κουμπιών του λογισμικού και στην αγγλική γλώσσα με ταυτόχρονη προσθήκη στην αρχική σελίδα κατάλληλων εικονιδίων με την «Ελληνική» και την «Αγγλική» γλώσσα, ώστε να είναι δυνατή η χρήση του λογισμικού μας και από χρήστες που δεν ομιλούν την ελληνική γλώσσα.

Όσον αφορά τις πιθανές μελλοντικές επεκτάσεις του αναπτυχθέν λογισμικού μας, μπορούμε να προσφέρουμε τις παρακάτω προτάσεις:

1. Παραμετροποίηση του λογισμικού μας, με σκοπό την δυνατότητα υποστήριξης για την λήψη (acquisition) και ανάλυση (analysis) πληροφοριών και από κινητή τηλεφωνική συσκευή. Η παραμετροποίηση αυτή θα περιλαμβάνει φυσικά την δημιουργία μίας επιπλέον σελίδας, πριν την σημερινή αρχική σελίδα, όπου θα καλείται ο ερευνητής να επιλέξει εάν, το υπό μελέτη σύστημα, είναι ηλεκτρονικός υπολογιστής ή κινητή τηλεφωνική συσκευή.
2. Εγκατάστατη του λογισμικού μας, σε έναν «web server» στον οποίο θα έχουν πρόσβαση μόνο οι ερευνητές εκείνοι που έχουν προβεί σε σχετική εγγραφή, για την απόκτηση κατάλληλών διαπιστευτηρίων (όνομα χρήστη – username και κωδικό πρόσβασης - password). Στον server αυτό, θα είναι εγκατεστημένα και όλα τα απαραίτητα εργαλεία, των οποίων η ακεραιότητα θα ελέγχεται περιοδικά, από βοηθητικό πρόγραμμα το οποίο και θα αναπτύξουμε.

Σκοπός των παραπάνω μελλοντικών επεκτάσεων είναι η δημιουργία μιας ολοκληρωμένης πλατφόρμας που θα υποστηρίζει τη μελέτη, όχι μόνο ηλεκτρονικών υπολογιστών, αλλά και κινητών τηλεφωνικών συσκευών. Η πλατφόρμα αυτή να αναπτυχθεί στα πλαίσια Διδακτορικής Διατριβής του συντάξα, της εν λόγω Μεταπτυχιακής εργασίας και να εγκατασταθεί σε server του Πανεπιστημίου Πειραιά, δίνοντας άμεση και δωρεάν πρόσβαση σε όλους τους φοιτητές του Μεταπτυχιακού Προγράμματος της Πληροφορικής «Προηγμένα Πληροφοριακά Συστήματα/ Τεχνολογίες Διαχείρισης Ασφάλειας».

Ταυτόχρονα, με την εγκατάσταση της ανωτέρω πλατφόρμας, να εγκατασταθούν και όλες οι απαραίτητες ασφαλιστικές δικλίδες, με σκοπό την παροχή μιας ολοκληρωμένης και ασφαλούς λύσης για εγκληματολογικές έρευνες (Digital Forensics), τόσο σε εκπαιδευτικό επίπεδο (από τους φοιτητές), όσο και σε παγκόσμιο επίπεδο (από ερευνητές) προάγοντας το έργο και το επίπεδο του τμήματος της Πληροφορικής του Πανεπιστημίου Πειραιά.

Βιβλιογραφία

[1] Wikipedia - The Free Encyclopedia. (2017, January 10). Retrieved from https://en.wikipedia.org/wiki/Digital_forensics

[2] Wikipedia - The Free Encyclopedia. (2017, January 27). Retrieved from Digital Forensics: https://en.wikipedia.org/wiki/Forensic_science
[3] Wikipedia - The Free Encyclopedia. (2016, December 18). Retrieved from Digital Forensics Process: https://en.wikipedia.org/wiki/Digital_forensic_process
[4]NirSoft. (2010-2016). Retrieved from WinPrefetchView v1.35: http://www.nirsoft.net/utils/win_prefetch_view.html
[5]EaseUS. (2004-2017). Retrieved from NTFS physical structure: http://www.easeus.com/resource/ntfs-disk-structure.htm
[6]Microsoft Developer Software. (2017). Retrieved from https://msdn.microsoft.com/en-us/library/bb742610.aspx
[7]Microsoft Technet. (2017). Retrieved from Using Netsh : https://technet.microsoft.com/en-us/library/bb490939.aspx

[8]Microsoft TechNet. (2016). Retrieved from Windows SysInternals: https://technet.microsoft.com/en-us/sysinternals/bb896649

[9]NirSoft. (2012-2017). Retrieved from BrowsingHistoryView v1.95 - View browsing history of your Web browsers: http://www.nirsoft.net/utils/browsing_history_view.html

[10]NirSoft. (2007-2016). Retrieved from IECacheView v1.58 - Internet Explorer Cache Viewer: http://www.nirsoft.net/utils/ie_cache_viewer.html

[11]NirSoft. (2007-2015). Retrieved from MZCacheView v1.69 - View the cache files of Mozilla/Firefox browsers: http://www.nirsoft.net/utils/mozilla_cache_viewer.html
[12]NirSoft. (2008-2016). Retrieved from ChromeCacheView v1.70 - Cache viewer for Google Chrome Web browser: http://www.nirsoft.net/utils/chrome_cache_view.html
[13]NirSoft. (2011-2012). Retrieved from SafariCacheView v1.11 : http://www.nirsoft.net/utils/safari_cache_view.html
[14]Microsoft Technet. (2016). Retrieved from Windows SystInternals: https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx
[15]Microsoft Technet. (n.d.). Retrieved from Cipher : https://technet.microsoft.com/en-us/library/bb490878.aspx
[16]LifeWire. (2017). Retrieved from Net Command Examples, Switches, and More: http://pcsupport.about.com/od/commandlinereference/p/net-command.html
[17]Microsoft Technet. (2017). Retrieved from https://technet.microsoft.com/en-us/library/bb491007.aspx
[18]Crysocome. (2010, July 17). Retrieved from DD for windows: http://www.chrysocome.net/dd
[19]Access Data. (2016). Retrieved from FTK® Imager Lite 3.1.1: http://marketing.accessdata.com/ftkimagerlite3.1.1
[20] RegRipper. (2015, 12 06). Retrieved from http://brettshavers.cc/index.php/brettsblog/entry/regripper
[21]Type. (2017). Retrieved from Microsoft/TechNet: https://technet.microsoft.com/en-us/library/cc732507.aspx
[22]NirSoft. (2006-2016). Retrieved from USBDeview v2.62: http://www.nirsoft.net/utils/usb_devices_view.html
[23]Magnet Forensics. (2017). Retrieved from Encrypted Disk Detector: https://www.magnetforensics.com/free-tool-encrypted-disk-detector/
[24]Qemu-img for Windows. (2016-2017). Retrieved from https://cloudbase.it/qemu-img-windows/

[25]Chrysocome.net. (2010, July 17). Retrieved from DD for Windows: http://www.chrysocome.net/dd
[26]Mounting VHDs in Windows 7 from a Command-Line Script . (2012, 01 04). Retrieved from http://nicj.net/mounting-vhds-in-windows-7-from-a-command-line-script/
[27]NirSoft. (2011-2016). Retrieved from DriveLetterView v1.46 : http://nirsoft.net/utils/drive_letter_view.html
[28]Dkovar/AnalyzeMFT. (2017). Retrieved from https://github.com/dkovar/analyzeMFT
[29]Py2EXE. (2014, 09 02). Retrieved from http://www.py2exe.org/
[30]WikiHow to do anything. (2017, February 03). Retrieved from How to Copy Files in Command Prompt: http://www.wikihow.com/Copy-Files-in-Command-Prompt
[31]InkParser. (2012, 03 11). Retrieved from https://code.google.com/archive/p/lnk-parser/
[32]JumpListsView. (2013-2016). Retrieved from NirSoft: http://www.nirsoft.net/utils/jump_lists_view.html
[33]Thumbcache Viewer. (2016, 10 25). Retrieved from https://thumbcacheviewer.github.io/
[34]Abelecheung/Rifiuti2. (2017). Retrieved from https://github.com/abelcheung/rifiuti2
[35]Show Hidden Files Using AttribCommand. (2017). Retrieved from http://visihow.com/Show_Hidden_Files_Using_Command_Prompt
[36]NirSoft. (2008-2014). Retrieved from SkypeLogView v1.55 - Skype Log Viewer (.dbb and main.db files): http://www.nirsoft.net/utils/skype_log_view.html
[37]Windows Command Line. (n.d.). Retrieved from Backup / Delete event log files: https://www.windows-commandline.com/backup-delete-event-log-files/
[38]LogParser 2.2. (2017). Retrieved from Microsoft\TechNet: https://technet.microsoft.com/en-us/scriptcenter/dd919274.aspx
[39]Microsoft TechNet. (2017). Retrieved from Vssadmin list shadows: https://technet.microsoft.com/en-us/library/cc788116(v=ws.11).aspx
[40]NirSoft. (2015-2017). Retrieved from TaskSchedulerView v1.25: http://www.nirsoft.net/utils/task_scheduler_view.html
[41]Bulk Extractor. (2015, 06 10). Retrieved from http://www.forensicswiki.org/wiki/Bulk_extractor
[42]Using Log2TimeLine. (2017). Retrieved from Log2TimeLine/ Plaso: https://github.com/log2timeline/plaso/wiki/Using-log2timeline
[43]Plaso - Google & Timelines. (2014, 11 10). Ανάκτηση από https://malwerewolf.com/2014/11/plaso-google-timelines/
[44]Technet/Move. (2017). Retrieved from Microsoft/Technet: https://technet.microsoft.com/en-us/library/bb490935.aspx
[45]NirSoft. (2007-2015). Retrieved from MyLastSearch v1.64 - View your search engine query in Google and others: http://www.nirsoft.net/utils/my_last_search.html
[46]NirSoft. (2009-2017). Retrieved from OutlookAttachView v2.98 - View/Extract/Save Outlook Attachments: http://www.nirsoft.net/utils/outlook_attachment.html
[47]NirSoft. (2009-2016). Retrieved from OutlookStatView v2.07: http://www.nirsoft.net/utils/outlook_statistics.html
[48]Forensicswiki. (2016, October 20). Retrieved from Personal Folder File (PAB, PST, OST): http://www.forensicswiki.org/wiki/Personal_Folder_File_(PAB,_PST,_OST)
[49]NirSoft. (2004-2013). Retrieved from FavoritesView v1.32: http://www.nirsoft.net/utils/faview.html
[50]NirSoft. (2004-2016). Retrieved from MZCookiesView v1.51: Cookies Manager For Mozilla/Firefox/Netscape Browsers: http://www.nirsoft.net/utils/mzcv.html
[51]Rifiuti2/Readme. (2017). Retrieved from https://github.com/abelcheung/rifiuti2/blob/master/README.md
[52]Magnet Forensics. (2017). Retrieved from Acquiring Memory with Magnet RAM Capture: https://www.magnetforensics.com/computer-forensics/acquiring-memory-with-magnet-ram-capture/
[53]Volatility-GitHub. (2017). Retrieved from https://github.com/volatilityfoundation/volatility/wiki/Command-Reference
[54}SleuthKit. (n.d.). Retrieved from FLS - List file and directory names in a disk image. : http://www.sleuthkit.org/sleuthkit/man/fls.html

[55]Microsoft Technet. (2017). Retrieved from Wevtutil: https://technet.microsoft.com/en-us/library/cc732848(v=ws.11).aspx
[56]Confidentiality-Integrity-Availability CIA Triad. (n.d.). Retrieved 1999-2017, from WhatIs.com: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS