Πανεπιστήμιο Πειραιώς – Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών «Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Δικανική Εξέταση των υπηρεσιών Cloud Storage**
Ονοματεπώνυμο Φοιτητή	**Σμέρος Γεώργιος**
Πατρώνυμο	**Χαράλαμπος**
Αριθμός Μητρώου	**MTE/1131**
Επιβλέπων	**Χρήστος Ξενάκης, Επίκουρος Καθηγητής**

Πειραιάς Οκτώβριος 2013

Τριμελής Εξεταστική Επιτροπή

Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα
(υπογραφή)	(υπογραφή)	(υπογραφή)

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Αντί Προλόγου

Το Cloud Storage αποτελεί την νέα πρόκληση που πρέπει να αντιμετωπίσουν οι δικανικοί ερευνητές. Υπάρχουν διάφοροι τύποι cloud υπηρεσιών, με το κάθε είδος να έχει μια δυνητικά διαφορετική χρήση σε εγκληματική δραστηριότητα. Η δυσκολία έγκειται στον προσδιορισμό και την απόκτηση (ή αλλιώς διατήρηση) των πιθανών δεδομένων όταν χρησιμοποιούνται ανόμοιες υπηρεσίες. Η επικοινωνία και η συνεργασία με τους παρόχους των υπηρεσιών για την ανάκτηση των αποθηκευμένων αρχείων είναι μια χρονοβόρα διαδικασία. Για αυτό οι ερευνητές πρέπει να γνωρίζουν που αποθηκεύονται τοπικά τα δεδομένα της εφαρμογής.

Υπάρχει η ανάγκη για ένα πλαίσιο ψηφιακής εγκληματολογικής έρευνας που να είναι προσαρμοσμένο στις απαιτήσεις και στις ιδιαιτερότητες των υπηρεσιών αυτών Σε αυτήν την διατριβή προτείνεται ένα πλαίσιο βασιζόμενο στις υπάρχουσες μεθοδολογίες.

Χρησιμοποιώντας δημοφιλείς Cloud υπηρεσίες αποθήκευσης όπως το Evernote,το SpiderOak, και το Box, εφαρμόστηκε το προτεινόμενο πλαίσιο κατά την δικανική έρευνα σε έναν υπολογιστή με Windows 7. Εξετάστηκε μια ποικιλία σεναρίων συμπεριλαμβανομένων διάφορων μεθόδων διακίνησης των αρχείων και πρόσβασης στις υπηρεσίες αυτές. Με τον καθορισμό των υπολειμμάτων των δεδομένων στο υπολογιστικό σύστημα, η έρευνα αυτή συμβάλλει στην καλύτερη κατανόηση των artifacts που είναι πιθανό να συναντήσουν οι ερευνητές στο στάδιο της αναγνώρισης. Τέτοιες πιθανές πηγές πληροφοριών αποτελούν τα αρχεία της εφαρμογής, το ιστορικό του περιηγητή και η μνήμη RAM.

Αξίζει να σημειωθεί είναι ότι ήταν δυνατόν να εντοπίσουμε το όνομα χρήστη και τον κωδικό πρόσβασης και για τις τρεις εξεταζόμενες υπηρεσίες.

Με την ανάλυση των δεδομένων διαπιστώσαμε ότι δεν υπήρχαν αλλαγές στο περιεχόμενο των φακέλων στα σενάρια που εξετάσαμε. Ωστόσο οι χρονοσφραγίδες (timestamps) των αρχείων άλλαξαν, κάτι που πρέπει να ληφθεί υπόψιν κατά την δημιουργία της χρονικής αλληλουχίας των γεγονότων.

Παρά το γεγονός ότι η χρήση και ο διαμοιρασμός λογισμικού που φιλοξενείται στο Διαδίκτυο είναι το επόμενο βήμα στην εκμετάλλευσή του World Wide Web, μπορεί να αποτελέσει, ωστόσο μια πρόκληση για τους ερευνητές της ψηφιακής εγκληματολογίας. Η εξάρτηση των ατόμων και των επιχειρήσεων από τους διάφορους παρόχους των Cloud υπηρεσιών (Saas/PaaS/IaaS) δύναται να παρεμποδίσει την διαδικασία της εγκληματολογικής έρευνας.

Κεφάλαιο 1: Εισαγωγή

Ο σκοπός αυτού του κεφαλαίου είναι να παράσχει μια εισαγωγή και να παρουσιάσει τη συνολική δομή της διατριβής. Αυτό το κεφάλαιο περιγράφει επίσης τους κύριους στόχους της έρευνας στα πλαίσια της εγκληματολογικής ανάλυσης των υπηρεσιών Cloud Storage.Τέλος ακολουθεί μια σύντομη περιγραφή της δομής της διατριβής.

Σαν ψηφιακή εγκληματολογία υπολογιστών ορίζεται η διαδικασία της αναγνώρισης, διατήρησης, ανάλυσης και παρουσίασης των ψηφιακών τεκμηρίων με τρόπο που να είναι νομικά αποδεκτός. (McKemmish, 1999)

Υπάρχουν επίσης σαφές καθορισμένες αρχές που διέπουν την διεξαγωγή της ηλεκτρονικής εγκληματολογικής έρευνας. Αυτές είναι:

1. Καμία ενέργεια δε δύναται να μεταβάλει δεδομένα που τηρούνται σε υπολογιστή ή μέσο αποθήκευσης, τα οποία μπορεί να προσκομισθούν στο δικαστήριο.
2. Χρήση αρχέτυπων δεδομένων από τρίτο άτομο, κατόπιν εξουσιοδότησης.
3. Στην περίπτωση που ένα άτομο θεωρεί ότι είναι απαραίτητη η πρόσβαση στα αρχέτυπα δεδομένα, το πρόσωπο αυτό πρέπει να είναι ικανό να το πράξει και να είναι σε θέση να επεξηγήσει την σημασία και τις συνέπειες των πράξεών τους. Το άτομο που έχει οριστεί ως υπεύθυνος της έρευνας, επιφορτίζεται με τη γενική ευθύνη για τη διασφάλιση τήρησης της επικείμενης νομοθεσίας και των εν λόγω αρχών.
4. Το άτομο που έχει οριστεί ως υπεύθυνος της έρευνας, επιφορτίζεται με τη γενική ευθύνη για τη διασφάλιση τήρησης της επικείμενης νομοθεσίας και των εν λόγω αρχών. (ACPO, 2007)

Τέλος, το αμερικανικό Ίδρυμα Δικαιοσύνης (US National Institute of Justice) έχει εκδώσει έναν οδηγό για την εγκληματολογική ανάλυση των υπολογιστών. Στον οδηγό αυτόν καθορίζει τις αρχές που πρέπει να τηρούν οι ερευνητές, ορισμένες από τις οποίες είναι: οποιασδήποτε δράση δεν θα πρέπει να επηρεάσει την ακεραιότητα των δεδομένων, τα πρόσωπα που αναλαμβάνουν την ανάλυση των δεδομένων θα πρέπει να είναι εκπαιδευμένα και η κάθε δραστηριότητα θα πρέπει να τεκμηριώνεται. (U.S Department of Justice, 2004)

Ωστόσο παρότι, όπως βλέπουμε, το πεδίο και οι διαδικασίες της ψηφιακής εγκληματολογίας υπολογιστών είναι σαφώς καθορισμένες , η τεχνολογία που χρησιμοποιεί το Cloud αλλά και οι νομικές του προεκτάσεις, μπορεί να περιπλέξουν και σε πολλές περιπτώσεις να παρεμποδίσουν την ερευνητική διαδικασία.

Το Cloud λόγω της υποδομής του, διευκολύνει τις εγκληματικές δραστηριότητες. Το Cloud προσφέρει στους εγκληματίες εύκολη πρόσβαση σε τεχνολογίες κρυπτογράφησης (όπως το SpiderOak). Επίσης ένας εγκληματίας μπορεί πολύ γρήγορα να διαγράψει όλα τα δεδομένα από τον λογαριασμό του, γεγονός που καθιστά πιο πιθανό το ενδεχόμενο να μην αφήσει πίσω στοιχεία για εγκληματολογική ανάλυση. Τέλος η αποθήκευση των δεδομένων σε εξυπηρετητές που βρίσκονται στο εξωτερικό καθώς και η πολιτική των εταιρειών που παρέχουν τις Cloud υπηρεσίες, δημιουργούν ένα ασαφές νομικό πλαίσιο που οι εγκληματίες μπορούν να εκμεταλλευτούν (QCC Information Security, 2012).

1.1. Στόχοι της Έρευνας

Το επίκεντρο αυτής της έρευνας είναι να διαπιστωθεί εάν υπάρχουν τυχόν υπολείμματα δεδομένων από την χρήση των Cloud υπηρεσιών αποθήκευσης σε ένα υπολογιστικό σύστημα με λειτουργικό σύστημα Windows 7.Αρχικά αναπτύξαμε ένα πλαίσιο που θα καθοδηγήσει την έρευνα μας. Το πλαίσιο αυτό κατασκευάστηκε με βάση τις αρχές τις ψηφιακής εγκληματολογίας των υπολογιστών ,έχοντας σαν πρότυπο την μεθοδολογία του Μοντέλου Διαδικασίας Επιβολής του Νόμου. Η μεθοδολογία που αναπτύξαμε μπορεί κάλλιστα να χρησιμοποιηθεί από τους ερευνητές στην διερεύνηση πραγματικών εγκληματικών πράξεων.

Στόχος 1: Να προσδιοριστεί το θεωρητικό υπόβαθρο όσον αφορά την ψηφιακή εγκληματολογία και την τεχνολογία Cloud Storage.
Στόχος 2: Να αναπτύξουμε ένα πλαίσιο ψηφιακής εγκληματολογικής ανάλυσης που θα βοηθήσει τους ερευνητές να ακολουθούν μια τυποποιημένη διαδικασία, όταν αναλαμβάνουν την εγκληματολογική ανάλυση των Cloud υπηρεσιών αποθήκευσης.
Στόχος 3: Να εξετάσουμε δημοφιλείς Cloud υπηρεσίες αποθήκευσης:Evernote, SpiderOak, Box και να διαπιστώσουμε να υπάρχουν τυχόν υπολείμματα δεδομένων που να συμβάλουν στην εγκληματολογική έρευνα και ανάλυση.
Στόχος 4: Να εξετάσουμε τις επιπτώσεις, από εγκληματολογική σκοπιά, που έχει η διακίνηση δεδομένων μέσω των εφαρμογών αυτών(metadata,ημερομηνία πρόσβασης, αλλαγή της τιμής κατακερματισμού).

Με την ολοκλήρωση της έρευνας μας θα έχουμε αποκτήσει μια καλύτερη κατανόηση των ψηφιακών δεδομένων που παράγονται από την χρήση των εφαρμογών αυτών. Τέλος θα έχουμε προσδιορίσει και τα σημεία στα οποία θα πρέπει να επιστήσουν την προσοχή τους οι ερευνητές στα στάδια της αναγνώρισης, της συντήρησης, της ανάλυσης και της παρουσίασης της έρευνας.

1.2. Δομή εργασίας

Τα κεφάλαια 2,3,4,5 αποτελούν το θεωρητικό υπόβαθρο της έρευνας μας. Συγκεκριμένα στο κεφάλαιο 2 θα προσδιορίσουμε τον όρο ψηφιακή εγκληματολογία, τι αποτελεί ψηφιακή απόδειξη και την διαδικασία που ακολουθούμε σε μια δικανική έρευνα. Στο κεφάλαιο 3 εξετάζουμε την τεχνολογία Cloud, τις υπηρεσίες Cloud αποθήκευσης και το πώς αυτή η τεχνολογία επηρεάζει την ψηφιακή εγκληματολογία. Στο κεφάλαιο 4 αναλύουμε την δικανική εξέταση της μνήμης RAM, τα δεδομένα που μπορούμε να βρούμε και τους παράγοντες που επηρεάζουν την διάρκεια της αποθήκευσης τους στην μνήμη. Στο κεφάλαιο 5 καθορίζουμε την μεθοδολογία που θα ακολουθήσουμε στην έρευνα μας. Στο κεφάλαιο 6 προσδιορίζουμε τα ερωτήματα που πρέπει να απαντήσει η έρευνα που θα κάνουμε καθώς και τα εργαλεία και τον τρόπο που θα τα χρησιμοποιήσουμε. Στα κεφάλαια 7,8 και 9 αναλύουμε τις Cloud υπηρεσίες Evernote, SpiderOak και Box αντίστοιχα. Τέλος στο κεφάλαιο 10 παρουσιάζουμε συνοπτικά τα ευρήματα μας και κάποιες μελλοντικές προεκτάσεις που μπορεί να έχει η έρευνα μας.

Κεφάλαιο 2: Ψηφιακή Δικανική Εγκληματολογία

Στο κεφάλαιο αυτό θα παρουσιάσουμε αναλυτικά την ψηφιακή εγκληματολογία, τους στόχους της και της αρχές που πρέπει να ακλουθεί. Τέλος θα αναλύσουμε τις φάσεις και τις κατηγορίες στις οποίες χωρίζεται.

2.1. Ορισμός

Η ψηφιακή εποχή έχει παράξει πολλά επαγγέλματα, αλλά ένα από τα πιο ασυνήθιστα είναι η *εγκληματολογία υπολογιστών*. Η *εγκληματολογία υπολογιστών* ασχολείται με την εφαρμογή του νόμου πάνω στην επιστήμη των υπολογιστών. Ένας ορισμός του παραπάνω όρου είναι ο παρακάτω: Ως *εγκληματολογία υπολογιστών* ορίσαμε την έρευνα των υπολογιστών και την ανάλυση των τεχνικών που περιλαμβάνουν την ταυτοποίηση, διατήρηση, εξαγωγή, τεκμηρίωση και ερμηνεία των δεδομένων ενός υπολογιστή ώστε να καθορίσουμε εκμεταλλεύσιμα και νόμιμα αποδεικτικά στοιχεία.

Παρ' όλο που η εγκληματολογία υπολογιστών είναι παρόμοια με τις άλλες μορφές εγκληματολογίας, η διαδικασία της εγκληματολογίας υπολογιστών απαιτεί άριστη γνώση του υλισμικού και του λογισμικού των υπολογιστών ώστε να αποφευχθεί η ακούσια ακύρωση ή καταστροφή των αποδεικτικών στοιχείων και ώστε να είναι δυνατή η διατήρησή τους για περαιτέρω ανάλυση. Επίσης ο εγκληματολόγος υπολογιστών οφείλει να γνωρίζει λεπτομερώς τους εθνικούς αλλά και διεθνείς νόμους σχετικώς με την συλλογή των αποδεικτικών στοιχείων. Η εγκληματολογία υπολογιστών έχει γίνει ένα δημοφιλές θέμα στην κοινωνία της ασφαλείας των υπολογιστών. Παρ' όλο που αποτελεί ένα συναρπαστικό πεδίο, λόγω της φύσεως των υπολογιστών, το μέγεθος της πληροφορίας που είναι διαθέσιμη είναι πολύ περισσότερο από το μέγεθος της πληροφορίας που είναι εφικτό να αναλυθεί και χρειάζεται εμπειρία ώστε ο εγκληματολόγος υπολογιστών να ξέρει πότε πρέπει να σταματήσει την ανάλυση.

Η κεντρική ιδέα πίσω από την εγκληματολογία υπολογιστών βρίσκεται στην ανάκτηση των δεδομένων. Για να γίνει αυτό, πρέπει:

- Να προσδιορισθούν τα αποδεικτικά στοιχεία
- Να καθορισθεί πώς θα διατηρηθούν αναλλοίωτα τα αποδεικτικά στοιχεία
- Να γίνει εξαγωγή, επεξεργασία και ανάλυση των αποδεικτικών στοιχείων
- Και να εξασφαλισθεί ότι τα αποδεικτικά στοιχεία θα γίνουν αποδεκτά από το δικαστήριο

2.2. Ψηφιακές αποδείξεις και δεδομένα

Οι ψηφιακές αποδείξεις αποτελούν το πιο σπουδαίο αποδεικτικό μέσο, κατά την εξέταση μιας υπόθεσης ηλεκτρονικού εγκλήματος και γενικά κατά την εξέταση οποιουδήποτε στοιχείου έχει ψηφιακή μορφή. Ο SWGDE (Scientific Working Group on Digital Evidence), μια κοινοπραξία διεθνών οργανισμών, που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή, διαχωρίζοντάς τις σε:

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

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

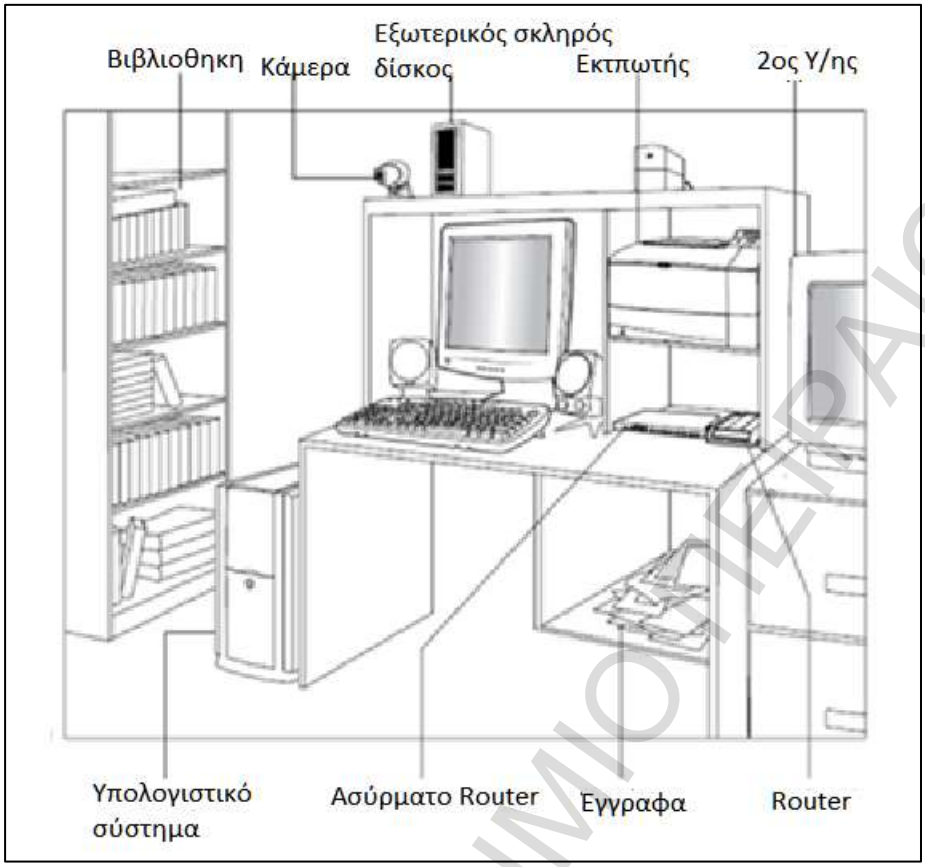
Βασικό χαρακτηριστικό των ψηφιακών αποδείξεων είναι ο μεγάλος βαθμός μεταβλητότητάς τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν με τη χρήση διαφόρων εργαλείων και μεθόδων. Ο ερευνητής, λοιπόν, πρέπει να αναζητεί και να μεταχειρίζεται τις πληροφορίες αυτές με ιδιαίτερη δεξιότητα.

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

2.3. Έρευνα αποδεικτικών στοιχείων

Ο αρχικός στόχος σε μία εγκληματολογική έρευνα υπολογιστών είναι να καθοριστεί το είδος των αποδεικτικών στοιχείων που αναζητούνται για την υπόθεση. Η γνώση του είδους των αποδεικτικών στοιχείων που αναζητούνται είναι αναπόσπαστο κομμάτι μίας επιτυχούς έρευνας.

Στην εικόνα που ακολουθεί παρουσιάζεται μια τυπική σκηνή ηλεκτρονικού εγκλήματος.



Εικόνα 2-1:Τυπική σκηνή ηλεκτρονικού εγκλήματος

Είναι απαραίτητο να εξετάσουμε κάθε ένα από τα αντικείμενα αυτά ώστε να ανακαλύψουμε αποδεικτικά στοιχεία αξιοποιήσιμα στην έρευνα μας.

Υλισμικό

Παρ' όλο που είναι αναμενόμενο ότι σε μία ερεύνα εστιάζουμε πρώτα στα περιεχόμενα του υλισμικού αυτό δεν είναι αληθές πάντα. Πολλές φορές είναι πιθανό να εξάγουμε αποδεικτικά στοιχεία εξετάζοντας εξωτερικά το υλισμικό (πληκτρολόγιο, ποντίκι, CD/DVD, σαρωτής κ.τ.λ.) για δακτυλικά αποτυπώματα. Σε αρκετές έρευνες, το αν ο ύποπτος χρησιμοποίησε ή όχι μία συσκευή είναι πρωτευούσης σημασίας. Πριν προβούμε σε ανάλυση των περιεχομένων του υλισμικού πρέπει να είμαστε σίγουροι ότι έχουμε την άδεια για να το κάνουμε. Αφού εξασφαλίσουμε την κατάλληλη άδεια, πρέπει να φτιάξουμε ένα κατάλογο με όλες τις αποδείξεις που βρήκαμε. Καταγράφουμε όλα τα μέρη του υπολογιστή καθώς και ο,τι συνδέεται σε αυτόν μέσω ενσύρματης ή ασύρματης συνδέσεως.

Υπολογιστικό Σύστημα

Περιγραφή: Ένα υπολογιστική σύστημα αποτελείται από υλισμικό και λογισμικό, που επεξεργάζονται τα δεδομένα, και είναι πιθανό να περιλαμβάνει:

- Ένα κουτί(case) που περιέχει τα κυκλώματα, τους μικρο/επεξεργαστές, τον σκληρό δίσκο, την μνήμη, και τις διεπαφές/συνδέσεις.
- Μια οθόνη

- Ένα πληκτρολόγιο.
- Ένα ποντίκι.
- Περιφερειακές ή εξωτερικά συνδεδεμένες μονάδες δίσκου, συσκευές και αξεσουάρ.

Τα υπολογιστικά συστήματα μπορούν να λάβουν πολλές μορφές, όπως επιτραπέζιοι υπολογιστές, φορητοί υπολογιστές, net-books κ.α. Οι πρόσθετες περιφερειακές συσκευές περιλαμβάνουν modems, routers, εκτυπωτές, σαρωτές, κ.α.

Αφαιρούμενα αποθηκευτικά μέσα

Τα αφαιρούμενα αποθηκευτικά μέσα χρησιμοποιούνται για πολλούς σκοπούς και είναι πηγή πληροφοριών για αποδεικτικά στοιχεία. Συνήθως χρησιμοποιούνται για:

- Αρχειοθέτηση-εφεδρεία (back up) δεδομένων
- Μεταφορά δεδομένων
- Εγκατάσταση προγραμμάτων

Οι δύο πρώτες χρήσεις είναι αυτές που έχουν περισσότερο ενδιαφέρον για τον εγκληματολόγο. Παρ' όλο που ενδέχεται να μην εντοπίσουμε αποδείξεις σε έναν σκληρό δίσκο, πάντα πρέπει να αναζητούμε backups ή δευτερεύοντα αντίγραφα.. Γενικώς υπάρχουν δύο είδη αρχείων στα αφαιρούμενα αποθηκευτικά μέσα. Τα σκόπιμα αποθηκευμένα και τα προσωρινά. Τα σκόπιμα αποθηκευμένα είναι αρχεία, τα οποία έχουν αποθηκευτεί ως αντίγραφα αρχείων που έχουν σβηστεί.

Αν στην ερεύνα το σύστημα μοιάζει να έχει «καθαριστεί» πρέπει να αναζητήσουμε εφεδρικά αντίγραφα. Για την ακρίβεια η ύπαρξη λογισμικού που «καθαρίζει» το σύστημα από αποδείξεις όπως το Evidence Eliminator, συνήθως δείχνει ότι ο χρήστης κάτι κρύβει. Είναι αρκετά πιθανό ο χρήστης να έφτιαξε εφεδρικά αντίγραφα πριν «καθαρίσει» το σύστημά του. Ο δεύτερος τύπος αρχείων, τα προσωρινά αρχεία, είναι αρχεία ή κατάλοιπα αρχείων, τα οποία έχουν προσωρινά αποθηκευθεί ώστε να μεταφερθούν δεδομένα από έναν υπολογιστή σε άλλον. Είναι αρκετά πιθανόν τα αρχεία να υπάρχουν και μετά την μεταφορά καθώς λίγοι άνθρωποι «καθαρίζουν» σωστά τα αφαιρούμενα αποθηκευτικά μέσα.

Έγγραφα

Ο τελευταίος κοινός τύπος αποδεικτικών στοιχείων είναι τα έγγραφα (μη-ηλεκτρονικά). Ως έγγραφο ορίζεται οτιδήποτε είναι γραμμένο και μπορεί να αγγιχθεί και να κρατηθεί. Αποδείξεις που αποτελούνται από έγγραφα καλούνται *έγγραφες αποδείξεις*. Εκτυπωμένες αναφορές, χειρόγραφες σημειώσεις, και πίνακες είναι μερικά παραδείγματα εγγράφων αποδείξεων. Το πιο σημαντικό χαρακτηριστικό των εγγράφων αποδείξεων είναι ότι δεν μπορούν σταθούν από μόνες τους. Πρέπει να αυθεντικοποιηθούν. Πρέπει να αποδειχθεί ότι οι αποδείξεις προήλθαν από τον υπολογιστή του υπόπτου και ότι δεν έχουν αλλαχθεί από τότε που συλέχθησαν.

Ο εγκληματολόγος πρέπει να βγάλει φωτογραφίες των πινάκων και των εγγράφων και να εξετάσει προσεκτικά τον τόπο του εγκλήματος για οτιδήποτε έγγραφα μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία. Αρκετοί άνθρωποι γράφουν τους κωδικούς προσβάσεως πάνω σε αυτοκόλλητα σημειώματα και τα έχουν κολλημένα στην οθόνη τους υπολογιστή. Επίσης στοιχεία ενδέχεται να υπάρχουν πάνω, πίσω ή κάτω από τα μέρη του υλισμικού.

2.4. Διαδικασία εγκληματολογικής έρευνας

Η δικανική εγκληματολογία έχει τέσσερις φάσεις:

- Συλλογή
- Διατήρηση
- Ανάλυση
- Παρουσίαση

2.4.1 Συλλογή

Περιλαμβάνει τις διαδικασίες και τις μεθόδους καταγραφής της φυσικής σκηνής του εγκλήματος. Η τεκμηρίωση της σκηνής του εγκλήματος δημιουργεί ένα μητρώο για την έρευνα. Είναι σημαντικό να καταγράφει με ακρίβεια η θέση της σκηνής, η σκηνή μόνη της, η κατάσταση των υπολογιστών, τα μέσα αποθήκευσης, οι ασύρματες δικτυακές συσκευές, τα κινητά τηλέφωνα, τα PDA ,οι διαδικτυακές και οι δικτυακές προσβάσεις και οι άλλες ηλεκτρονικές συσκευές.

2.4.2 Διατήρηση

Ένα βασικό θέμα στην διαδικασία της ψηφιακής εγκληματολογίας είναι η διατήρηση των δεδομένων. Το στάδιο της διατήρησης αντιστοιχεί στο «πάγωμα» του τόπου του εγκλήματος. Επικεντρώνεται στην διακοπή ή την πρόληψη κάθε δραστηριότητας που μπορεί να βλάψει τις ψηφιακές πληροφορίες που συλλέγονται. Το στάδιο της διατήρησης περιλαμβάνει ενέργειες όπως η απομόνωση των ηλεκτρονικών υπολογιστών, η διακοπή των εν εξελίξει διαδικασιών διαγραφής, και η επιλογή του ασφαλέστερου τρόπου για την συλλογή των πληροφοριών.

Ένας υπολογιστής έχει ουσιαστικά δύο πηγές δεδομένων που παρουσιάζουν ενδιαφέρον για έναν ερευνητή: την πτητική και την μη πτητική μνήμη. Η πτητική μνήμη σχετίζεται κυρίως με την κύρια μνήμη RAM του υπολογιστή, αλλά περιλαμβάνει επίσης τη μνήμη cache και την μνήμη μητρώου (Registry Memory). Η μη πτητική μνήμη σχετίζεται με όλους τους άλλους τύπους μέσων που δεν χάνουν τα δεδομένα τους, όταν η πηγή ενέργειας αφαιρεθεί. Οι σκληροί δίσκοι είναι από τις πιο κοινές μορφές της μη πτητικής μνήμης, με χωρητικότητες που τώρα φτάνουν σε terabytes. Στην κατηγορία αυτή ανήκουν ακόμα, τα διάφορα αφαιρούμενα αποθηκευτικά μέσα (π.χ. USB drives, iPods και SD κάρτες).

Το πρώτο πρόβλημα που θα αντιμετωπίσει ένας ερευνητής είναι το τι θα κάνει με τον ύποπτο υπολογιστή. Αν το σύστημα είναι απενεργοποιημένο, η απόφαση είναι κάπως πιο απλή, αφού πιθανότατα όλα τα πτητικά δεδομένα έχουν χαθεί. Αν το σύστημα εξακολουθεί να τροφοδοτείται με ρεύμα, ο ερευνητής πρέπει να αποφασίσει εάν θα τερματίσει την λειτουργία του αμέσως, ή αν θα προχωρήσει σε ανάκτηση των πτητικών δεδομένων του συστήματος (Μνήμη Ram, μνήμη cache). Στο κεφάλαιο 4 θα εξετάσουμε με περισσότερη λεπτομέρεια την μνήμη RAM.

Μόλις αντιγραφούν τα πτητικά δεδομένα, μια σειρά από άλλα εργαλεία μπορούν στη συνέχεια να χρησιμοποιηθούν για την εξαγωγή χρήσιμων πληροφοριών σχετικά με το υπολογιστικό σύστημα. Υπάρχει ακόμα μια μεγάλη ποικιλία από διαθέσιμα εργαλεία που θα μπορούσαν να χρησιμοποιηθούν κατά τη διάρκεια της ζωντανής ανάλυσης για την συλλογή των σχετικών στοιχείων.

Προκειμένου να διασφαλιστεί η ακεραιότητα των πληροφοριών που λαμβάνονται κατά τη διάρκεια της ζωντανής ανάλυσης, είναι σημαντικό να εξασφαλιστεί ότι θα χρησιμοποιούν εκδόσεις των εργαλείων που ανήκουν σε εμάς (δηλ. έμπιστες) – και όχι τα εργαλεία που είναι εγκατεστημένα στο σύστημα που αναλύεται. Ως εκ τούτου, είναι σύνηθες για τους δικανικούς εξεταστές να δημιουργούν την δικιά τους σουίτα εργαλείων για χρήση κατά την διάρκεια της ζωντανής (Live) απόκτησης και ανάλυσης.

Αφού ολοκληρωθεί η ζωντανή ανάλυση ,ακολουθεί η διακοπή της τροφοδοσίας του συστήματος και η μεταφορά του στο εργαστήριο για την δικανική απόκτηση των μη πτητικών δεδομένων. Η απόκτηση του σκληρού δίσκου (και των άλλων αφαιρούμενων μέσων) μπορεί να επιτευχθεί με διάφορους τρόπους:

- Αφαίρεση της μονάδας του δίσκου από τον ύποπτο υπολογιστή και σύνδεση του το με ένα αξιόπιστο μηχάνημα. Η μέθοδος σύνδεσης με το αξιόπιστο σύστημα θα εξαρτηθεί από το είδος του σκληρού δίσκου (π.χ. IDE, SCSI, SATA).Η παρεμβολή ενός writeblocker μεταξύ του σκληρού δίσκου και του υπολογιστή εξασφαλίζει την ακεραιότητα των δεδομένων του προς εξέταση σκληρού δίσκου.

- Δημιουργία σύνδεσης με το ύποπτο μηχάνημα μέσω δικτυακής σύνδεσης. Η ασφαλής εκκίνηση του ύποπτου υπολογιστή με την χρήση των κατάλληλων προγραμμάτων (αποθηκευμένα είτε σε κάποιο CD ή USB Stick) μας επιτρέπει την ανάκτηση του προς εξέταση σκληρού δίσκου.

Από την σκοπιά των οργανισμών/επιχειρήσεων, δεν είναι πάντα δυνατό να ακολουθήσουμε τα προηγούμενα βήματα για την απόκτηση των μη πτητικών δεδομένων. Πολλοί οργανισμοί διαθέτουν συστήματα που απλά δεν μπορούν να διακόψουν την λειτουργία τους. Για αυτό είναι απαραίτητη η χρήση άλλων μεθόδων για την ανάκτηση των μη μεταβλητών δεδομένων.

Ακολουθούν τα τέσσερα επίπεδα συλλογής δεδομένων, ταξινομημένα με βάση την αύξηση της ακρίβειας:

- μεμονωμένα αρχεία
- εφεδρικοί αποθηκευτικοί χώροι (back up repositories)
- bit-προς-bit ανάκτηση των ατομικών διαμερισμάτων του δίσκου (disk partition)
- bit-προς-bit ανάκτηση ολόκληρου του δίσκου.

Αν τα στοιχεία είναι αποθηκευμένα ή εξακολουθούν να παραμένουν εντός υπαρχόντων αρχείων, τότε και οι δύο πρώτες προσεγγίσεις θα είναι επιτυχής στον εντοπισμό των στοιχείων. Το πλεονέκτημα των τελευταίων δύο προσεγγίσεων είναι ο πλούτος των πληροφοριών που μπορούν να ληφθούν από μη κατανεμημένα τμήματα (unallocated clusters) της μνήμης και του ίδιο του λειτουργικού συστήματος.

Υπάρχει μια ποικιλία από εργαλεία που διευκολύνουν την διαδικασία της αντιγραφής. Η αρχική μέθοδος της δικανικής αντιγραφής δίσκων ήταν η δημιουργία μιας ακριβής bit προς bit (raw) εικόνας του δίσκου. Η εντολή «dd» του λειτουργικού Unix χρησιμοποιήθηκε ευρέως γι 'αυτό το σκοπό. Αυτό σημαίνει, ο τι για την αντιγραφή ενός δίσκο 250GB, ο ερευνητής θα χρειαστεί επίσης, ένα δίσκο τουλάχιστον 250GB για την αποθήκευση του αντιγράφου.

Το υποκεφάλαιο αυτό άρχισε παραπέμποντας στο γεγονός ότι η διατήρηση των δεδομένων είναι επιτακτική ανάγκη σε αυτό το στάδιο. Η διαδικασία εξασφάλισης της διατήρησης των δεδομένων προέρχεται από την ανάγκη να εγγυηθεί η ακεραιότητα των δεδομένων. Το καθολικό εργαλείο που χρησιμοποιείται για το σκοπό αυτό είναι οι εξισώσεις κατακερματισμού (hash functions) ή αλλιώς συναρτήσεις σύνοψης. Μια εξίσωση κατακερματισμού είναι σε θέση να λάβει μια είσοδο μεταβλητού μήκους και να παράγει μία έξοδο σταθερού μήκους που προσδιορίζει μονοσήμαντα την είσοδο και συχνά αναφέρεται ως ένα δακτυλικό αποτύπωμα των δεδομένων.

Δύο αλγόριθμοι χρησιμοποιούνται:

- Ο Message Digest 5 (MD5) ,που δημιουργήθηκε από τον Ronald Rivest , με έξοδο 128-bit
- Ο Ασφαλής Αλγόριθμος κατακερματισμού (Secure Hashing Algorithm SHA-1),που δημοσιεύθηκε από το NIST, με έξοδο 160 bit.

Με την απόκτηση ενός δακτυλικού αποτυπώματος του υπόπτου δίσκου πριν από την αντιγραφή του και στη συνέχεια, συγκρίνοντας το αρχικό αποτέλεσμα με την έξοδο κατακερματισμού του αντιγράφου, ένας ερευνητής είναι σε θέση να επιβεβαιώσει ότι ένα, ακριβές bit προς bit, αντίγραφο του δίσκου έχει παραχθεί.

Αν και υπάρχει πληθώρα εργαλείων που μπορούν να αναλάβουν αυτή την διαδικασία απαιτείται προσεκτική εξέταση του υλισμικού, του λογισμικού και των διαδικασιών που θα χρησιμοποιηθούν.Οι ασυμβατότητες μεταξύ του υλισμικού, η πρόσβαση στο BIOS για την τροποποίηση της σειράς εκκίνησης των συσκευών και οι διαφορετικές εκδόσεις οδηγών (drivers) είναι παράγοντες που μπορεί να επηρεάσει την διαδικασία της ανάκτησης. Ωστόσο, από τη στιγμή που αποκτηθεί με επιτυχία, ο δίσκος μπορεί στη συνέχεια να αναλυθεί.

Μόλις δημιουργηθεί το αντίγραφο του δίσκου ή του διαμερίσματος (partition) και επαληθευτεί η ακεραιότητα του, ο ερευνητής δεν χρειάζεται πλέον να λειτουργεί με την αρχική μονάδα δίσκου. Πράγματι είναι κοινή πρακτική τα αρχικά στοιχεία να αποθηκεύονται σε φυλασσόμενους χώρους δίνοντας ιδιαίτερη προσοχή στους περιβαλλοντικούς παράγοντες που μπορεί να επηρεάσουν την ποιότητα των αποδεικτικών στοιχείων (π.χ. τοποθέτηση σκληρών δίσκων κοντά σε μαγνητικά πηγές).

2.4.3 Ανάλυση

Η φάση της ανάλυσης παίρνει τα επίκτητα στοιχεία και τα εξετάζει για να προσδιορίσει τα αποδεικτικά στοιχεία. Υπάρχουν τρεις μεγάλες κατηγορίες αποδεικτικών στοιχείων:

- επιβαρυντικά/ενοχοποιητικά στοιχεία: Αυτά τα οποία υποστηρίζουν μια δεδομένη θεωρία
- απαλλακτικά στοιχεία: Εκείνα που έρχονται σε αντίθεση με μια δεδομένη θεωρία
- Αποδεικτικά στοιχεία αλλοίωσης/παραβίασης: αυτά που δεν μπορούν να συνδεθούν με οποιαδήποτε θεωρία, αλλά δείχνουν ότι η κατάσταση του συστήματος έχει αλλοιωθεί.

Η ανάλυση των ψηφιακών στοιχείων μπορεί να μην είναι τόσο συναρπαστική όσο ο εντοπισμός και η συλλογή τους, αλλά αυτό είναι το πιο κρίσιμο συστατικό της δικανικής εγκληματολογίας. Σε αυτή την φάση, εξάγουμε και ερμηνεύουμε τα δεδομένα για να δημιουργήσουμε μια αναφορά που να οργανώνει και να ερμηνεύει το μυστήριο κόσμο των ψηφιακών τεκμηρίων έτσι ώστε να μπορεί να χρησιμοποιηθεί για να αποδείξει ή να αποκλείσει αστικές, διοικητικές ή ποινικές κατηγορίες.

Η ανάλυση των ψηφιακών συσκευών και των μέσων αποθήκευσης για τον εντοπισμό και την εξαγωγή των δεδομένων έχει εξελιχθεί σε μια προηγμένη μεθοδολογία που οδηγείται από την ανάπτυξη όλο και πιο ισχυρών και εξελιγμένων ψηφιακών δικανικών εργαλείων.

Πρόκειται για αυτοματοποιημένες βιβλιοθήκες εργαλείων -εργαλειοθήκες- που ενσωματώνουν πληθώρα λειτουργιών και προσφέρουν ένα περιβάλλον γραφικής διεπαφής μεταξύ του χρήστη και της εφαρμογής. Έτσι αντί να χρησιμοποιούμε διάφορα εξειδικευμένα προγράμματα για την ανάλυση των δεδομένων, μπορούμε να χρησιμοποιήσουμε ένα πρόγραμμα και να επιτύχουμε τα περισσότερα από αυτά τα κοινά καθήκοντα:

- Αναγνώριση του είδους των αρχείων από την κεφαλίδα τους (header).
- Ανάκτηση διαγραμμένων αρχείων.
- Η αναζήτηση αρχείων στον κατανεμημένο / μη εκχωρημένο χώρο.
- Εξόρυξη και επεξεργασία ηλεκτρονικού ταχυδρομείου.
- Ανάλυση των αρχείων καταγραφής (log files) και των αρχείων μητρώου (Registry)
- Ανάλυση των μεταδεδομένων (metadata).
- Δημιουργία αναφορών.

Επιπλέον, ορισμένες διεργασίες, όπως η επεξεργασία του ηλεκτρονικού ταχυδρομείου (e-mail) και η ανάκτηση των διαγεγραμμένων αρχείων, εκτελούνται αυτόματα στο παρασκήνιο.

Οι αυτοματοποιημένες Εργαλειοθήκες Δικανικής Πληροφορικής έχουν αυξήσει κατακόρυφα την παραγωγικότητα και έχουν γίνει ο κανόνας για την ανάλυση των διαφόρων μέσων αποθήκευσης. Υπάρχει ωστόσο πληθώρα εργαλείων γραμμής εντολών (command line tools) και ανεξάρτητων προγραμμάτων που εκτελούν συγκεκριμένες διεργασίες. Ανεξάρτητα από το είδος των εργαλείων που θα χρησιμοποιηθεί, αν ο χρήστης των ψηφιακών συσκευών που θα εξετάσουμε δεν έχει χρησιμοποιήσει κάποια μέθοδο απόκρυψης των δεδομένων (π.χ. κρυπτογραφία) , μπορούμε να ανακτήσουμε όλα τα δεδομένα.

Στην πραγματικότητα αν δεν εφαρμόσουμε περιορισμούς στην έρευνα μας (λέξεις-κλειδιά, χρονικοί περιορισμοί) θα καταλήξουμε με υπερβολικά πολλές πληροφορίες που θα επιβαρύνουν την έρευνα μας.

Τα αντικείμενα (artifacts) του λειτουργικού συστήματος είναι ένας όρος που περιγράφει τα δεδομένα, μετα-δεδομένα (metadata), τα αρχεία καταγραφής (log files), inodes, plists, τα σημεία επαναφοράς (restore points) και τα προσωρινά αρχεία που όλα τα λειτουργικά συστήματα δημιουργούν καθώς εκτελούν τις μυριάδες λειτουργίες τους. Ο εντοπισμός, η εξαγωγή/ανάκτηση και (το σημαντικότερο) η ερμηνεία των artifacts μας επιτρέπει την αναδημιουργία των ενεργειών και της κατάστασης των μέσων που εξετάζουμε. Η πρόκληση που αντιμετωπίζει ένας δικανικός ερευνητής όταν εντοπίσει τέτοια artifacts είναι διττή. Πρωτίστως πρέπει να ερμηνεύσει σωστά τις πληροφορίες που μεταφέρει το artifact αυτό, λαμβάνοντας υπόψιν ότι διαφορετικά λειτουργικά συστήματα αντιμετωπίζουν διαφορετικά τα ίδια artifacts.

Η δεύτερη πρόκληση είναι ίσως πιο δύσκολη. Θα πρέπει να εξηγήσουμε σε ένα μη -εξοικειωμένο με τα υπολογιστικά συστήματα- ακροατήριο πως οι εσωτερικές λειτουργίες ενός λειτουργικού συστήματος δημιούργησαν αυτά τα δεδομένα και ποια η σημασία τους

2.4.4 Παρουσίαση

Ο ειδικός θα πρέπει να παρουσιάσει τα ευρήματα του σε μια καθαρή, περιεκτική, δομημένη και σαφή αναφορά στην οποία θα εξηγεί όλα τα συμπεράσματα στα οποία έχει καταλήξει. Ανεξάρτητα από τον χαρακτήρα της έρευνας (εταιρικός, νομικός), τα βήματα που εκτελούνται στα στάδια της απόκτησης και ανάλυσης είναι παρόμοια επειδή κυριαρχούνται από τεχνικά, παρά από νομικά, θέματα. Η φάση της Παρουσίασης ωστόσο εξαρτάται εξ ολοκλήρου από την εταιρική πολιτική και το νομικό δίκαιο, που μπορεί να διαφέρουν για κάθε υπόθεση .Σε αυτό το στάδιο παρουσιάζουμε τα συμπεράσματα μαζί με τα αντίστοιχα στοιχεία από μια έρευνα. Σε μια εταιρική έρευνα, το κοινό συνήθως περιλαμβάνει το γενικό συμβούλιο, τον διευθυντή και τα στελέχη.. Σε ένα δικαστήριο, το κοινό είναι συνήθως ένας δικαστής. Έτσι η εταιρική πολιτική και το νομικό πλαίσιο καθορίζουν τον τρόπο, τον σκοπό και τα περιεχόμενα της παρουσίασης.

2.5. Κατηγορίες Δικανικής εγκληματολογίας

Η Δικανική Πληροφορική χωρίζεται στις παρακάτω υποκατηγορίες:

- Δικανική Υπολογιστών,
- Δικανική Δικτύων
- Εγκληματολογία Βάσεων Δεδομένων ή αλλιώς Δικανική Βάσεων Δεδομένων
- Δικανική φορητών συσκευών.
- Εγκληματολογία Υπολογιστών Νέφους(Cloud forensics)

Η *Δικανική Υπολογιστών (Computer Forensics)* ορίζεται ως «η εφαρμογή των τεχνικών της εγκληματολογικής επιστήμης στο υπολογιστικό υλικό». Με άλλα λόγια η Δικανική Υπολογιστών είναι η διαδικασία του προσδιορισμού, της διατήρησης, της ανάλυσης και της παρουσίασης των ψηφιακών τεκμηρίων με νομικά αποδεκτό τρόπο.

Από την άλλη πλευρά, *Δικανική δικτύου (Network Forensics)* είναι η σύλληψη, καταγραφή και ανάλυση των δικτυακών γεγονότων, προκειμένου να ανακαλύψουμε την προέλευση των επιθέσεων ασφαλείας. Η Δικανική Δικτύου έχει γενικά δύο χρήσεις. Η πρώτη, που αφορά την ασφάλεια, περιλαμβάνει την παρακολούθηση ενός δικτύου για τον εντοπισμό μη αποδεκτών ενεργειών. Ένας εισβολέας θα μπορούσε να διαγράψει όλα τα αρχεία καταγραφής (log files) σε ένα υπολογιστή, και έτσι τα δικτυακά στοιχεία να αποτελούν τα μόνα διαθέσιμα αποδεικτικά στοιχεία για την εγκληματολογική ανάλυση. Η δεύτερη μορφή της Δικανικής δικτύου σχετίζεται με την επιβολή του νόμου. Στην περίπτωση αυτή, η ανάλυση της καταγεγραμμένης δικτυακής κίνησης μπορεί να περιλαμβάνει ενέργειες όπως την ανακατασκευή των αρχεία που έχουν μεταφερθεί, την αναζήτηση λέξεων-κλειδιών και την ανάλυση της ανθρώπινης επικοινωνίας, όπως τα ηλεκτρονικά μηνύματα (e-mail) ή οι συνομιλίες (chat sessions).

Η *Δικανική Βάσεων Δεδομένων* είναι ένας κλάδος της Δικανικής Πληροφορικής που εστιάζει στην εγκληματολογική ανάλυση των βάσεων δεδομένων και των σχετικών μεταδεδομένων τους (metadata). Οι ενέργειες που εκτελούνται είναι παρόμοιες με την Δικανική Υπολογιστών, ακολουθώντας τη συνήθη διαδικασία της εγκληματολογικής έρευνας και της εφαρμογής της στο περιεχόμενο της βάσης δεδομένων και των μεταδεδομένων. Μια εγκληματολογική εξέταση μιας βάσης δεδομένων μπορεί να σχετίζονται με τις χρονικές σημάνσεις (timestamps) των διαφόρων ενεργειών που εκτελέστηκαν προκειμένου να ελεγχθούν οι ενέργειες ενός χρήστη της βάσης δεδομένων. Εναλλακτικά, η εγκληματολογική εξέταση μπορεί να εστιάζει στον προσδιορισμό των συναλλαγών μέσα σε ένα σύστημα βάσης δεδομένων ή μιας εφαρμογής οι οποίες υποδηλώνουν παράνομες πράξεις, όπως η απάτη.

Η *Δικανική φορητών συσκευών* είναι ένας κλάδος της Δικανικής Πληροφορικής που αφορά την ανάκτηση των ψηφιακών τεκμηρίων ή δεδομένων από μια φορητή συσκευή. Ο όρος φορητή συσκευή περιλαμβάνει όχι μόνο τα κινητά τηλέφωνα αλλά και οποιαδήποτε ψηφιακή συσκευή που διαθέτει τόσο εσωτερική μνήμη όσο

και την ικανότητα επικοινωνίας. Η διάδοση των τηλεφώνων (ειδικά των smartphones) δημιούργησε την ανάγκη για εγκληματολογική εξέταση των συσκευών, ανάγκες που δεν μπορούσαν να καλυφθούν από τις υπάρχουσες τεχνικές Δικανικής Πληροφορικής. Ο τύπος μνήμης, ο διαφορετικός τρόπος λειτουργίας και επικοινωνίας χρήστη και φορητής συσκευής απαιτούν μια διαφορετική εγκληματολογική διαδικασία σε σύγκριση με την Δικανική Υπολογιστών. Απαιτείται η ύπαρξη εξειδικευμένων τεχνικών εξαγωγής δεδομένων οι οποίες είναι προσαρμοσμένες στην εκάστοτε συσκευή. Οι φορητές συσκευές μπορούν να χρησιμοποιηθούν για την αποθήκευση αρκετών ειδών προσωπικών πληροφοριών, όπως φωτογραφίες ,επαφές, ημερολόγια και σημειώσεις.

Η *εγκληματολογία υπολογιστών νέφους* είναι ο συνδυασμός του cloud computing και της ψηφιακής εγκληματολογίας. Το cloud computing είναι μια κοινή συλλογή ρυθμιζόμενων πόρων δικτύου (π.χ. δίκτυα, servers, συστήματα αποθήκευσης, εφαρμογών και υπηρεσιών) που μπορούν να επαναρυθμιστούν γρήγορα με ελάχιστη προσπάθεια. Η ψηφιακή εγκληματολογία είναι η εφαρμογή των αρχών της επιστήμης των υπολογιστών για την ανάκτηση ηλεκτρονικών αποδείξεων και για την παρουσίαση τους. Η εγκληματολογία υπολογιστών νέφους είναι ένα υποσύνολο της δικανικής δικτύου.. Ως εκ τούτου, η εγκληματολογία υπολογιστών νέφους ακολουθεί τις κύριες φάσεις της εγκληματολογίας δικτύου με τις τεχνικές προσαρμοσμένες στο cloud computing. Το cloud computing είναι μια εξελισσόμενη τεχνολογία με πολύπλοκες πτυχές που θα εξετάσουμε στην συνέχεια.

Κεφάλαιο 3: Εξέταση της τεχνολογίας Cloud

Στο κεφάλαιο αυτό θα προσδιορίσουμε τον όρο "Cloud Computing" και 'Cloud Storage'.Ακόμα θα εξετάσουμε την άνοδο των Cloud τεχνολογιών και τους τρόπους με τους οποίους επηρεάζουν την ψηφιακή εγκληματολογική ανάλυση.

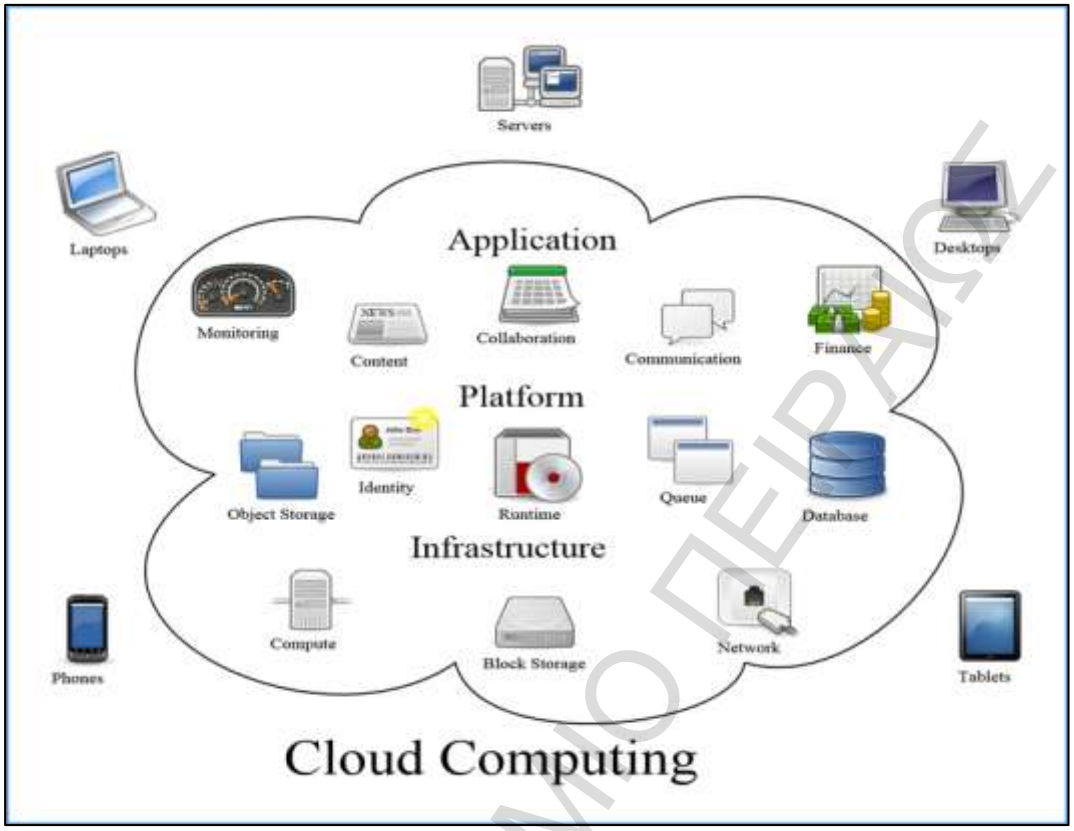
3.1. Ορισμός της τεχνολογίας Cloud

Τα τελευταία χρόνια, όλο και πιο συχνά συναντάται ο ορός "*Cloud Computing"* ως μία από τις τεχνολογίες αιχμής στο τομέα της παροχής υπολογιστικών υπηρεσιών. Στην πραγματικότητα όμως το *Cloud Computing* δεν αποτελεί μία πρόσφατη ανακάλυψη. Επί της ουσίας, είναι η φυσική εξέλιξη τριών τεχνολογικών τάσεων (National Institute of Standars and Technology):

1. *Virtualization:* Εκμετάλλευση της δυνατότητας του φυσικού υλικού (hardware) ώστε να παρέχει περισσότερες από μία λογικές υπηρεσίες. Αυτό επιτυγχάνεται με τη δημιουργία «ιδεατών μηχανών» με ανεξάρτητη λειτουργία, χρησιμοποιώντας όλους τους δυνατούς πόρους του φυσικού μηχανήματος.
2. *Utility Computing:* Παροχή υπολογιστικών πόρων (αποθηκευτικοί χώροι, υπηρεσίες) ως μετρήσιμη υπηρεσία με την ίδια λογική παροχής υπηρεσιών κοινής ωφέλειας (ΔΕΗ, ΟΤΕ κλπ).
3. *ServiceOriented Architecture:* Σχεδιασμός δυναμικού και ελαστικού περιβάλλοντος διάθεσης υπηρεσιών με δυνατότητες αυτοματοποιημένης επιτήρησης, ανάκαμψης, διαχείρισης, επαναδιαμόρφωσης και κλιμάκωσης.

Αυτή τη στιγμή ο ορός "*Cloud Computing*" αντικατοπτρίζει ένα σύνολο υπολογιστικών πόρων που παρέχονται από απόσταση μέσω ενός δικτύου, συνήθως του Internet, ως μετρήσιμη υπηρεσία. Οι υπηρεσίες που προσφέρονται αφορούν υπολογιστικούς πόρους, πλατφόρμες ανάπτυξης εφαρμογών μαζί με την παροχή καταλλήλων εργαλείων αλλά και έτοιμες εφαρμογές (Department of Finance and Deregulation,Australia, 2011).

Στην εικόνα που ακολουθεί παρουσιάζονται συνοπτικά οι υπηρεσίες αυτές.



Εικόνα 3-1: Υπηρεσίες που προσφέρει το Cloud Computing

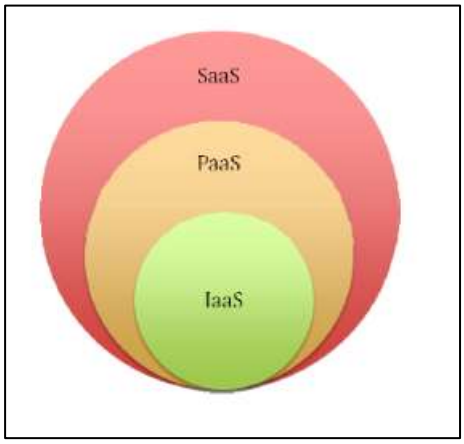
Το *Cloud Computing* χωρίζεται σε τρία επίπεδα (Deloitte, 2009):

- IaaS (Infrastructure as a Service): Με τις υπηρεσίες που προσφέρονται σε αυτό το επίπεδο, δίνεται η δυνατότητα χρήσης υπολογιστικών και δικτυακών υποδομών για τις ανάγκες ενός οργανισμού ως μία "outsourced" υπηρεσία. Δηλαδή αφορά την υπενοικίαση υλικού (hardware) σε αναλογία με τις -ανά πάσα στιγμή- απαιτήσεις του πελάτη, χωρίς να είναι αναγκαία η αγορά τεχνολογικού εξοπλισμού. Η λειτουργιά, η διαχείριση και η συντήρηση του υλικού είναι ευθύνη του παρόχου ενώ για οτιδήποτε φιλοξενείται στις συγκεκριμένες υποδομές, υπεύθυνος είναι ο ίδιος ο πελάτης.

- PaaS (Platform as a Service): Οι υπηρεσίες PaaS προσφέρουν μια υπολογιστική πλατφόρμα, ένα λειτουργικό σύστημα καθώς και εργαλεία για την ανάπτυξη εφαρμογών. Απευθύνονται κυρίως σε developers προσφέροντας ένα πλήρες περιβάλλον για τον σχεδιασμό, την ανάπτυξη, την υλοποίηση και τη δόκιμη εφαρμογών. Οι εφαρμογές που υλοποιούνται από τον πελάτη, μπορούν να διατεθούν σε επιλεγμένους χρήστες του πελάτη ή σε πελάτες του πελάτη. Με τη συγκεκριμένη υπηρεσία, ο πελάτης δε χρειάζεται να ασχολείται με τη συντήρηση του λειτουργικού συστήματος και της πλατφόρμας που το παρέχεται, ωστόσο στερείται τη δυνατότητα λεπτομερούς ελέγχου αυτών.

- SaaS (Software as a Service): Σε αυτό το επίπεδο η εφαρμογή «φιλοξενείται» από τον πάροχο και είναι διαθέσιμη στους πελάτες κυρίως μέσω του Internet. Στην ουσία είναι η υπενοικίαση λογισμικού από ένα πάροχο υπηρεσιών, αντί της αγοράς της άδειας χρήσης του. Χαρακτηριστικά παραδείγματα είναι το πακέτο *Google Apps* της *Google* και το προϊόν *DeskAway* της *Synage Software* τα οποία δίνουν τη δυνατότητα πρόσβασης σε εφαρμογές τύπου Office από οποιοδήποτε υπολογιστή, tablet ή smartphone που έχει σύνδεση προς το διαδίκτυο.

Όπως γίνεται κατανοητό, τα επίπεδα των υπηρεσιών που προσφέρονται έχουν άμεση σχέση μεταξύ τους. Θεωρώντας το επίπεδο υποδομής σαν βάση τότε με την προσθήκη κατάλληλων στοιχείων προκύπτουν και τα υπόλοιπα επίπεδα (*εικόνα 3-2*).



Εικόνα 3-2: Επίπεδα Cloud Computing

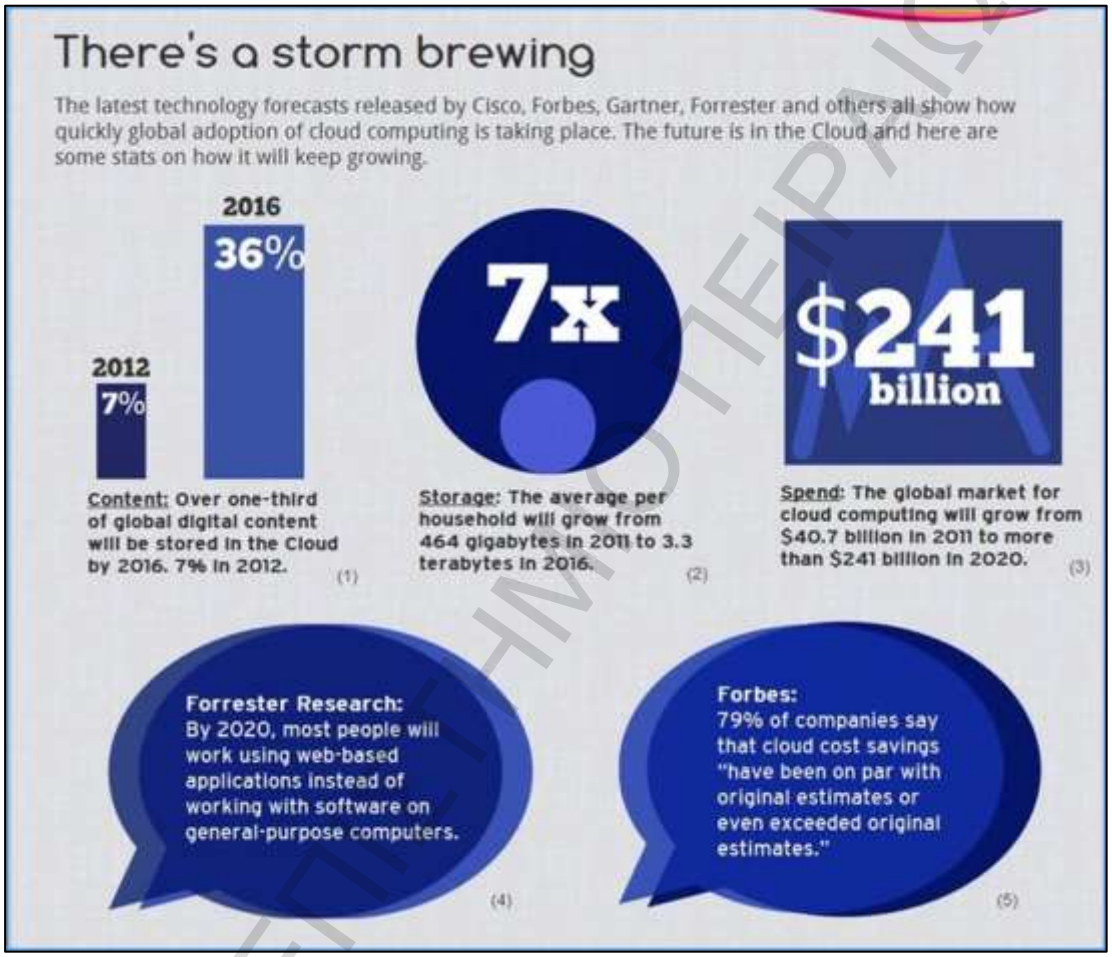
Τα βασικά χαρακτηριστικά των υπηρεσιών που παρέχονται μέσω *Cloud computing* είναι (National Institute of Standars and Technology):

- 'Sold on Demand': Άμεση αγορά της υπηρεσίας από τη στιγμή που αναγνωριστεί αντίστοιχη ανάγκη.
- 'Scalability – Flexibility': Δυνατότητα εκμετάλλευσης της υπηρεσίας στο βαθμό που χρειάζεται την οποιαδήποτε χρονική στιγμή.
- 'Managed by the Provider': Η διαχείριση ενός "Cloud" και των υπηρεσιών που παρέχονται από αυτό, γίνεται εξολοκλήρου από τον πάροχο είτε σε επίπεδο ποιότητας και διάθεσης μέσω υφιστάμενων SLAs είτε σε επίπεδο ασφάλειας. Σε περίπτωση που ο πελάτης διαθέτει ελεγκτικούς μηχανισμούς, μπορεί να θεωρήσει ως δεδομένο ότι ο πάροχος είναι εκ των προτέρων ελεγμένος και πιστοποιημένος ως προς τα διεθνή πρότυπα ασφάλειας. Τα τρία αυτά χαρακτηριστικά των υπηρεσιών είναι που έχουν κατατάξει το *Cloud Computing* στη κορυφή της τεχνολογικής αγοράς τα τελευταία χρόνια, αφού και τα τρία αυτά χαρακτηριστικά μεταφράζονται σε σημαντική εξοικονόμηση χρημάτων.
- 'Measured Service': Τόσο ο χρήστης όσο και ο πάροχος, σε κάθε δεδομένη στιγμή, πρέπει να είναι σε θέση να λάβουν αναφορές σχετικά με τη χρήση των υπηρεσιών cloud.

Η δυνατότητα άμεσης αγοράς της υπηρεσίας από έναν Cloud πάροχο, γλυτώνει τον πελάτη από χρονοβόρες μελέτες, από την αγορά του υλικού και την εύρεση χώρου για εγκατάσταση. Η δυνατότητα εκμετάλλευσης της υπηρεσίας στο βαθμό που κρίνεται αναγκαίο, δίνει στον πελάτη την ευκαιρία να αξιοποιήσει περισσότερους ή λιγότερους πόρους, οποιαδήποτε χρονική στιγμή κρίνει αυτός απαραίτητο, με χρέωση αντίστοιχη των υπηρεσιών που εκμεταλλεύτηκε *(Pay as you go / Pay per use / Pay as you grow)*. Επίσης η διαχείριση των πόρων από έναν *"trusted third party"*, απαλλάσσει κατά κάποιο τρόπο τον πελάτη από θέματα ασφάλειας, ορίζοντας ένα νέο επίπεδο ελεγκτικών μηχανισμών το οποίο αφορά αποκλειστικά τον πάροχο.

3.2. Άνοδος του Cloud Computing

Τα τελευταία χρόνια τα στατιστικά στοιχεία δείχνουν μια ταχεία αύξηση της χρήσης των υπηρεσιών cloud. Για να είμαστε πιο ακριβείς άνθρωποι στρέφονται προς τις υπηρεσίες cloud,όπως το Evernote και το Box για την αποθήκευση των ψηφιακών δεδομένων τους. Από την άλλη πλευρά οι στατιστικές δείχνουν ότι όλο και περισσότερες μεγάλες εταιρείες εκμεταλλεύονται τα οφέλη του cloud computing (*εικόνα 3-3*). Παρατηρούμε επίσης ότι οι υπηρεσίες cloud έχουν ένα αυξανόμενο ρόλο και σε μικρές επιχειρήσεις (εικόνα 3-4). (Why the Future is in the Cloud, 2012)



Εικόνα 3-3: Στατιστικά στοιχεία σχετικά με την ανάπτυξη του Cloud

Εικόνα 3-4: Η σχέση του Cloud Computing και των εταιριών

3.3. Cloud Υπηρεσίες Αποθήκευσης (Cloud Storage)

Η αποθήκευση στο Cloud(cloud storage) ή αλλιώς file hosting, είναι η αποθήκευση των ηλεκτρονικών δεδομένων σε απομακρυσμένες υποδομές, και όχι σε τοπικά αποθηκευτικά μέσα τα οποία είναι συνδεδεμένα στον υπολογιστή.

Υπάρχει ένας μεγάλος αριθμός παρόχων υπηρεσιών Cloud Storage,πολλοί από τους οποίους προσφέρουν δωρεάν υπηρεσίες αποθήκευσης: όπως το Dropbox,το SpiderOak,το Box κ.α. Η πρόσβαση στις διάφορες αυτές υπηρεσίες μπορεί να πραγματοποιηθεί με διάφορους τρόπους, ο χρήστης μπορεί να εγκαταστήσει το λογισμικό της εφαρμογής σε έναν υπολογιστή ή να χρησιμοποιήσει ένα πρόγραμμα περιήγησης.

Το Cloud storage μπορεί να χρησιμοποιηθεί από εγκληματίες για την αποθήκευση παράνομων δεδομένων και την παροχή ενός σημείου διανομής που να μην συνδέει τον ιδιοκτήτη ή τους χρήστες με τα παράνομα δεδομένα. Παρέχει ,δηλαδή, μια δυσκολία στην απόδοση κυριότητας ή της συσχέτισης με παράνομα στοιχεία. Τα δεδομένα που είναι αποθηκευμένα στο Cloud μπορεί επίσης να γίνουν στόχος από εγκληματίες του κυβερνοχώρου, οι οποίοι ενδέχεται να είναι σε θέση να αποκτήσουν πρόσβαση στο λογαριασμό του θύματος και στα δεδομένα που περιέχονται σε αυτό. Τέλος μπορούν να αποκτήσουν τον έλεγχο του λογαριασμό για να χρησιμοποιήσουν τους πόρους του για εγκληματικούς σκοπούς, όπως η διανομή παράνομων δεδομένων. Έτσι αυξάνεται η πρόκληση της διερεύνησης κυβερνο-εγκλημάτων (cybercrimes) ή των παραδοσιακών εγκλημάτων που διενεργούνται στο περιβάλλον του κυβερνοχώρου. (Lawton, 2011)

Όπως προαναφέραμε, το Cloud Storage χρησιμοποιείται από εγκληματίες, και αποτελεί στόχο των κυβερνό-εγκληματιών. Η ασφάλεια των υπηρεσιών cloud αντιμετωπίζονται σωστά, όμως από εγκληματολογική σκοπιά το Cloud Storage,δεν μεριμνά για την εγκληματολογική του ετοιμότητα ή για την διευκόλυνση της δικανικής ανάλυσης.

Οι υπηρεσίες επιβολής του νόμου και οι ερευνητές έχουν ανάγκη να έχουν πρόσβαση στα δεδομένα που αποθηκεύονται στους λογαριασμούς του Cloud Storage. Οι δυσκολίες προκύπτουν από την προσπάθεια εφαρμογής των παραδοσιακών εγκληματολογικών μεθόδων έρευνας σε ένα περιβάλλον cloud. Σε μια παραδοσιακή έρευνα ενός υπολογιστή, το φυσικό υλικό κατάσχεται, δημιουργείται ένα πιστό αντίγραφο, και η ανάλυση γίνεται στο αντίγραφο. Σε ένα περιβάλλον Cloud storage,το υλισμικό φιλοξενείται σε ένα μεγάλο κέντρο δεδομένων(Data Center), το οποίο μπορεί να βρίσκεται σε άλλη χώρα, και τα δεδομένα μπορούν να βρίσκονται κατανεμημένα σε πολλά τέτοια κέντρα δεδομένων σε όλο τον κόσμο. Ως εκ τούτου, η φυσική ανάλυση αποτελεί το λιγότερο μια πρόκληση. (Dykstra, 2013)

3.4. Ψηφιακή Εγκληματολογία και Cloud Storage

Τα εγκλήματα που σχετίζονται με το cloud storage μπορούν να ταξινομηθούν με βάση τους ορισμούς του ηλεκτρονικού εγκλήματος. Το ηλεκτρονικό έγκλημα μπορεί να περιλαμβάνει αδικήματα όπου ένας υπολογιστής χρησιμοποιείται σαν εργαλείο, στόχος, ή σαν συσκευή αποθήκευσης. Τα δεδομένα που είναι αποθηκευμένα στο Cloud μπορεί να είναι στόχος των εγκληματιών, ενώ και το cloud storage μπορεί να χρησιμοποιηθεί για την αποθήκευση παράνομων δεδομένων ή δεδομένων που σχετίζονται με κάποιο έγκλημα. Οι Cloud υπηρεσίες μπορούν επίσης να χρησιμοποιηθούν ως εργαλείο για την διάπραξη ενός εγκλήματος. Έχει αναφερθεί ότι ένας εικονικός διακομιστής (server) από την Cloud υπηρεσία Amazon EC2 χρησιμοποιήθηκε στην επίθεση που οδήγησε στην διακοπή της υπηρεσίας του Sony PlayStation Network. (Pavel Alpeyev, et al., 2011)

Η δυσκολία πρόσβασης στο υλισμικό για τον εντοπισμό αποδεικτικών στοιχείων είναι μια πρόκληση για τους ερευνητές. Τα βασικά αποδεικτικά στοιχεία μπορεί να είναι κατανεμημένα σε πολλαπλά data centers σε διάφορες χώρες. Δεδομένου του γεγονότος αυτού, μπορεί να υπάρχουν νομικά και δικαιοδοτικά ζητήματα που πρέπει να αντιμετωπιστούν από τους ερευνητές.

Ο προσδιορισμός των πραγματικών υπόπτων μέσα στο περιβάλλον cloud είναι επίσης ένα θέμα. Με την κατάσχεση ενός υπολογιστή η μιας συσκευής, μπορεί να υπάρχουν στοιχεία που να αποδεικνύουν την ιδιοκτησία η την συσχέτιση με κάποιο φυσικό πρόσωπο. Αντίθετα μέσα στο περιβάλλον λειτουργίας μιας cloud εφαρμογής αυτή η συσχέτιση μπορεί να μην είναι δυνατή. Η χρήση ανώνυμων δικτύων, όπως το «The Onion Router» (TOR), για την πρόσβαση σε ένα λογαριασμό cloud storage μπορεί να παρεμποδίσει τις έρευνες. (Deloitte, 2012)

Τέλος ένα ακόμα ζήτημα που αντιμετωπίζουν οι δικανικοί εξεταστές είναι ο προσδιορισμός των φορέων παροχής υπηρεσιών και των λογαριασμών των , όπως τα ονόματα των χρηστών και οι κωδικοί πρόσβασης τους. Η ανάλυση των συσκευών των χρηστών-όπως των σκληρών δίσκων-της δικτυακής κίνησης, ή των κινητών συσκευών, μπορεί να προσφέρει αυτές τις πληροφορίες.

Κεφάλαιο 4: Εξέταση της μνήμης RAM

Ένα μεγάλο μέρος της έρευνας μας θα επικεντρωθεί στην ανάλυση της μνήμης RAM. Για αυτό κρίνεται απαραίτητο να προσδιορίσουμε το είδος των αποδείξεων που μπορούμε να ανακαλύψουμε σε αυτήν. Τέλος, καθώς πρόκειται για ένα είδος πτητικής μνήμης, θα προσπαθήσουμε να αποσαφηνίσουμε την διάρκειας ζωής των δεδομένων και τους παράγοντες από τους οποίους εξαρτάται.

Ενώ η παραδοσιακή εγκληματολογία Υπολογιστών περιλαμβάνει την μελέτη των μη πτητικών μέσων αποθήκευσης, όπως οι σκληροί δίσκοι και οι USB συσκευές, η εγκληματολογία μνήμης(memory forensics) περιλαμβάνει την σύλληψη και την ανάλυση της πτητικής μνήμης, όπως είναι για παράδειγμα η μνήμη RAM.

Τα δεδομένα θεωρούνται πτητικά όταν είναι πιθανό να χαθούν, μετά την επανεκκίνηση ενός συστήματος ή να αντικατασταθούν κατά τη διάρκεια της κανονικής του λειτουργίας. Τέτοια δεδομένα συχνά δεν είναι δομημένα με τον ίδιο τρόπο με τα συστήματα αρχείων, και μπορεί να είναι πιο δύσκολο να αναγνωριστούν και να αναλυθούν σε ουσιώδη συμπεράσματα .Συχνά, ωστόσο, οι πληροφορίες που μπορεί να ανακτηθούν από τα πτητικά στοιχεία είναι πολύτιμα στην διευκόλυνση της έρευνας ενώ και πολλά είδη δεδομένων μπορούν να ανακτηθούν μόνο από τη μνήμη Ram. (Scientific Working Group on, 2008)

4.1. Ο ρόλος της ανάλυσης της μνήμης RAM στο σύγχρονο ψηφιακό περιβάλλον

Η εγκληματολογική εξέταση της μνήμης έχει τη δυνατότητα να συμβάλει σημαντικά σε οποιαδήποτε έρευνα. Είναι εξαιρετικά πολύτιμη καθώς ξεπερνά αρκετούς περιορισμούς της παραδοσιακής εγκληματολογικής ανάλυσης, ενώ ακόμα συμβάλει στην αντιμετώπιση των προβλημάτων που δημιουργούν οι νέες τεχνολογίες, όπως η κρυπτογράφηση. Καθώς οι τεχνολογίες εξακολουθούν να εξελίσσονται, η εγκληματολογική εξέταση της μνήμης RAM θα γίνεται όλο και πιο κρίσιμη για την αποτελεσματική συγκέντρωση των απαραίτητων αποδεικτικών στοιχείων.

4.2. Δικανική Ανάλυση της μνήμης RAM

Η ανάλυση της πτητικής μνήμης είναι μία λιγότερο ακριβή και καθορισμένη διαδικασία από την ανάλυση ενός σκληρού δίσκου. Οι σκληροί δίσκοι έχουν μια αυστηρά προκαθορισμένη δομή, και οι αναλυτές ξέρουν πού να ψάξουν για ορισμένες δομές και τύπους δεδομένων σε ένα συγκεκριμένο είδος αρχείων (FAT32, για παράδειγμα). Όσον αφορά την πτητική μνήμη , είναι αδύνατο να προβλέψουμε τι θα βρεθεί ή που θα αποθηκευτεί. Αυτό οφείλεται στο γεγονός ότι η πτητική μνήμη κατανέμεται σε διαφορετικές περιοχές ανάλογα με το πιο μέρος της μνήμης χρησιμοποιείται.

4.3. Είδη αποδεικτικών στοιχείων που βρίσκονται στην RAM

Πολλοί τύποι αποδεικτικών στοιχείων είναι διαθέσιμοι στην μνήμη του υπολογιστή. Οι πτητικές και εφήμερες μορφές αποδεικτικών στοιχείων περιλαμβάνουν (Amari, 2009):

- Τις εν εκτέλεση διαδικασίες και υπηρεσίες(processes/services).
- Τις αποκρυπτογραφημένες εκδόσεις προγραμμάτων.
- Πληροφορίες συστήματος (π.χ. χρονικό διάστημα που παρήλθε από την τελευταία επανεκκίνηση).
- Πληροφορίες για συνδεδεμένους χρήστες.
- Πληροφορίες μητρώου(registry).
- Ανοιχτές συνδέσεις δικτύου.
- Απομεινάρια(artifacts) των συνομιλιών και των επικοινωνιών σε κοινωνικά δίκτυα και MMORPG παιχνίδια.

- Πρόσφατες επικοινωνίες μέσω Webmail συστημάτων.
- Πληροφορίες από τις υπηρεσίες cloud.
- Τα κλειδιά αποκρυπτογράφησης για τους κρυπτογραφημένους δίσκους την στιγμή της ανάκτησης της μνήμης.
- Πρόσφατα εικόνες που είδε ο χρήστης.
- Διάφορα κακόβουλα λογισμικά (malware).

4.4. Νομικές προεκτάσεις της ζωντανής ανάκτησης της μνήμης RAM

Είναι σημαντικό να συνειδητοποιήσουμε ότι η διαδικασία της απόκτηση της πτητικής μνήμης αναπόφευκτα θα αφήσει το αποτύπωμα της στο σύστημα. Ενώ αυτό μπορεί να είναι αποδεκτό από τον αναλυτή, θα πρέπει να ληφθούν υπόψιν οι νόμοι που διέπουν την διαδικασία αυτή. Η σωστή και σε κάθε βήμα τεκμηρίωση της διαδικασίας απόκτησης της μνήμης είναι απαραίτητη για τη συλλογή αποδεικτικών στοιχείων που ανταποκρίνονται στο νομικό πλαίσιο που ισχύει.

4.5. Περιορισμοί της ανάλυσης της μνήμης RAM

Ρεαλιστικά, η ανάλυση της μνήμης Ram έχει τους περιορισμούς της. Πολλοί τύποι των δεδομένων που αποθηκεύονται στη μνήμη του υπολογιστή είναι εφήμεροι. Οι πληροφορίες σχετικά με τις διεργασίες που εκτελούνται δεν θα εξαφανιστούν μέχρι να τερματιστεί η εκτέλεση. Δεν συμβαίνει το ίδιο όμως και με τα υπόλοιπα περιεχόμενα της μνήμης Ram.Τα απομεινάρια των πρόσφατων συνομιλιών, των επικοινωνιών και των άλλων δραστηριοτήτων του χρήστη μπορεί να αντικατασταθούν με άλλα περιεχόμενα οποιαδήποτε στιγμή το λειτουργικό σύστημα απαιτεί ένα ακόμα μπλοκ μνήμης. (Iqbal, 2009)

4.6. Εργαλεία και τεχνικές

Μια σειρά από εργαλεία και μέθοδοι είναι διαθέσιμα για την απόκτηση της πτητικής μνήμης. Από εγκληματολογική σκοπιά, υπάρχουν ορισμένες προϋποθέσεις που κάθε τέτοιο εργαλείο πρέπει να εκπληρώνει. Αυτές είναι:

- Λειτουργία σε επίπεδο πυρήνα (kernel).
- Όσο το δυνατόν μικρότερο αποτύπωμα.
- Φορητότητα
- Να επιτρέπει μόνο την ανάγνωση των δεδομένων.

Η λειτουργία σε επίπεδο πυρήνα είναι απαραίτητη προϋπόθεση για ένα τέτοιο εργαλείο. Πολλές εφαρμογές έχουν προληπτικά μέτρα ασφαλείας κατά των μεθόδων απόκτησης της μνήμης RAM. Στην καλύτερη περίπτωση θα διαβαστούν μηδενικά αντί για τα δεδομένα και στην χειρότερη περίπτωση η εφαρμογή θα λάβει άμεσα μέτρα για την καταστροφή των προστατευόμενων πληροφοριών και για την επανεκκίνηση του συστήματος. Για αυτό το λόγο απαιτείται το εργαλείο να εκτελείται σε επίπεδο πυρήνα.

Όσο μικρότερο αποτύπωμα αφήνεται από ένα εργαλείο απόκτησης μνήμης, τόσο το καλύτερο. Η χρήση ενός εργαλείου που αφήνει ίχνη/αποτυπώματα ,μπορεί ενδεχομένως να οδηγήσει στην καταστροφή ορισμένων αποδεικτικών στοιχείων. Όσα λιγότερα ίχνη αφήνει, τόσο το καλύτερο.

Τα εργαλεία αυτά πρέπει να είναι φορητά και έτοιμα να τρέξουν από μια συσκευή που παρέχεται από τον ερευνητή (π.χ. μια εξωτερική συσκευή USB). Τέλος, οποιοσδήποτε δικανικό εργαλείο ποτέ δεν θα αλλοιώσει ή θα τροποποιήσει τα δεδομένα δίσκο του υπολογιστή που αναλύεται. (Amari, 2009)

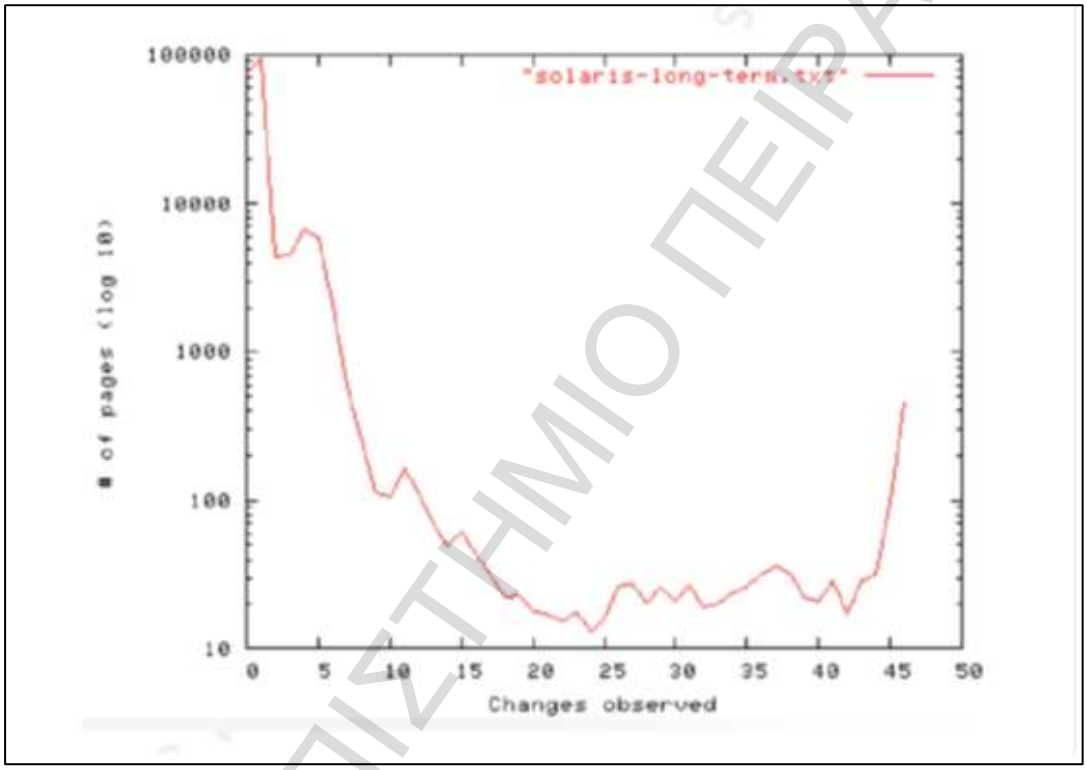
4.7. Διατήρηση των δεδομένων στην μνήμη RAM

Σκοπός της εργασίας αυτής δεν είναι ο προσδιορισμός και η εξέταση του τρόπου συμπεριφοράς και λειτουργίας της πτητικής μνήμης. Ωστόσο στα πλαίσια της έρευνας μας θα πρέπει να αποσαφηνίσουμε την διάρκεια ζωής των δεδομένων στην πτητική μνήμη και τους παράγοντες που τους επηρεάζουν.

Έτσι στην ενότητα αυτή θα προσπαθήσουμε να αποκτήσουμε κάποια επίγνωση για την διάρκεια ζωής των δεδομένων που είναι αποθηκευμένα στην μνήμη-π.χ. όταν ένα πρόγραμμα φορτώνεται στην μνήμη όταν τρέχει, πόσο καιρό θα παραμείνει φορτωμένο; Όσο ένα πρόγραμμα εξακολουθεί να εκτελείται θα συνεχίσει να διαμένει στη μνήμη.

Μετά τον τερματισμό όμως του προγράμματος θα ακολουθήσει η ανακατανομή της μνήμης που χρησιμοποιείτο. Αυτή η ενέργεια δεν μπορεί να οριστεί πλήρως και επακριβώς. Υπάρχει ένα πλήθος παραγόντων που μπορεί να επηρεάσει την κατανομή, ανακατανομή και την αντικατάσταση της πτητικής μνήμης. (Tal Garfinkel, et al., 2004).

Η εικόνα που ακολουθεί μας ενημερώνει για την διατήρηση των δεδομένων της μνήμης σε ένα λειτουργικό σύστημα Solaris (Amari, 2009).



Εικόνα 4-1: Γράφημα αλλαγών στης μνήμη RAM

Το γράφημα αυτό αναπαριστά στον άξονα xx΄ τις μέρες που έτρεχε το μηχάνημα και στον άξονα yy΄ τον αριθμό των σελίδων που άλλαξαν. Σε αυτήν την μελέτη το 86 % της μνήμης δεν άλλαξε.

Ακόμα στα πλαίσια της έρευνας αυτής αποδείχθηκε ότι τα metadata διαφόρων διεργασιών και άλλων δεδομένων παρέμειναν στην μνήμη για περισσότερο από 14 μέρες όσο το σύστημα χρησιμοποιείτο. Τέλος πρέπει να προσθέσουμε ότι η πιθανότητα να αντικατασταθούν τα δεδομένα στην μνήμη συνδέεται με τις δραστηριότητες του χρήστη.

4.8. Συμπεράσματα

Συνοψίζοντας μπορούμε να προσδιορίσουμε τους παράγοντες που επηρεάζουν την διατήρηση των δεδομένων στην πτητική μνήμη. Ο τύπος του λειτουργικού συστήματος είναι ένας σημαντικός παράγοντας, όπως είναι και η διαθέσιμη μνήμη. Όσο λιγότερο αποτελεσματικό είναι το λειτουργικό σύστημα στην κατανομή της διαθέσιμης μνήμης, τόσο πιο σποραδική θα είναι αυτή η κατανομή. Επιπλέον, το επίπεδο της δραστηριότητας στο ίδιο το μηχάνημα παίζει τεράστιο ρόλο.

Κεφάλαιο 5: Μεθοδολογία

Επόμενος στόχος μας είναι χρησιμοποιώντας το θεωρητικό υπόβαθρο των προηγούμενων κεφαλαίων να δημιουργήσουμε μια μεθοδολογία προσαρμοσμένη στις ιδιαιτερότητες των Cloud υπηρεσιών. Για να το πετύχουμε αυτό όμως πρώτα θα προσδιορίσουμε τους γενικούς κανόνες που πρέπει να διέπουν μια τέτοια μεθοδολογία. Τέλος θα παρουσιάσουμε και την μεθοδολογία στην οποία θα στηριχτούμε για την δημιουργία της δικιάς μας.

Η επιστήμη της πληροφορικής με τον ένα ή τον άλλο τρόπο, σχετίζεται με τις περισσότερες εγκληματικές έρευνες. Η εισαγγελική αρχή είναι δυνατόν να εκδώσει ένταλμα έρευνας του ηλεκτρονικού ταχυδρομείου και των ηλεκτρονικών εγγράφων ατόμων που είναι ύποπτα για δολοφονία ή παιδική πορνογραφία. Ιδιωτικές εταιρείες, ελέγχουν τους προσωπικούς υπολογιστές των εργαζομένων τους, στοχεύοντας στην αποφυγή διαρροής εταιρικών μυστικών σε ανταγωνιστές. Απάτες εξακριβώνονται μέσα από τη συλλογή και ανάλυση στοιχείων από το πληροφοριακό σύστημα του υπό έρευνα οργανισμού. Έτσι λοιπόν δημιουργείται η ανάγκη τυποποίησης της συγκεκριμένης ερευνητικής διαδικασίας μέσα από μια κοινά αποδεκτή μεθοδολογία.

5.1. Απαιτήσεις

Η μεθοδολογία ανεύρεσης ψηφιακών αποδεικτικών στοιχείων θα πρέπει να είναι πρακτική και να βασίζεται στη γενική διαδικασία συλλογής αποδεικτικών στοιχείων. Δεν θα πρέπει να επηρεάζεται από τις τεχνολογικές αλλαγές, αλλά θα πρέπει να προσαρμόζεται ανάλογα με τους περιορισμούς και τις ιδιαιτερότητες του περιστατικού και του περιβάλλοντος στο οποίο συνέβη. Το πιο σημαντικό όμως είναι ότι θα πρέπει να είναι καλά δομημένη με τέτοιο τρόπο έτσι ώστε να είναι δυνατή η τυποποίησή της με τη μορφή ενός ηλεκτρονικού εργαλείου.

Με την πάροδο του χρόνου έχουν προταθεί πολλά μοντέλα ψηφιακής εγκληματολογίας. Στα πλαίσια της έρευνας μας θα βασιστούμε στο Μοντέλο Διαδικασίας Επιβολής του Νόμου, το οποίο παρουσιάζουμε στην συνέχεια.

Μοντέλο Διαδικασίας Επιβολής του Νόμου (Law Enforcement Process Model - 2001)

Η συγκεκριμένη μεθοδολογία συλλογής και αξιολόγησης στοιχείων έχει τυποποιηθεί από το υπουργείο δικαιοσύνης των Ηνωμένων Πολιτειών. Αποτελείται από τα εξής βήματα:

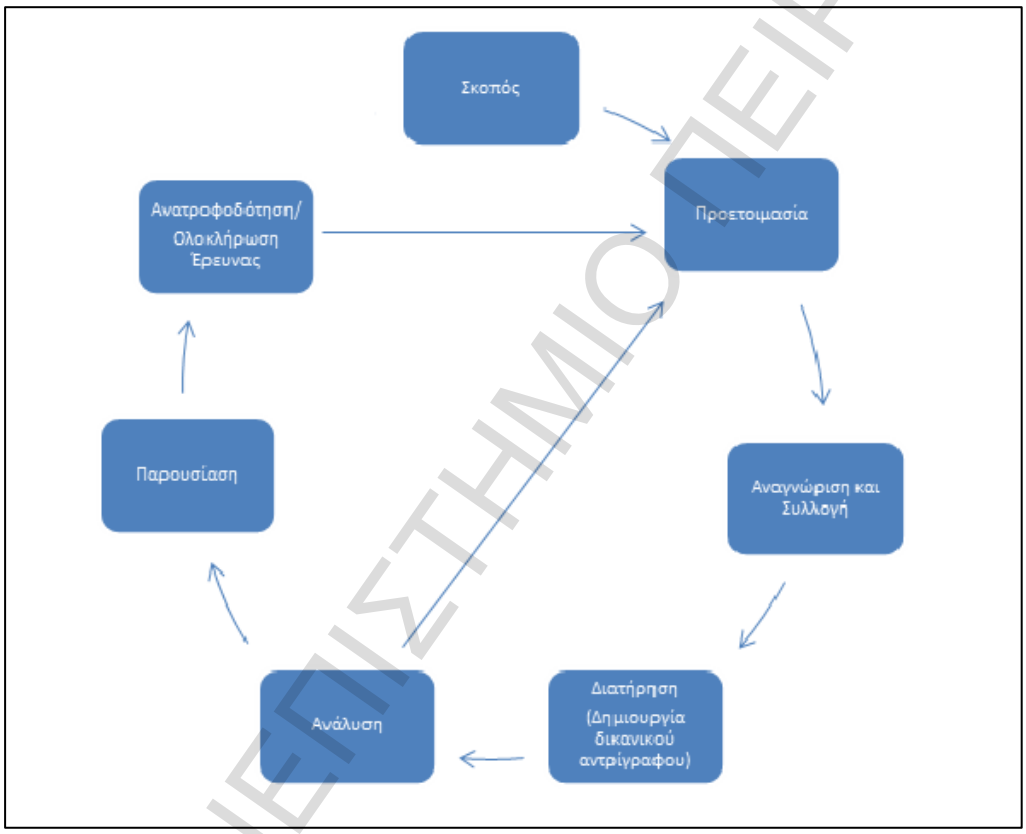
1. **Προετοιμασία**: Ορίζονται τα εργαλεία που θα χρησιμοποιήσει ο ερευνητής.
2. **Συλλογή**: Οι διαδικασίες συλλογής στοιχείων χωρίζονται σε τρία στάδια:
    a. *Απομόνωση του χώρου*: Μόνο εξουσιοδοτημένη πρόσβαση.
    b. *Καταγραφή του χώρου*: Λεπτομερής καταγραφή του χώρου και όσων στοιχείων υπάρχουν μέσα σε αυτόν. Απαιτείται η φωτογράφιση του χώρου.
    c. *Συλλογή δεδομένων*: Αναζήτηση τόσο φυσικών όσο και ψηφιακών στοιχείων.
3. **Επεξεργασία Δεδομένων**: Τα δεδομένα που συλλέχθηκαν επεξεργάζονται για την παραγωγή πληροφοριών.
4. **Ανάλυση των Αποτελεσμάτων**: Οι πληροφορίες ελέγχονται, αξιολογούνται και σε περιπτώσεις που δεν επαρκούν (πληρότητα) επαναλαμβάνεται το προηγούμενο βήμα.
5. **Σύνταξη Αναφοράς**: Παραθέτουμε αναλυτικά τα βήματα που ακολουθήθηκαν για να καταλήξουμε στα συμπεράσματα της αναφοράς και στη συνέχεια παραδίδεται στις αρχές.

5.2. Προτεινόμενη μεθοδολογία

Στα προηγούμενα κεφάλαια προσδιορίσαμε τους γενικούς νόμους και κανόνες που διέπουν την εγκληματολογία υπολογιστών. Στην συνέχεια προσδιορίσαμε την τεχνολογία Cloud, το Cloud Storage και το πώς η χρήση του επηρεάζει τις δικανικές έρευνες. Τέλος αναφερθήκαμε σε ένα ξεχωριστό κεφάλαιο στον ιδιαίτερο ρόλο που μπορεί να παίξει η μνήμη Ram στις ψηφιακές εγκληματολογικές έρευνες.

Χρησιμοποιώντας το θεωρητικό υπόβαθρο του κεφαλαίου αυτού και τα συμπεράσματα των προηγούμενων θα δημιουργήσουμε μια μεθοδολογία που να μπορεί εύκολα, αποτελεσματικά και αξιόπιστα να χρησιμοποιηθεί για την δικανική ανάλυση των υπηρεσιών Cloud. Η μεθοδολογία της Διαδικασίας Επιβολής του Νόμου αποτελεί το πρότυπο πάνω στο οποίο θα δημιουργήσουμε το δικό μας πλαίσιο έρευνας.

Στην εικόνα που ακολουθεί παρουσιάζουμε την προτεινόμενη μεθοδολογία ενώ στην συνέχεια παρουσιάζουμε συνοπτικά τα στάδια της.



Εικόνα 5-1: Προτεινόμενη μεθοδολογία

5.2.1 Σκοπός

Στην αρχή μιας έρευνας είναι σημαντικό να προσδιορίσουμε τον σκοπό, την φύση και το υπόβαθρο της ανάλυσης. Πρέπει ακόμα να καθορίσουμε τα όρια της έρευνας μας. Στο στάδιο αυτό θα αναφέρουμε τα εμπλεκόμενα πρόσωπα, λέξεις-κλειδιά, χρονοδιαγράμματα που πρέπει να τηρηθούν και οποιαδήποτε άλλη σχετική πληροφορία. Ο αρχικός σκοπός της έρευνας μπορεί να είναι αρκετά γενικός και με την εξέλιξη της, να επικεντρωθεί σε τυχόν θέματα που θα προκύψουν.

5.2.2 Προετοιμασία

Μετά τον καθορισμό του σκοπού ,το επόμενο βήμα στην έρευνα είναι η κατανόηση των απαιτήσεων και η διασφάλιση ότι ο σωστός εξοπλισμός και πληροφορίες είναι διαθέσιμες. Το στάδιο αυτό μπορεί να περιλαμβάνει την απόκτηση εξοπλισμού και την κατάρτιση των ερευνητών.

Η προετοιμασία μπορεί επίσης να περιλαμβάνει την έρευνα κάποιου συγκεκριμένου προγράμματος ή τεχνολογίας γενικότερα. Για παράδειγμα αν η έρευνα σχετίζεται με κάποια συγκεκριμένη υπηρεσία Cloud Storage, ο ερευνητής μπορεί αρχικά να διεξάγει μια έρευνα με την χρήση εικονικών μηχανών για την κατανόηση της συμπεριφοράς και της λειτουργίας της. Στο στάδιο αυτό καθορίζεται το χρονοδιάγραμμα της έρευνας ,το προσωπικό και τα καθήκοντα του.

5.2.3 Αναγνώριση και Συλλογή

Το επόμενο στάδιο, όπως και σε μια τυπική εγκληματολογική έρευνα, είναι ο εντοπισμός και η συλλογή των ψηφιακών δεδομένων. Περιλαμβάνει τις διαδικασίες και τις μεθόδους καταγραφής της φυσικής σκηνής του εγκλήματος καθώς και των ενεργειών που εκτελέσαμε για την συλλογή των αποδεικτικών στοιχείων και για την ασφαλή αποθήκευση τους.

Στην φάση αυτήν, ο ερευνητής μπορεί να ανακαλύψει την χρήση υπηρεσιών Cloud Storage.Σε αυτήν την περίπτωση, σε πρώτη φάση, ο ερευνητής θα επικοινωνήσει με τον πάροχο της εν λόγω υπηρεσίας .Αν έχει στην κατοχή του πληροφορίες που ο πάροχος μπορεί να χρησιμοποιήσει (όνομα χρήστη, ημερομηνίες πρόσβασης) τότε ο πάροχος, σύμφωνα πάντα με την ισχύουσα νομοθεσία, μπορεί να επιτρέψει την πρόσβαση στα δεδομένα.

5.2.4 Διατήρηση (Δικανικό Αντίγραφο)

Είναι η απόλυτα πιστή αντιγραφή της πρωτότυπης ψηφιακής απόδειξης χρησιμοποιώντας τυποποιημένες και αποδεκτές πρακτικές. Η πλήρης και προσεκτική καταγραφή των βημάτων μας και σε αυτό το στάδιο εξασφαλίζει την αξιοπιστία των ενεργειών μας.

5.2.5 Ανάλυση

Σε αυτή την φάση προσδιορίζεται η σημαντικότητα των συλλεγμένων δεδομένων και βγαίνουν συμπεράσματα που βασίζονται στις αποδείξεις που βρέθηκαν. Στην περίπτωση της ανακάλυψης νέων δεδομένων, η διαδικασία επιστρέφει στο βήμα της Προετοιμασίας. Η ανάλυση θα συνεχιστεί με τα ήδη αντιγραμμένα δεδομένα και τα νέα δεδομένα θα αναλυθούν όταν είναι διαθέσιμα.

5.2.6 Παρουσίαση

Στο επόμενο στάδιο της μεθοδολογίας μας, τα στοιχεία καταγράφονται και παρουσιάζονται στους εντολείς. Ο ειδικός θα πρέπει να παρουσιάσει τα ευρήματα του σε μια καθαρή, περιεκτική, δομημένη και σαφή αναφορά στην οποία θα εξηγεί όλα τα συμπεράσματα στα οποία έχει καταλήξει. Η δημιουργία και η χρήση ενός χρονοδιαγράμματος των γεγονότων θα συμβάλει στην κατανόηση και στην εξήγηση της αλληλουχίας των γεγονότων.

5.2.7 Ανατροφοδότηση/Ολοκλήρωση

Η ανατροφοδότηση είναι το επόμενο βήμα στην έρευνα μας. Έτσι αξιολογούμε τα αποτελέσματα της έρευνας μας, την ορθότητα της διαδικασίας και αν οι πρακτικές που εφαρμόσαμε συνιστώνται για να επαναχρησιμοποιηθούν. Το τελικό βήμα είναι η ολοκλήρωση της έρευνας. Με βάση την ανατροφοδότηση από τον ερευνητή η διαδικασία μπορεί να επιστρέψει στο στάδιο της Προετοιμασίας. Αν δεν απαιτείται περεταίρω έρευνα, τότε η υπόθεση μπορεί να ολοκληρωθεί.

Κεφάλαιο 6: Μεθοδολογία Έρευνας

6.1. Ερευνητικό Πρόβλημα

Όπως αναφέρθηκε προηγουμένως, το Cloud χρησιμοποιείται για την αποθήκευση μεγάλου όγκου δεδομένων, συμπεριλαμβανομένων παράνομων δεδομένων και αποδεικτικών στοιχείων εγκληματικών πράξεων. Παρατηρούμε ότι υπάρχει έλλειψη πληροφοριών σχετικά με την εγκληματολογική ανάλυση του Cloud Storage και με τα υπολείμματα δεδομένων που δημιουργούνται από την χρήση του. Τέλος υπάρχει και έλλειψη πληροφόρησης σχετικά με τις αλλαγές, αν υπάρχουν, που μπορούν να συμβούν στα αρχεία μετά την χρήση της υπηρεσίας αυτής.

6.2. Ερευνητικός Σκοπός

Ο σκοπός της παρούσας έρευνας είναι να απαντήσει στο ερευνητικό πρόβλημα που αναλύθηκε στο προηγούμενο υποκεφάλαιο. Στόχος μας είναι να προσδιορίσουμε αν υπάρχουν δεδομένα που να αποδεικνύουν την πρόσβαση και την χρήση τέτοιων υπηρεσιών και αν υπάρχει κάποια μέθοδος για την αναγνώριση και την διατήρηση των δεδομένων που σχετίζονται με τις υπηρεσίες αυτές.

Τα ευρήματα της έρευνας μας θα βοηθήσουν τους δικανικούς εξεταστές στην αναγνώριση της χρήσης υπηρεσιών Cloud Storage και στην παροχή μιας μεθοδολογίας για τον εντοπισμό και την διατήρηση των σχετικών ψηφιακών αποδείξεων με δικανικά αποδεκτό τρόπο.

6.3. Ερευνητικές Ερωτήσεις

Οι δυο ερωτήσεις που θα προσπαθήσουμε να απαντήσουμε αναλύονται στα υποκεφάλαια που ακολουθούν.

6.3.1 Ερευνητική Ερώτηση 1

Ποιά είναι τα αποδεικτικά στοιχεία/ απομεινάρια δεδομένων (data remnants) που δημιουργούνται από την χρήση των cloud υπηρεσιών και μας επιτρέπουν να εξακριβώσουμε αν όντως έγινε χρήση των υπηρεσιών αυτών;

Η ερώτηση αυτή οδηγεί στις εξής υποθέσεις:

Υπόθεση 1: Δεν υπάρχουν data remnants από την χρήση των cloud υπηρεσιών που να επιτρέπουν τον προσδιορισμό του φορέα παροχής υπηρεσιών(service provider), του ονόματος του χρήστη, ή των αρχεία που μεταφέρθηκαν.
Υπόθεση 2: Υπάρχουν υπολείμματα από την χρήση των cloud υπηρεσιών που επιτρέπουν την αναγνώριση της υπηρεσίας, του ονόματος του χρήστη, ή των λεπτομερειών των αρχείων.

Η υπόθεση 2 μας οδηγεί στις ακόλουθες υπο-ερωτήσεις:

- Ποιά είναι τα δεδομένα που παραμένουν στον υπολογιστή μετά την εγκατάσταση του λογισμικού της εφαρμογής και την χρήση του για «ανέβασμα» και αποθήκευση δεδομένων;
- Ποιά είναι τα δεδομένα που παραμένουν στον υπολογιστή μετά την πρόσβαση στην υπηρεσία cloud μέσω ενός προγράμματος πλοήγησης;
- Ποια δεδομένα παραμένουν στην πτητική μνήμη, όταν χρησιμοποιείται το λογισμικό της εφαρμογής και ποιά όταν χρησιμοποιείται ένα πρόγραμμα πλοήγησης;

6.3.2 Ερευνητική Ερώτηση 2

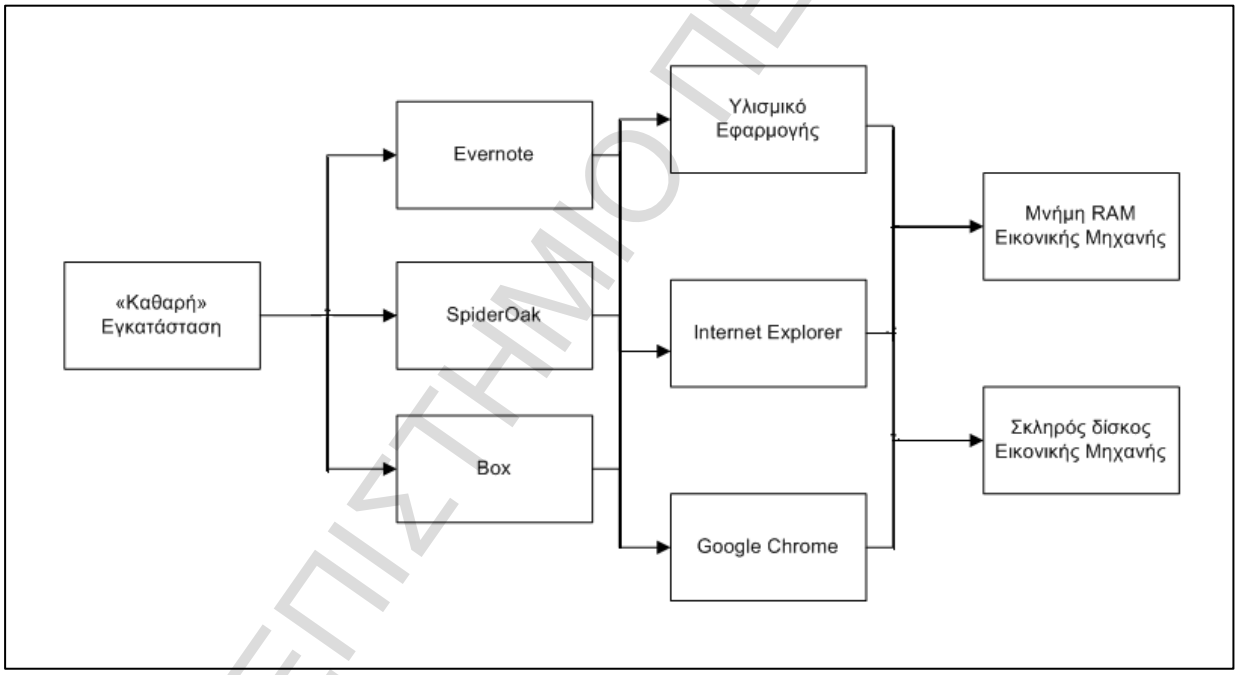
Η δεύτερη ερώτηση είναι η εξής:

Πως επηρεάζει η διαδικασία «ανεβάσματος»(upload) και «κατεβάσματος» (download) αρχείων από μια υπηρεσία cloud τα εσωτερικά δεδομένα και τα μεταδεδομένα (metadata) των αρχείων;

6.4. Πειραματική Διαδικασία

Η διαδικασία αυτή θα εφαρμοστεί για να απαντήσει στις ερευνητικές ερωτήσεις σε σχέση με τη χρήση των cloud υπηρεσιών αποθήκευσης: Evernote, Spideroak και Box.

Το διάγραμμα της εικόνας 6.1 παρουσιάζει την διαδικασία που ακολουθήσαμε. Ξεκινώντας από μία «καθαρή» εγκατάσταση, κάθε cloud υπηρεσία εξετάστηκε ξεχωριστά σε ποικίλα σενάρια που περιλαμβάνουν την χρήση του λογισμικού της εφαρμογής και δυο διαφορετικών προγραμμάτων περιήγησης. Σε καθένα από τα σενάρια αυτά ανακτούμε και διατηρούμε την μνήμη RAM και τον σκληρό δίσκο του υπολογιστικού συστήματος.



Εικόνα 6-1: Πειραματική διαδικασία έρευνας

Για την εξέταση των διαφορετικών αυτών σεναρίων δημιουργήθηκε ένα πλήθος εικονικών μηχανών (Virtual Machines ή Vm). Οι εικονικές μηχανές μας επέτρεψαν εύκολα και γρήγορα να χρησιμοποιήσουμε και να εξετάσουμε μια ποικιλία από υπηρεσίες cloud.Επίσης μπορέσαμε να εξετάσουμε κάθε μια από αυτές τις Cloud υπηρεσίες σε συνδυασμό με ένα διαφορετικό πρόγραμμα περιήγησης: τον Internet Explorer (IE) και τον Google Chrome (GC).

Αν αυτή η διαδικασία είχε γίνει χρησιμοποιώντας υλισμικό, ο χρόνος και γενικά οι πόροι για την εγκατάσταση, την διαγραφή και την εκ νέου εγκατάσταση θα ήταν επαχθείς.

6.4.1 Πειραματική διαδικασία απάντησης του πρώτου ερωτήματος

Στους πίνακες που ακολουθούν παρουσιάζονται τα βήματα που ακολουθούμε ,στα πλαίσια της έρευνας μας, για να απαντήσουμε στο πρώτο ερώτημα που θέσαμε.

Πίνακας 6-1: Βήματα έρευνας με την χρήση του λογισμικού της εφαρμογής

Βήματα	Διαδικασία
1.	Εγκατάσταση σε ένα καθαρό Vm του λογισμικού της cloud εφαρμογής που θα χρησιμοποιήσουμε.
2.	«Ανέβασμα» αρχείων από τον υπολογιστή στον διακομιστή(server) της υπηρεσίας μέσω του εγκατεστημένου λογισμικού.
3.	Ανάκτηση της πτητικής μνήμης του Vm καθώς και δημιουργία της εικόνας του σκληρού του δίσκου του.
4.	Εξέταση των δεδομένων για την εύρεση πληροφοριών και την εξαγωγή χρήσιμων συμπερασμάτων.
5.	Επανάληψη της διαδικασίας από το βήμα 1,σε ένα καινούργιο «καθαρό» Vm,μόνο που αυτή την φορά θα «κατεβάζουμε» τα αρχεία που είναι αποθηκευμένα στον server της εφαρμογής.

Τέλος αυτή η διαδικασία θα επαναληφθεί και για όσες cloud υπηρεσίες είναι προσβάσιμες μέσω κάποιου προγράμματος περιήγησης. Συνοπτικά:

Πίνακας 6-2: Βήματα έρευνας με την χρήση ενός περιηγητή

Βήματα	Διαδικασία
1.	Εγκατάσταση σε ένα καθαρό VM του περιηγητή που θα χρησιμοποιήσουμε.
2.	«Ανέβασμα» αρχείων από τον υπολογιστή στον διακομιστή(server) της υπηρεσίας μέσω του περιηγητή.
3.	Ανάκτηση της πτητικής μνήμης του Vm καθώς και δημιουργία της εικόνας του σκληρού του δίσκου του.
4.	Εξέταση των δεδομένων για την εύρεση πληροφοριών και την εξαγωγή χρήσιμων συμπερασμάτων.
5.	Επανάληψη της διαδικασίας από το βήμα 1,μόνο που αυτή την φορά, μέσω του περιηγητή, θα «κατεβάζουμε» τα αρχεία που είναι αποθηκευμένα στον server της εφαρμογής.

6.4.2 Πειραματική διαδικασία απάντησης του δεύτερου ερωτήματος

Για την απάντηση στο δεύτερο ερευνητικό ερώτημα, χρησιμοποιούμε μια διαφορετική πειραματική διαδικασία. Επιλέγουμε τα δεδομένα που θα χρησιμοποιήσουμε και στην συνέχεια ακολουθεί η φόρτωση τους στις, προς εξέταση, cloud υπηρεσίες αποθήκευσης.

Στην συνέχεια χρησιμοποιείται ένα διαφορετικό υπολογιστικό σύστημα για την πρόσβαση στις υπηρεσίες αποθήκευσης και το «κατέβασμα» των προς εξέταση αρχείων. Το «κατέβασμα» αυτό των αρχείων μπορεί να γίνει είτε χρησιμοποιώντας την εφαρμογή της υπηρεσίας είτε ένα πρόγραμμα περιήγησης. Τέλος ,διεξάγεται η ανάλυση για την σύγκριση των αρχικών αρχείων με τα αρχεία που «κατεβάσαμε». Η διαδικασία συνοψίζεται στους ακόλουθους πίνακες:

Πίνακας 6-3: Διακίνηση αρχείων μέσω του λογισμικού της εφαρμογής

Βήματα Διαδικασία
1. Δημιουργία ενός καινούργιου Vm για που θα χρησιμοποιηθεί για την πρόσβαση στις cloud εφαρμογές. 2. Χρήση του Vm και σύνδεση με την cloud εφαρμογή μέσω της χρήσης ενός περιηγητή και είσοδος στο λογαριασμό που χρησιμοποιούμε για την έρευνα αυτή. 3. Περιήγηση στα αρχεία. 4. «Κατέβασμα» των προς εξέταση αρχείων. Εξέταση των metadata των αρχείων..

Πίνακας 6-4: Διακίνηση αρχείων μέσω ενός περιηγητή

Βήματα Διαδικασία
1. Πλοήγηση στην σελίδα της cloud εφαρμογής, «κατέβασμα» και εγκατάσταση του λογισμικού της. 2. Συγχρονισμός του λογαριασμού. 3. Παρατηρούμε ότι τα περιεχόμενα του λογαριασμού «κατεβαίνουν» στο Vm. 4. Εξέταση των metadata των αρχείων. 5. Κλείσιμο του Vm.

6.5. Υλισμικό

Οι λεπτομέρειες του υπολογιστικού συστήματος που θα χρησιμοποιηθεί περιγράφονται στον ακόλουθο πίνακα.

Πίνακας 6-5: Υπολογιστικό σύστημα έρευνας

Υ/ης έρευνας	Προσωπικός Υπολογιστής
Λειτουργικό Σύστημα	Windows® 7 64-bit Professional 6.1.7601 SP1
Επεξεργαστής	Intel® Core™ i3-3220 @ 3.20GHz
Μνήμη	8.0 GB Dual-Channel DDR3 @ 1600 MHz
Αποθηκευτικός χώρος	Εξωτερικός δίσκος 500GB Western Digital 750 GB Seagate Hard Drive

6.6. Λογισμικό

Στην ενότητα που ακολουθεί, θα εξετάσουμε εν συντομία τα εργαλεία και τα προγράμματα που πρόκειται να χρησιμοποιήσουμε στην έρευνα μας. Προγράμματα που χρησιμοποιούνται στη διαδικασία της έρευνας:

Access Data FTK Imager

Πρόκειται για μια σουίτα εργαλείων που μας παρέχει δυνατότητες προεπισκόπησης των δεδομένων και δημιουργίας εικόνων .Μας επιτρέπει την γρήγορη αξιολόγηση των ηλεκτρονικών στοιχείων ώστε να προσδιορίσουμε αν απαιτείται περαιτέρω έρευνα. Τέλος μας δίνει την δυνατότητα να δημιουργούμε πιστά αντίγραφα των ψηφιακών δεδομένων χωρίς να επιφέρουμε αλλαγές στις αρχικές αποδείξεις. (Access Data)

HexEdit

Πρόκειται για ένα δωρεάν πρόγραμμα επεξεργασίας που μας επιτρέπει να αναλύσουμε τα αρχεία, ανεξαρτήτου μεγέθους και είδους, σε δεκαεξαδική μορφή (hexadecimal) (HexEdit).

MoonSols DumpIt

Είναι ένα βοηθητικό πρόγραμμα που λειτουργεί σε περιβάλλον κονσόλας. Πρόκειται για ένα μικρό εκτελέσιμο αρχείο(230 KB) που μας επιτρέπει να αποθηκεύσουμε τα περιεχόμενα της μνήμης RAM (MoonSols).

Vmware Workstation

Αυτό είναι το πρόγραμμα που θα χρησιμοποιήσουμε για την δημιουργία εικονικών μηχανών. Ιδιαίτερη μνεία πρέπει να κάνουμε στην λειτουργία Snapshot που προσφέρει και την οποία θα αναλύσουμε στην συνέχεια (VMware).

Prodiscover basic

Πρόκειται για ένα εργαλείο δημιουργίας εικόνων διάφορων συσκευών αποθήκευσης (Prodiscover Basic).

OSForensics

Το OSForensics είναι ένα ψηφιακό εργαλείο έρευνας που μας επιτρέπει να εξάγουμε εγκληματολογικά δεδομένα ή να ανακαλύψουμε κρυμμένες πληροφορίες σε έναν υπολογιστή. Προσφέρει μια ποικιλία από προηγμένα χαρακτηριστικά (OSForensics).

Στα πλαίσια της έρευνας μας θα χρησιμοποιήσουμε τις λειτουργίες της δημιουργίας υπογραφών (signature) ενός λειτουργικού συστήματος και την εκτέλεση συναρτήσεων κατακερματισμού για την εξακρίβωση τις ακεραιότητας των δεδομένων. Τέλος πρέπει να αναφέρουμε ότι είναι δυνατή η εγκατάσταση του OSForensics σε μια αποσπώμενη μονάδα αποθήκευσης.

Στην εικόνα που ακολουθεί παρουσιάζεται το περιβάλλον του προγράμματος αυτού και οι λειτουργίες που προσφέρει.

Εικόνα 6-2: Πρόγραμμα OSForensics

ESE DatabaseView v1.07

Το ESE DatabaseView είναι ένα πρόγραμμα της Nirsoft κατασκευασμένο για να προσφέρει πρόσβαση στις βάσεις δεδομένων ESE.Το χρησιμοποιούμαι για να πάρουμε μια γενική εικόνα της βάσης δεδομένων αλλά και για να επαληθεύσουμε τα δεδομένα που έχουν αποθηκευτεί από τα πειράματα μας (ESEDatabaseView).

Esentutl.exe

Είναι ένα εργαλείο γραμμής εντολών που είναι ενσωματωμένο στα Windows Παρέχει βοηθητικά προγράμματα για τις βάσης δεδομένων ESE και μπορεί, μεταξύ άλλων, να χρησιμοποιηθεί για την προβολή των metadata ή για να ανακτήσει μια βάση δεδομένων ESE (Esentutl.exe).

CC cleaner

Είναι ένα πρόγραμμα που χρησιμοποιείται για να καθαρίσει το λειτουργικό μας σύστημα από ανεπιθύμητα αρχεία και με έγκυρες καταχωρήσεις μητρώου (Registry) (CC cleaner).

Eraser

Το Eraser είναι ένα προηγμένο εργαλείο ασφαλείας για τα Windows που μας επιτρέπει να αφαιρέσουμε εντελώς τα ευαίσθητα δεδομένα από το σκληρό μας δίσκο (Eraser).

SQLite Database Browser

Όπως δηλώνει και ο τίτλος του πρόκειται για ένα δωρεάν εργαλείο που μας επιτρέπει να δημιουργήσουμε, να σχεδιάσουμε και να επεξεργαστούμε SQLite βάσεις δεδομένων (SQLite Database Browser).

Backtrack

Μια πολύ καλή προσπάθεια συλλογής και αξιοποίησης λογισμικού ψηφιακής εγκληματολογίας είναι η έκδοση Linux με το όνομα Backtrack. Το Backtrack μπορούμε να το κατεβάσουμε και να το χρησιμοποιήσουμε , σε μορφή Live CD.

Πρόκειται για ένα παραμετροποιημένο λειτουργικό σύστημα βασισμένο στη διανομή Ubuntu Linux, το οποίο περιέχει πολλά και χρήσιμα εργαλεία που συμβάλουν στο έργο ενός δικανικού ερευνητή. Βασικό πλεονέκτημα της συγκεκριμένης προσέγγισης είναι ότι λειτουργούμε σε μη μεταβαλλόμενο ή "νεκρό" περιβάλλον (Dead Analysis) το οποίο είναι το ενδεδειγμένο για έρευνες δικανικής πληροφορικής (Backtrack).

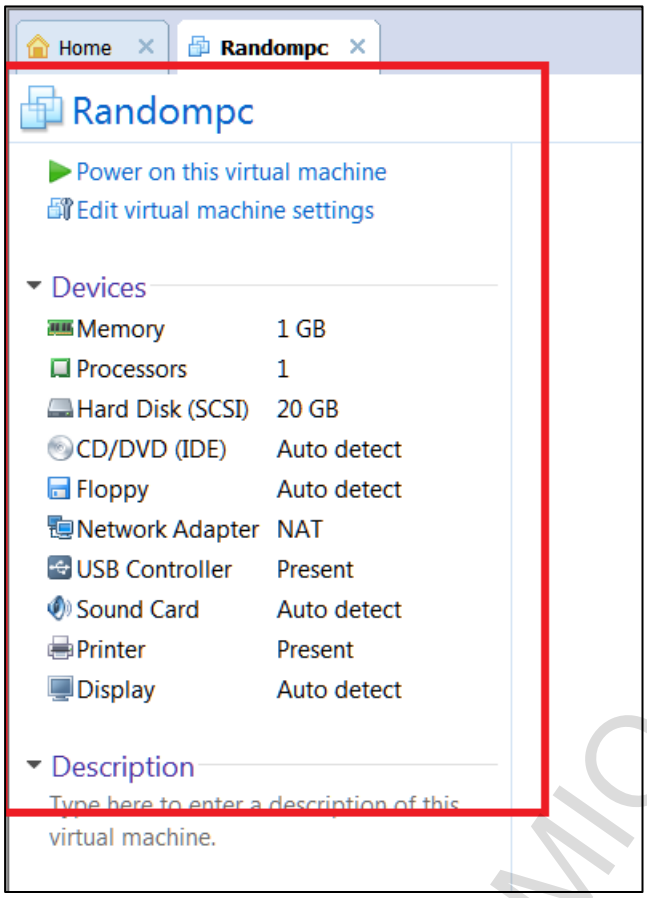
Dcfldd

Η εντολή 'dd' του Linux επιτρέπει στους χρήστες να κάνουν μια bit-προς-bit αντιγραφή ενός μέσου. Το εργαλείο 'dcfldd' , λειτουργεί παρόμοια με την εντολή 'dd', αλλά έχει πολλά χαρακτηριστικά σχεδιασμένα για την εγκληματολογία υπολογιστών (Dcffld).

Τέλος πρέπει να αναφέρουμε ότι τα προγράμματα που θα χρησιμοποιήσουμε είναι εγκατεστημένα/αποθηκευμένα σε μια εξωτερική μονάδα αποθήκευσης μεγέθους 500GB.Αυτό μας επιτρέπει να εκτελούμε τα προγράμματα αυτά γρήγορα και εύκολα και χωρίς να επιφέρουμε αλλαγές στο υπολογιστικό σύστημα που εξετάζουμε

6.7. Δημιουργία των εικονικών μηχανών

Τα Vm δημιουργήθηκαν με το VMware® Workstation 9.0.0. Αρχικά δημιουργήθηκε ένα Vm στο οποίο εγκαταστάθηκε το λειτουργικό σύστημα Windows 7 Ultimate 64-bit σε έναν εικονικό δίσκο με μέγιστο μέγεθος 20 GB (NFTS) και με ένα ένα(1) GB Ram.Στα πλαίσια της έρευνας μας επιλέχθηκε να διαθέσουμε στο λειτουργικό μας σύστημα τους λιγότερο δυνατόν πόρους ώστε να περιορίσουμε το μέγεθος των προς εξέτασιν δεδομένων.



Εικόνα 6-3: Χαρακτηριστικά εικονικής μηχανής

Για κάθε σενάριο που θα εξετάσουμε απαιτείται η εκ νέου δημιουργία ενός «καθαρού» Vm ώστε να αποκλείσουμε κάθε ενδεχόμενο να βρούμε δεδομένα που δεν ανταποκρίνονται στην πραγματικότητα.

Για να αποφύγουμε την χρονοβόρα διαδικασία της δημιουργίας καινούργιων Vm, της εγκατάστασης του λειτουργικού συστήματος των Windows και της ενημέρωσης του με τις τελευταίες αναβαθμίσεις θα χρησιμοποιήσουμε την επιλογή του Snapshot (VMware).

Η λειτουργία Snapshot χρησιμοποιείται όταν θέλουμε να διατηρήσουμε την ακριβή κατάσταση μιας εικονικής μηχανής ώστε να επιστρέψουμε σε αυτήν επανειλημμένα. Ένα στιγμιότυπο(snapshot) διατηρεί την εικονική μηχανή όπως ακριβώς ήταν όταν πήραμε το στιγμιότυπο .Όταν επιστρέφουμε σε ένα στιγμιότυπο αποβάλλουμε όλες τις αλλαγές που έγιναν στην εικονική μηχανή από τη στιγμή που πήραμε το στιγμιότυπο αυτό.

6.8. Αρχεία

Στα πλαίσια της έρευνας μας θα χρησιμοποιήσουμε ένα αριθμό αρχείων. Τα αρχεία αυτά θα ανήκουν σε διάφορες κατηγορίες(.pdf, .jpeg κ.α).

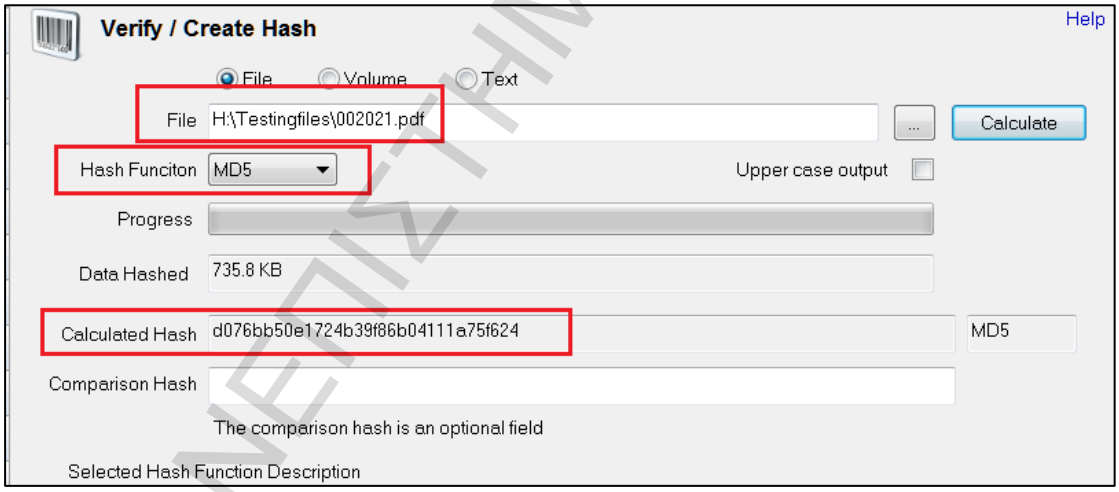
Συγκεκριμένα θα επισκεφτούμε τον ιστότοπο της DigitalCorpora. Πρόκειται για μια ιστοσελίδα που χρησιμοποιείται στην εκπαίδευση της εγκληματολογίας υπολογιστών. Παρέχει πρόσβαση σε ένα πλήθος αρχείων όπως εικόνες δίσκων, πακέτα δικτύων κ.α.

Θα επιλέξουμε ένα σύνολο αρχείων που θα χρησιμοποιήσουμε στην έρευνα μας. Τέλος η ιστοσελίδα αυτή μας παρέχει την δυνατότητα να βρούμε εύκολα και γρήγορα την τιμή κατακερματισμού των αρχείων που μας ενδιαφέρουν καθώς και τα μεταδεδομένα τους (Digital Corpora). Τα αρχεία παρουσιάζονται στον πίνακα που ακολουθεί.

Πίνακας 6-6: Παρουσίαση των αρχείων που θα διακινήσουμε

Όνομα	Μέγεθος	MD5 hash	Ημερομηνία (Created/Accessed/modified)
002021.pdf	753418	d076bb50e1724b39f86b04111a75f624	31-08-2013 17:42
002052.txt	95225	2c6d3b78a52e6ba8ccede39f7eff55a4	31-08-2013 17:42
002098.jpg	115561	b417b165ff13812b4d7a2c35a71ca88f	31-08-2013 17:42
002150.doc	256000	ec84d2595a6f7e0da5252a61d63fcc69	31-08-2013 15:18

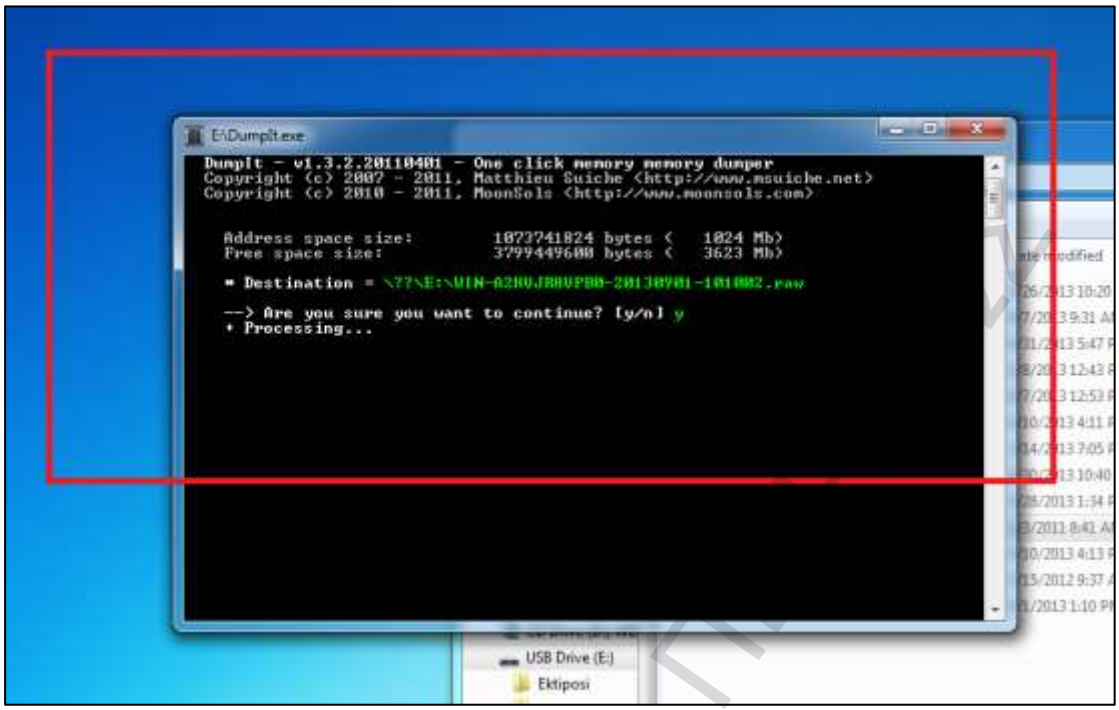
Στην συνέχεια χρησιμοποιώντας την σουίτα εργαλείων OSForensics επαληθεύουμε ότι οι κώδικες κατακερματισμού των αρχείων που «κατεβάσαμε» παραμένουν αναλλοίωτοι.



Εικόνα 6-4: Διαδικασία δημιουργίας κωδικών κατακερματισμού

6.9. Δημιουργία Δικανικών Εικόνων

Αρχικά συνδέουμε το USB δίσκο μας στο προς εξέταση Vm. Χρησιμοποιούμε το πρόγραμμα dumpit για την απόκτηση της μνήμη RAM του υπολογιστή. Όταν το πρόγραμμα ολοκληρωθεί ,τα περιεχόμενα της μνήμης RAM θα έχουν αποθηκευθεί σε ένα αρχείο της μορφής %% όνομα υπολογιστή-%%ημερομηνία-%ώρα.raw%.



Εικόνα 6-5: Χρήση του προγράμματος dumpit

Το επόμενο βήμα είναι να δημιουργήσουμε την εικόνα του υπολογιστικού συστήματος που θα εξετάσουμε. Πλοηγούμαστε στις ρυθμίσεις του BIOS και επιλέγουμε σαν πρώτη συσκευή εκκίνησης (First boot device) το CD-ROM. Στην συνέχεια επανεκκινούμε την εικονική μηχανή τρέχοντας όμως το Backtrack Live CD και όχι το λειτουργικό σύστημα των Windows.

Επιλέγουμε το Backtrack Forensics για τους λόγους που αναφέραμε στο προηγούμενο κεφάλαιο.

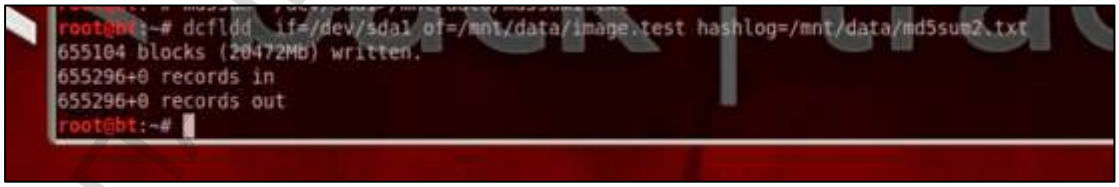
Εικόνα 6-6: Επιλογή του τρόπου λειτουργίας του Backtrack

Αφού φορτώσει το λειτουργικό Backtrack ανοίγουμε ένα τερματικό παράθυρο. Στην συνέχεια με την χρήση της εντολής *fdisk* βρίσκουμε χρήσιμες πληροφορίες τόσο για τον σκληρό δίσκο της εικονικής μηχανής -dev/sda1- , όσο και για τον εξωτερικό σκληρό που θα αποθηκεύσουμε τα δεδομένα-/dev/sdb1.

Εικόνα 6-7: Πληροφορίες για τους σκληρούς δίσκους

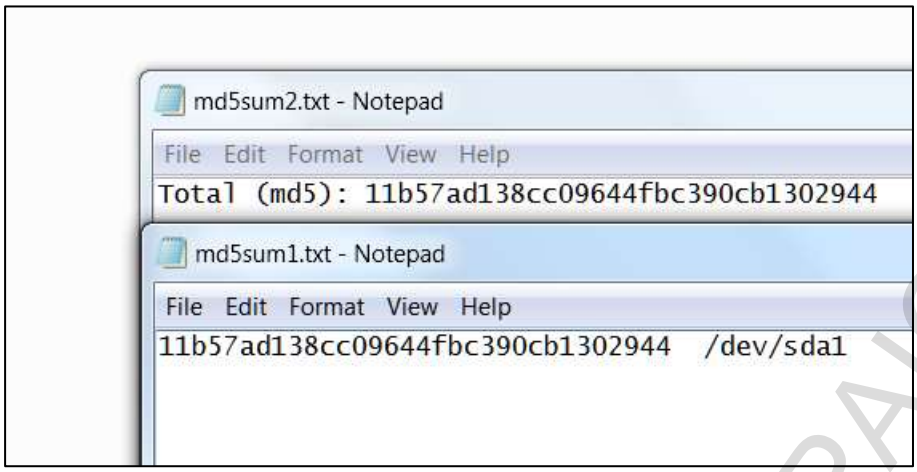
Στην συνέχεια θα χρησιμοποιήσουμε το πρόγραμμα *Dcfldd*. Αρχικά μέσω της εντολής *mount* δημιουργούμε μια εικονική σύνδεση μεταξύ του εξωτερικού σκληρού δίσκου και του λειτουργικού Backtrack. Με την εντολή *md5sum* δημιουργούμε το ψηφιακό αποτύπωμα του στόχου μας. Τέλος με την εντολή *dcfldd* αρχίζουμε την διαδικασία της δημιουργίας της εικόνας καθώς και του ψηφιακού αποτυπώματος της.

Εικόνα 6-8: Ακολουθία εντολών για την δημιουργία της εικόνας



Εικόνα 6-9: Ολοκλήρωση της δημιουργίας της εικόνας

Μετά την ολοκλήρωση της διαδικασίας συγκρίνουμε το αρχικό και το τελικό ψηφιακό αποτύπωμα προκειμένου να εξασφαλίσουμε την ακεραιότητα των δεδομένων μας.



Εικόνα 6-10: Επιβεβαίωση ακεραιότητας της εικόνας

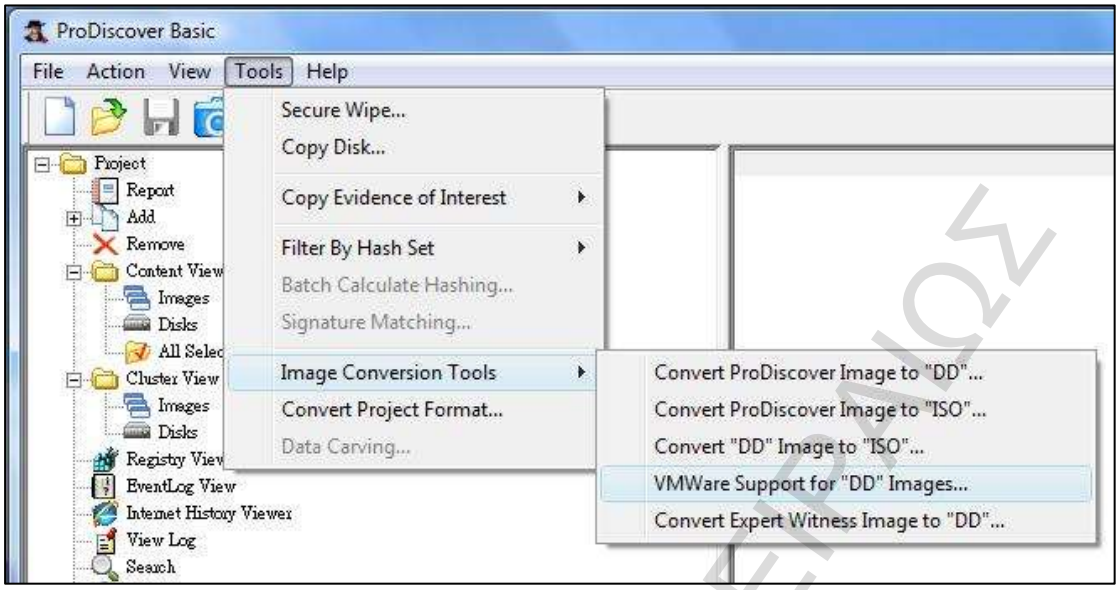
Αυτό σημαίνει ότι το αρχείο image.dd αποτελεί ένα πιστό αντίγραφο του σκληρού δίσκου της εικονικής μηχανής

6.10. Ανάλυση Δικανικών Εικόνων

Τώρα μπορούμε να χρησιμοποιήσουμε διάφορα εργαλεία (π.χ. το FTK Imager) για να αναλύσουμε την εικόνα που έχουμε αποκτήσει. Λόγω του γεγονότος ότι η έρευνά μας περιορίζεται σε μια συγκεκριμένη εφαρμογή θα χρησιμοποιήσουμε απλές μεθόδους και συγκεκριμένα προγράμματα.

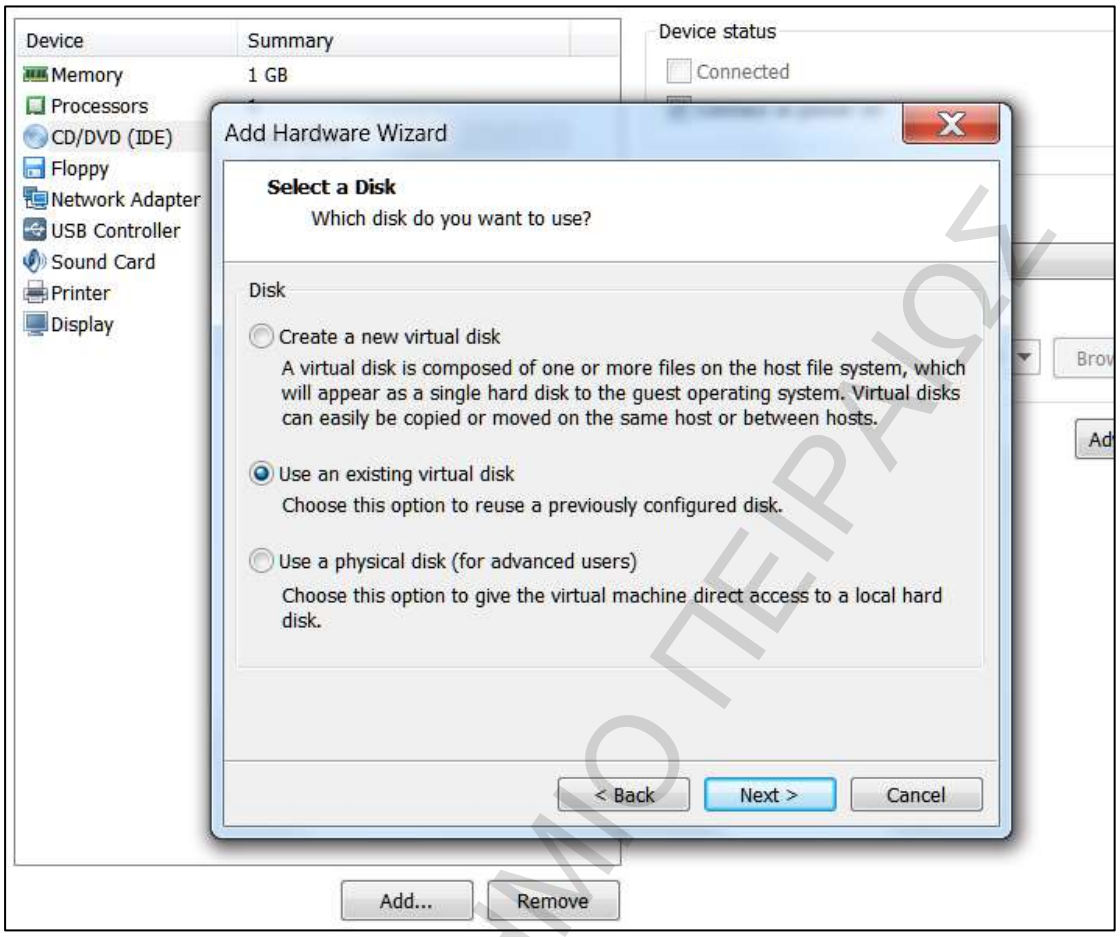
Πριν προχωρήσουμε περαιτέρω θα πρέπει να αναφέρουμε ότι χρησιμοποιούμαι ένα αντίγραφο της αρχικής εικόνας που έχουμε αποκτήσει. Χρησιμοποιούμε το FTK Imager για την δημιουργία δικανικών εικόνων των αρχείων που ανακτήσαμε στο προηγούμενο βήμα .Έτσι τα αυθεντικά αρχεία παραμένουν απροσπέλαστα και αναλλοίωτα.

Αρχικά χρησιμοποιούμε το πρόγραμμα Prodiscover Basic. Το πρόγραμμα αυτό έχει την δυνατότητα να δημιουργήσει τα αρχεία που χρειάζονται ώστε να μπορούμε να «φορτώσουμε» την εικόνα που δημιουργήσαμε σε μια εικονική μηχανή. Συγκεκριμένα με βάση το αρχείο image.dd δημιουργεί το αρχείο image.Vmdk και το οποίο θα χρησιμοποιήσουμε στην συνέχεια.



Εικόνα 6-11: Στιγμιότυπο από την χρήση του προγράμματος Prodiscover

Δημιουργούμε μια νέα εικονική μηχανή με την χρήση του VMWare. Χρησιμοποιούμε τον οδηγό(wizard) και επιλέγουμε να εγκαταστήσουμε το λειτουργικό αργότερα .Όλες οι άλλες ρυθμίσεις είναι οι προεπιλεγμένες. Στην συνέχεια, αφαιρούμαι την προεπιλεγμένη μονάδα σκληρού δίσκου και επιλέγουμε να προσθέσουμε το αρχείο που δημιουργήθηκε με το Prodiscover Basic.



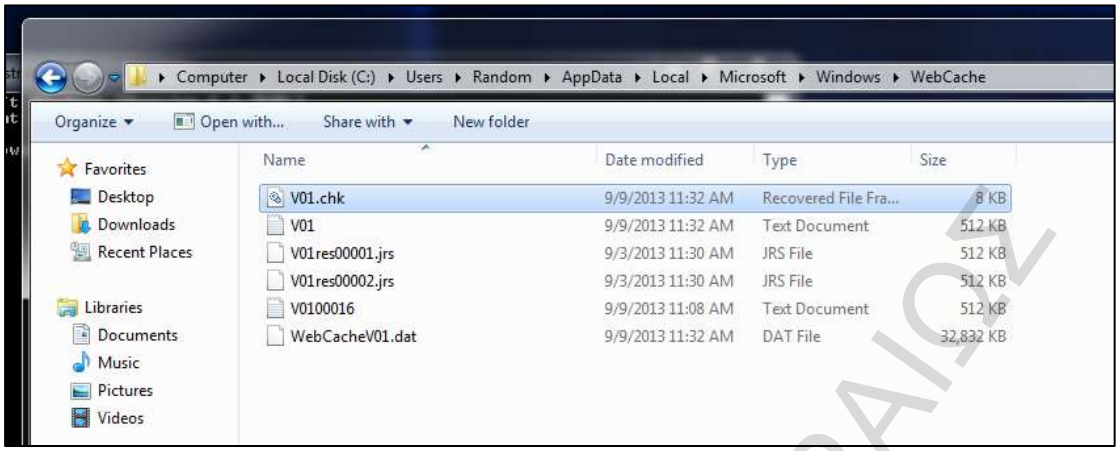
Εικόνα 6-12: Προσθήκη του εικονικού δίσκου που δημιουργήσαμε

Με αυτό τον τρόπο δημιουργήσαμε μια, δικανικά ασφαλή, εικονική μηχανή του προς εξέτασιν υπολογιστικού συστήματος

6.11. Ανάλυση των περιηγητών

6.11.1 Ανάλυση του Internet Explorer 10 (IE)

Ο Internet Explorer 10 χρησιμοποιεί μια ESE βάση δεδομένων που ονομάζεται WebCacheV01.dat για να διατηρήσει το ιστορικό, τα cookies και γενικά οποιαδήποτε άλλη πληροφορία δημιουργείται από την χρήση του. Αυτή η βάση δεδομένων περιέχει έναν πλούτο των πληροφοριών που μπορεί να έχει μεγάλο ενδιαφέρον για τον δικανικό ερευνητή (Bonnie Malmström & Philip Teveldal, 2013).



Εικόνα 6-13: Παρουσίαση των, προς εξέτασιν, αρχείων του Internet Explorer

Πριν αναλύσουμε την βάση αυτή πρέπει να διαπιστώσουμε σε πια κατάσταση βρίσκεται. Αυτό γίνεται με την χρήση της εντολής *esentutl /mh WebCacheV01.dat.* Αν η κατάσταση της είναι «βρώμικη» (dirty) σημαίνει ότι τα log αρχεία που έχουν δημιουργηθεί από την χρήση του Internet Explorer δεν έχουν ενσωματωθεί στην βάση. Για να το πετύχουμε αυτό χρησιμοποιούμε την εντολή *esentutl /r V01 /d.*

Με το άνοιγμα της βάσης δεδομένων με το ESEDatabaseView και την πλοήγηση μας στο table Containers θα πάρουμε μια γενική εικόνα της βάσης δεδομένων του Internet Explorer.

Containers [Table ID = 9, 14 Columns]

ContainerId	SetId	Flags	Size	Limit	EntryMaxAge	LastAccessTime	Name
1	0	65	0	8388608	0	6/9/2013 9:10:56 πμ	feedplat
2	0	64	0	8388608	0	3/9/2013 8:30:37 πμ	ietld
3	0	68	0	8388608	0	9/9/2013 6:30:06 πμ	History
4	0	79	906280	262144000	0	9/9/2013 6:36:21 πμ	Content
5	0	64	0	8388608	0	9/9/2013 6:36:25 πμ	Cookies
6	0	112	0	1024	0	9/9/2013 6:36:21 πμ	iecompat
7	0	112	0	1024	0	9/9/2013 6:37:22 πμ	iecompatua
9	0	68	0	1024	0	9/9/2013 6:36:21 πμ	History
10	0	79	12297755	262144000	0	9/9/2013 6:36:21 πμ	Content
11	0	64	6562	1024	0	9/9/2013 6:36:21 πμ	Cookies
13	0	65	39	1024000	0	9/9/2013 6:37:28 πμ	DOMStore
14	0	64	0	8388608	0	9/9/2013 6:39:17 πμ	iedownload
15	0	64	0	8388608	0	9/9/2013 6:36:24 πμ	MSHist012013090920130910

Εικόνα 6-14: Παρουσίαση της βάσης δεδομένων του Internet Explorer(1)

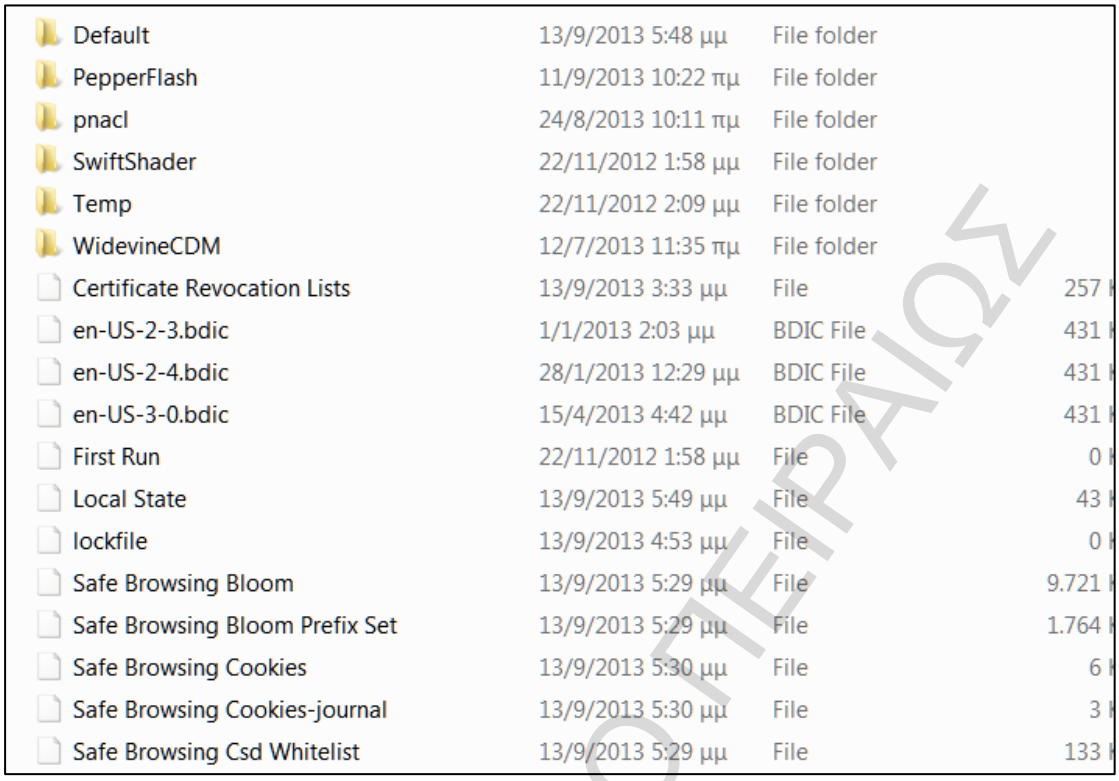
PartitionId	Directory
M	C:\Users\Random\AppData\Local\Microsoft\Feeds Cache\
M	C:\Users\Random\AppData\Roaming\Microsoft\Windows\IETldCache\
M	C:\Users\Random\AppData\Local\Microsoft\Windows\History\History.IE5\
M	C:\Users\Random\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
M	C:\Users\Random\AppData\Roaming\Microsoft\Windows\Cookies\
M	C:\Users\Random\AppData\Roaming\Microsoft\Windows\IECompatCache\
M	C:\Users\Random\AppData\Roaming\Microsoft\Windows\iecompatuaCache\
L	C:\Users\Random\AppData\Local\Microsoft\Windows\History\Low\History.IE5\
L	C:\Users\Random\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\
L	C:\Users\Random\AppData\Roaming\Microsoft\Windows\Cookies\Low\
L	C:\Users\Random\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\
M	C:\Users\Random\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
M	C:\Users\Random\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013090920130910\

Εικόνα 6-15: Παρουσίαση της βάσης δεδομένων του Internet Explorer(2)

Τα container τρία και έξι έχουν πολύ σημασία, διότι αυτά περιέχουν τις URL διευθύνσεις που επισκεφτήκατε, μαζί με τις χρονοσφραγίδες (timestamps).Το container δεκατρία με όνομα "iedownload" περιέχει τα πιθανά αρχεία που έχουμε «κατεβάσει»

6.11.2 Ανάλυση του Google chrome (GC)

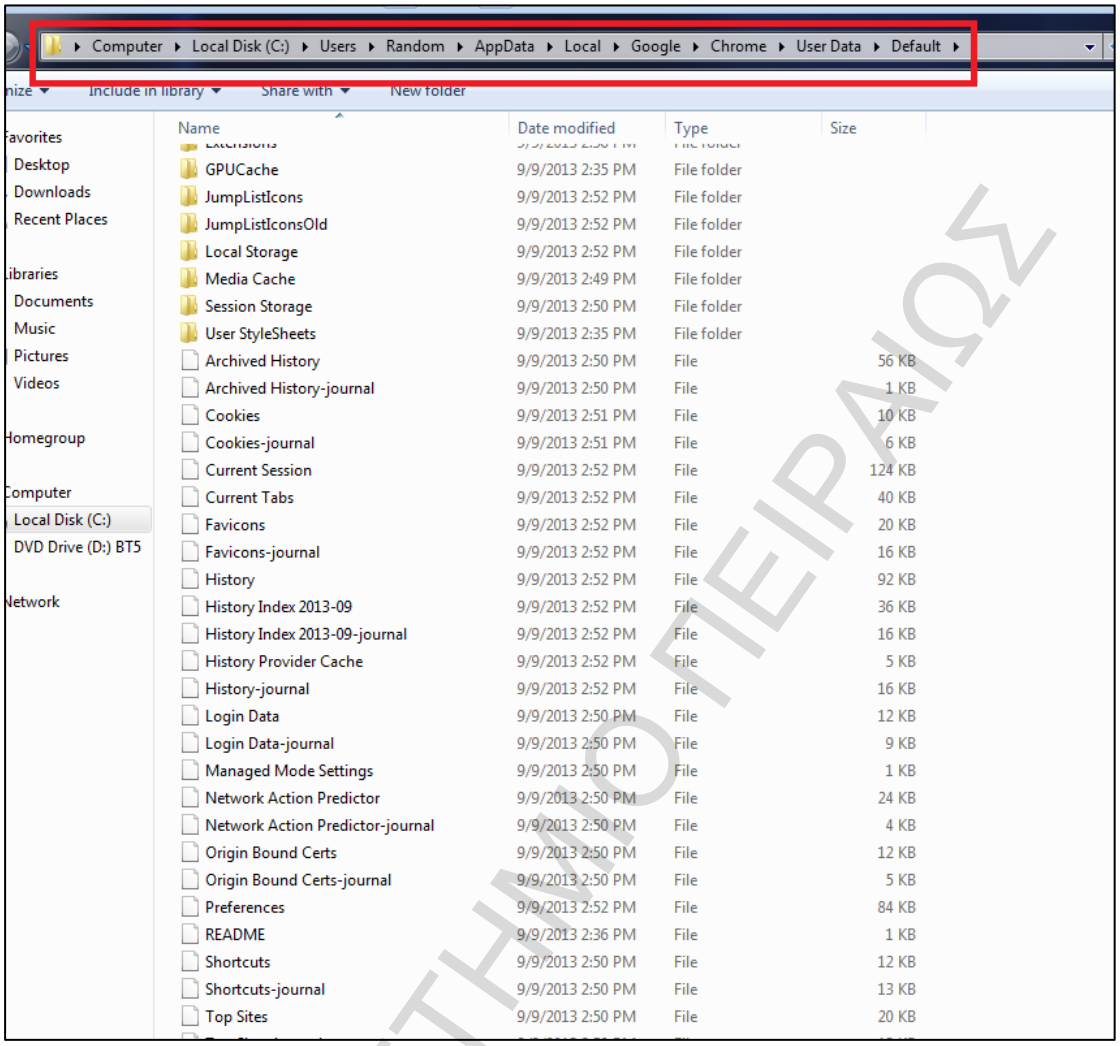
Τα δεδομένα που παράγονται από την χρήση του Chrome αποθηκεύονται στην εξής τοποθεσία *C:\Users\User name\AppData\Local\Google\Chrome*.



Default	13/9/2013 5:48 μμ	File folder	
PepperFlash	11/9/2013 10:22 πμ	File folder	
pnacl	24/8/2013 10:11 πμ	File folder	
SwiftShader	22/11/2012 1:58 μμ	File folder	
Temp	22/11/2012 2:09 μμ	File folder	
WidevineCDM	12/7/2013 11:35 πμ	File folder	
Certificate Revocation Lists	13/9/2013 3:33 μμ	File	257 K
en-US-2-3.bdic	1/1/2013 2:03 μμ	BDIC File	431 K
en-US-2-4.bdic	28/1/2013 12:29 μμ	BDIC File	431 K
en-US-3-0.bdic	15/4/2013 4:42 μμ	BDIC File	431 K
First Run	22/11/2012 1:58 μμ	File	0 K
Local State	13/9/2013 5:49 μμ	File	43 K
lockfile	13/9/2013 4:53 μμ	File	0 K
Safe Browsing Bloom	13/9/2013 5:29 μμ	File	9.721 K
Safe Browsing Bloom Prefix Set	13/9/2013 5:29 μμ	File	1.764 K
Safe Browsing Cookies	13/9/2013 5:30 μμ	File	6 K
Safe Browsing Cookies-journal	13/9/2013 5:30 μμ	File	3 K
Safe Browsing Csd Whitelist	13/9/2013 5:29 μμ	File	133 K

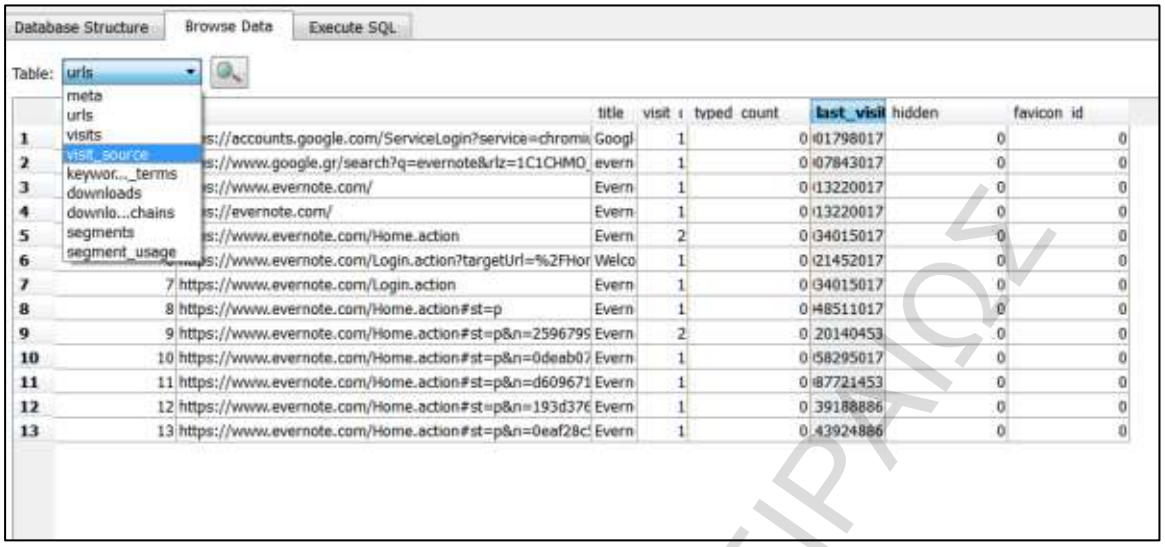
Εικόνα 6-16: Παρουσίαση των αρχείων του Google Chrome

Επίσης στον φάκελο Default βρίσκουμε αποθηκευμένα σε μορφή sql τα δεδομένα που δημιουργούνται από την χρήση του περιηγητή.(History,downloads, Login, κ.α)



Εικόνα 6-17: Παρουσίαση των, προς εξέτασιν, SQL βάσης δεδομένων

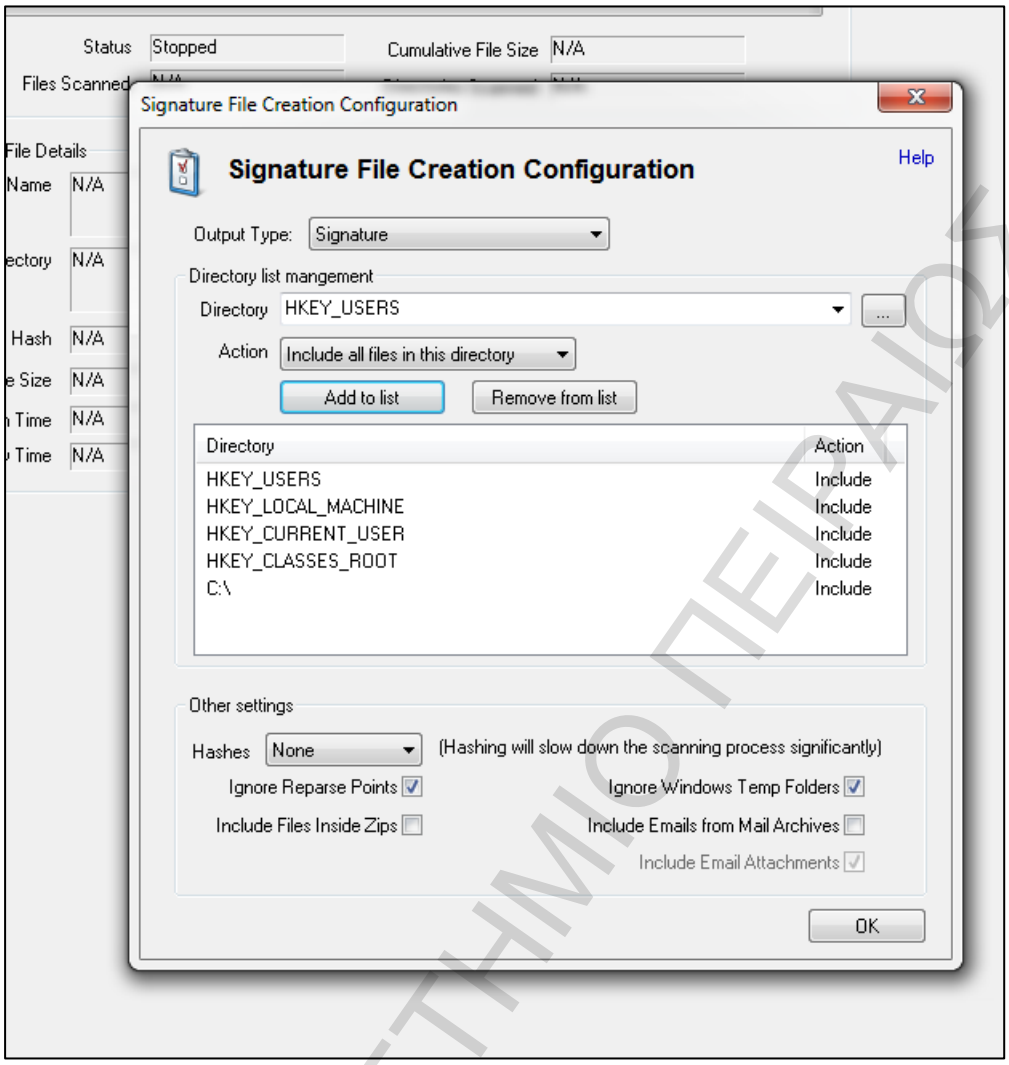
Χρησιμοποιώντας το πρόγραμμα SQLite Database Browser εξετάζουμε τα περιεχόμενα των αρχείων αυτών. Στο αρχείο History βρίσκουμε πληροφορίες όχι μόνο για τα τις διευθύνσεις που επισκεφθήκαμε αλλά και για τυχόν αρχεία που κατεβάσαμε.



Εικόνα 6-18: Εξέταση των βάσης δεδομένων του Google Chrome

6.12. Μεθοδολογία για την σύγκριση υπογραφών

Στα πλαίσια της έρευνας μας και για την εύρεση των αλλαγών που επιφέρουν η εγκατάσταση/απεγκατάσταση των προγραμμάτων που εξετάζουμε θα χρησιμοποιήσουμε την λειτουργία της δημιουργίας και σύγκρισης υπογραφών του OSForensics.



Εικόνα 6-19: Στιγμιότυπο από την διαδικασία δημιουργίας υπογραφών

Το OSForensics μας επιτρέπει να δημιουργήσουμε μια ιατροδικαστική/δικανική υπογραφή ενός σκληρού δίσκου .Συγκρίνοντας υπογραφές που δημιουργήθηκαν σε διαφορετικές χρονικές στιγμές μπορούμε να ανακαλύψουμε τις αλλαγές που έγιναν στο υπολογιστικό μας σύστημα (OSForensics).

6.13. Περιορισμοί της έρευνας

Εξαρτώμενη από την έκδοση: Λόγω του πειραματικού χαρακτήρα της έρευνας, τα αποτελέσματα ισχύουν για τις εκδόσεις του λογισμικού που χρησιμοποιήθηκαν κατά την διάρκεια της έρευνας. Οι προηγούμενες εκδόσεις του λογισμικού μπορεί να έχουν διαφορετικά αποτελέσματα ενώ οι μεταγενέστερες αλλαγές στο λογισμικό μπορεί να οδηγήσουν σε διαφορετικά συμπεράσματα. Επιπλέον, η πρόσβαση σε μια cloud υπηρεσία μέσω ενός περιηγητή βασίζεται στις πληροφορίες που επιστρέφονται από τον πάροχο. Αυτό μπορεί να αλλάξει, καθώς ο κάθε πάροχος ενημερώνει τον HTML-ή όποιον άλλον-κώδικα χρησιμοποιείται για την παρουσίαση των πληροφοριών στον τελικό χρήστη.

Εξαρτώμενη από το λειτουργικό σύστημα :Η έρευνα διεξήχθη αξιολογώντας τις αλλαγές που έγιναν στα αρχεία ενός συστήματος με λειτουργικό σύστημα Windows 7 και με το σύστημα αρχείων NTFS. Εναλλακτικά λειτουργικά συστήματα, όπως τα Microsoft Vista, XP, Apple Mac OSX ή Linux, μπορεί να έχουν διαφορετικά απομεινάρια δεδομένων. Εναλλακτικά συστήματα αρχείων, όπως το EXT3, μπορεί επίσης

να οδηγήσουν σε διαφορετικά ευρήματα. Ως εκ τούτου, μπορεί να υπάρχουν διαφορετικά πορίσματα σε σχέση με τις ερωτήσεις της έρευνας, όταν δεν χρησιμοποιούνται τα Windows 7 με το NFTS σύστημα αρχείων.

6.14. Συμπεράσματα

Το κεφάλαιο αυτό περιγράφει τον σκοπό της έρευνας μας. Καταγράψαμε τα ερωτήματα της έρευνας μας και μέσω της μεθοδολογίας προσδιορίσαμε την διαδικασία που θα ακολουθήσουμε στα επόμενα κεφάλαια. Περιγράψαμε το υλισμικό και το λογισμικό που θα χρησιμοποιήσουμε και προσδιορίσαμε τους περιορισμούς της έρευνας μας.

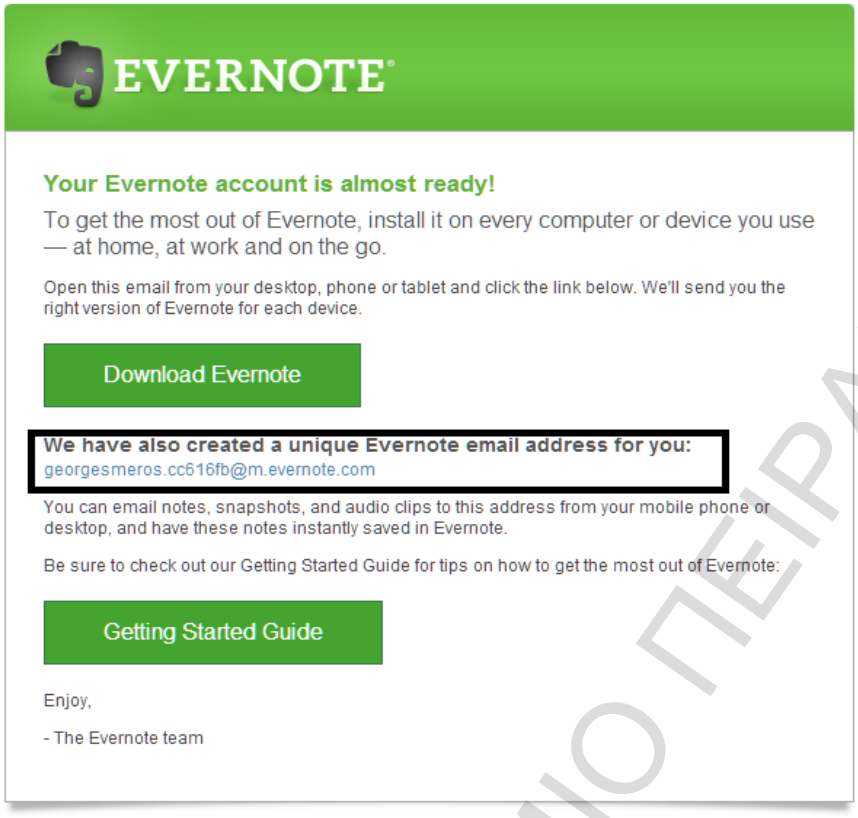
Κεφάλαιο 7: Ψηφιακή Εγκληματολογική Ανάλυση του Evernote

7.1. Εισαγωγή

Το Evernote είναι μια σουίτα λογισμικού και υπηρεσιών που έχει σχεδιαστεί για την δημιουργία σημειώσεων και την αρχειοθέτηση εγγράφων. Ένα «σημείωμα» μπορεί να είναι ένα κομμάτι από ένα κείμενο, μια πλήρη ιστοσελίδα ή ένα απόσπασμα της ιστοσελίδας, μια φωτογραφία, ένα αρχείο ήχου, ή ένα χειρόγραφο σημείωμα. Οι σημειώσεις μπορούν επίσης να έχουν συνημμένα αρχεία. Το Evernote υποστηρίζει μια σειρά από πλατφόρμες λειτουργικών συστημάτων (συμπεριλαμβανομένων των OS X, iOS, Chrome OS, Android, Microsoft Windows, Windows Phone και BlackBerry) και, επίσης, προσφέρει online συγχρονισμό και back-up των «σημειώσεων» του χρήστη (Evernote, 2013).

Το Evernote, όπως είδαμε, μπορεί να τρέξει σε πολλές διαφορετικές συσκευές και οι χρήστες με σύνδεση στο διαδίκτυο μπορούν επίσης να επωφεληθούν από τις λειτουργίες συγχρονισμού που παρέχονται από την υπηρεσία αυτή. Όταν ένα αντίγραφο των δεδομένων αποθηκεύεται στο cloud,σε έναν server του Evernote δηλαδή, τότε αυτά τα δεδομένα συγχρονίζονται με όλες τις συσκευές στις οποίες λειτουργεί το Evernote. Υπάρχει η ελεύθερη και πιο περιορισμένη έκδοση του Evernote με ένα ανώτατο μηνιαίο όριο χρήσης(60 MB).Τέλος υπάρχει και η πληρωμένη έκδοση χωρίς κάποιο περιορισμό χρήσης.

Το Evernote απαιτεί από τους χρήστες να έχουν ένα λογαριασμό, για τον οποίο απαιτείται μια έγκυρη ηλεκτρονική διεύθυνση-που μπορεί να χρησιμοποιηθεί και σαν όνομα χρήστη- και ένα συνθηματικό. Με την εγγραφή του χρήστη το Evernote θα δημιουργήσει επίσης μια μοναδική διεύθυνση ηλεκτρονικού ταχυδρομείου του Evernote.Έτσι θα μπορούμε να στέλνουμε μέσω ηλεκτρονικού ταχυδρομείου τις σημειώσεις μας στο Evernote και αυτές να προσθέτονται αυτόματα στον λογαριασμό μας.



Εικόνα 7-1: Διεύθυνση ηλεκτρονικού ταχυδρομείου του Evernote

7.2. Σκοπός/Στόχος

Ο σκοπός της παρούσας έρευνας είναι να προσδιορίσουμε τα υπολείμματα δεδομένων σε έναν υπολογιστή με Windows 7 μετά την χρήση του Evernote, όπως το όνομα χρήστη, ο κωδικός πρόσβασης, τα αρχεία που αποθηκεύτηκαν στο λογαριασμό, και τα σχετικά με αυτά τα αρχεία μεταδεδομένα.Επίσης στα πλαίσια της έρευνας χρησιμοποιούμε αντιδικανικές διαδικασίες για την σύγκριση της αρχικής και της τελικής κατάστασης του συστήματος.

7.3. Ανάλυση του Evernote στο περιβάλλον των Windows 7

7.3.1 Προετοιμασία

Για την συλλογή των δεδομένων που απαιτούνται για να απαντήσουμε στις ερωτήσεις της έρευνας μας δημιουργήσαμε μια εικονική μηχανή. Ακολουθώντας την μεθοδολογία που προσδιορίσαμε στο κεφάλαιο χρησιμοποιήσαμε το Evernote για την δημιουργία σημειώσεων και την επισύναψη 3 αρχείων(.pdf,.txt,.jpeg). Τέλος εξετάσαμε και τις λειτουργίες συγχρονισμού που προσφέρει.

Για την προετοιμασία της έρευνας του Evernote,εκτός από το λογισμικό που αναλύσαμε στο κεφάλαιο 6, χρησιμοποιήσαμε επίσης:

- Evernote version 5.0.0.1137
- CCleaner v3.17.1689
- Eraser
- SQLite Database Browser 2.0 b1
- ESEDatabaseView v1.07
- Internet explorer 10

- Google Chrome Version 29.0.1547.66

Τέλος στα πλαίσια της προετοιμασίας έχουμε χρησιμοποιήσει την λειτουργία δημιουργίας υπογραφών του OSFORENSICS πριν και μετά την εγκατάσταση του Evernote ώστε να ανακαλύψουμε με ακρίβεια και αποτελεσματικότητα τις αλλαγές που έγιναν στο λειτουργικό σύστημα της εικονικής μηχανής.

Δημιουργήσαμε μια σειρά από σημειώσεις. Κάποιες από αυτές είναι μόλις μια σειρά χαρακτήρων. Άλλες περιέχουν αποσπάσματα από βιβλία. Κάποιες από αυτές περιέχουν επισυνημμένα αρχεία. Τέλος κάποιες από αυτές είναι στα ελληνικά.

7.3.2 Αναγνώριση και Ανάκτηση

Στο πλαίσιο αυτής της έρευνας, εντοπίστηκαν τα μέσα που θα περιέχουν τις πληροφορίες που απαιτούνται για τη διεξαγωγή της ανάλυσης. Πρόκειται για την μνήμη RAM της εικονικής μηχανής και τον σκληρό δίσκο του VM.Ακολουθώντας τις διαδικασίες που προσδιορίσαμε στο κεφάλαιο 6,ανακτήσαμε με δικανικά αποδεκτό τρόπο την μνήμη RAM και τον σκληρό δίσκο της προς εξέτασιν εικονικής μηχανής.

7.3.3 Διατήρηση

Για την έρευνα αυτή δημιουργήσαμε ένα δικανικό αντίγραφο των δυο αρχείων που αποκτήσαμε στο στάδιο της συλλογής και της ανάκτησης. Για να το πετύχουμε αυτό χρησιμοποιήσαμε το πρόγραμμα Access Data FTK Imager.

7.3.4 Ανάλυση

Στο στάδιο αυτό χρησιμοποιήσαμε μια σειρά από εργαλεία όπως το OSFORENSICS.Αρχικά θέλουμε να προσδιορίσουμε τις αλλαγές που γίνονται στο λειτουργικό των Windows με την εγκατάσταση και την απεγκατάσταση του Evernote. Θέλουμε να δούμε δηλαδή αν μπορούμε να ανακαλύψουμε ότι χρησιμοποιήθηκε το πρόγραμμα αυτό ακόμα και αν έχει απεγκατασταθεί από το λειτουργικό σύστημα.

Για αυτό τον λόγο χρησιμοποιούμαι το OSFORENSICS και την επιλογή της δημιουργίας και σύγκρισης υπογραφών .Στον πίνακα που ακολουθεί βλέπουμε τα αρχεία που δημιουργήθηκαν με την εγκατάσταση του Evernote. Πρέπει να επισημάνουμε την προσοχή μας στα αρχείο στον φάκελο “Databases”.

Πίνακας 7-1: Αρχεία που δημιουργούνται με την εγκατάσταση του Evernote

C:\ProgramData\Microsoft\Windows\StartMenu\Programs\Evernote\Evernote.lnk,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\.accounts,"6/9/2013, 12:40
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\.sessiondata,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\georgesmeros.exb,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\georgesmeros.exb.activitylog,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\georgesmeros.exb.announcements,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\georgesmeros.exb.bak,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Databases\georgesmeros.exb.snippets,"6/9/2013, 12:40
C:\Users\Random\AppData\Local\Evernote\Evernote\Dict\user.dic,"6/9/2013, 12:40
C:\Users\Random\AppData\Local\Evernote\Evernote\Logs\AppLog_2013-09-06.txt,"6/9/2013, 12:39
C:\Users\Random\AppData\Local\Evernote\Evernote\Logs\enclipper_2013-09-06.txt,"6/9/2013, 12:39

Με αυτόν τον τρόπο προσδιορίσαμε τα αρχεία στα οποία θα επικεντρωθούμε στα μετέπειτα στάδια της έρευνας μας. Στην συνέχεια εξετάζουμε τις αλλαγές που έγινα στην Registry των Windows.

Πίνακας 7-2: Αλλαγές στην Registry των Windows

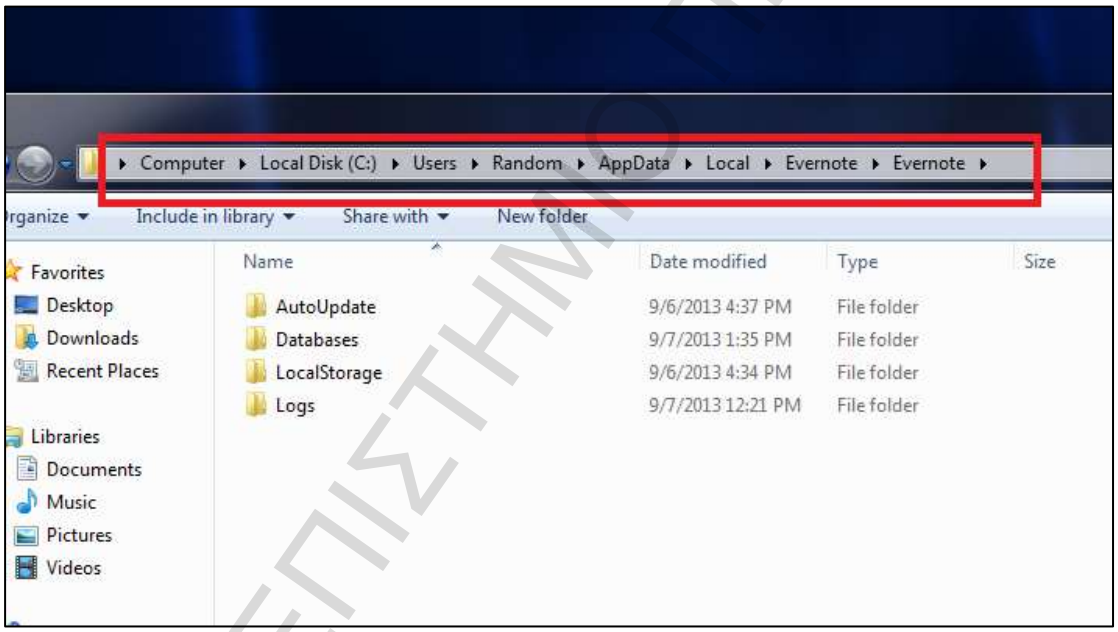
HKEY_CURRENT_USER\Software\Evernote\Evernote,"1/1/1601, 3:00
HKEY_CURRENT_USER\Software\Evernote\Evernote3,"1/1/1601, 3:00
HKEY_CURRENT_USER\Software\Evernote\Evernote5,"1/1/1601,3:00
HKEY_CURRENT_USER\Software\Evernote\Evernote\ApplicationLanguage,"1/1/1601, 3:00
HKEY_CURRENT_USER\Software\Evernote\Evernote\AudioRecordingLevel,"1/1/1601,3:00
HKEY_CURRENT_USER\Software\Evernote\Evernote\AutoResponse,"1/1/1601, 3:00

7.4. Χρήση του λογισμικού της εφαρμογής

7.4.1 Εξέταση των αρχείων

Όπως προσδιορίσαμε στο προηγούμενο υποκεφάλαιο το Evernote αποθηκεύει τα αρχεία που χρησιμοποιεί στην ακόλουθη τοποθεσία:C:\Users\\AppData\Local\Evernote\Evernote\Database\ .Στο σενάριο μας είναι η εξής: C:\Random\\AppData\Local\Evernote\Evernote\Database\.

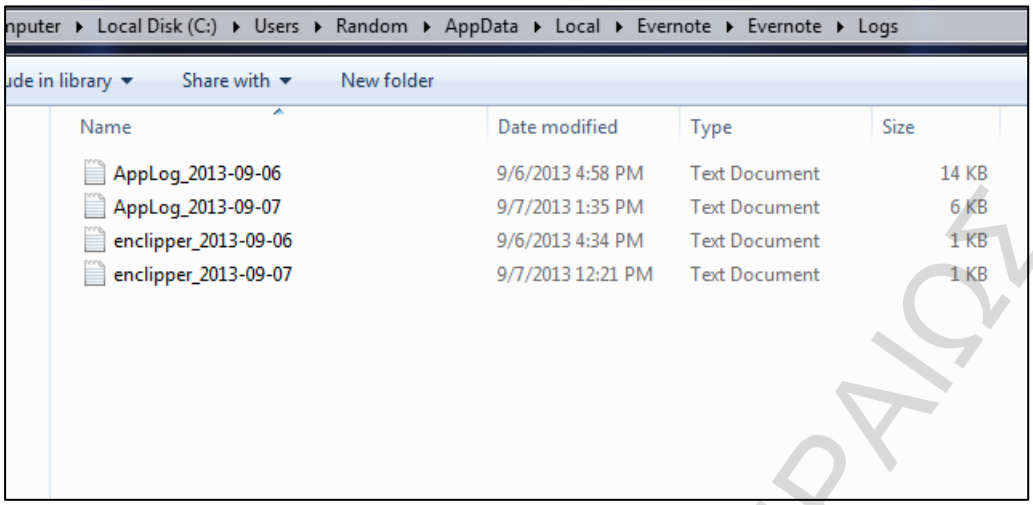
Στην εικόνα που ακολουθεί παρουσιάζονται συνοπτικά τα αρχεία.



Εικόνα 7-2: Προς εξέτασιν αρχεία του Evernote

7.4.2 Αρχεία καταγραφής συμβάντων

Πρώτα θα εξετάσουμε τα αρχεία καταγραφής συμβάντων.



Εικόνα 7-3: Αρχεία καταγραφής συμβάντων

Στον φάκελο αυτό είναι αποθηκευμένα τα αρχεία καταγραφής των ενεργειών του Evernote. Συγκεκριμένα καταγράφονται οι ενέργειες συγχρονισμού του Evernote με τον Server της cloud αυτής εφαρμογής. Έτσι ανακαλύπτουμε τα «notes» που είτε είναι ήδη αποθηκευμένα στον λογαριασμό του χρήστη είτε τα δημιούργησε στο σύστημα που εξετάζουμε. Στους πίνακες που ακολουθούν παραθέτουμε όλες τις πληροφορίες που ανακτήσαμε.

Πίνακας 7-3: Καταχώριση του αρχείου καταγραφής συμβάντων(1)

```
14:06:52 [2700] 100% Creating local note "this is an importan document saved i."
, resource count: 0
14:06:52 [2700] 100% * guid={7052CE90-98EB-4885-BB0D-29B1BB35DFDD}
```

Πίνακας 7-4:Καταχώριση του αρχείου καταγραφής συμβάντων(2)

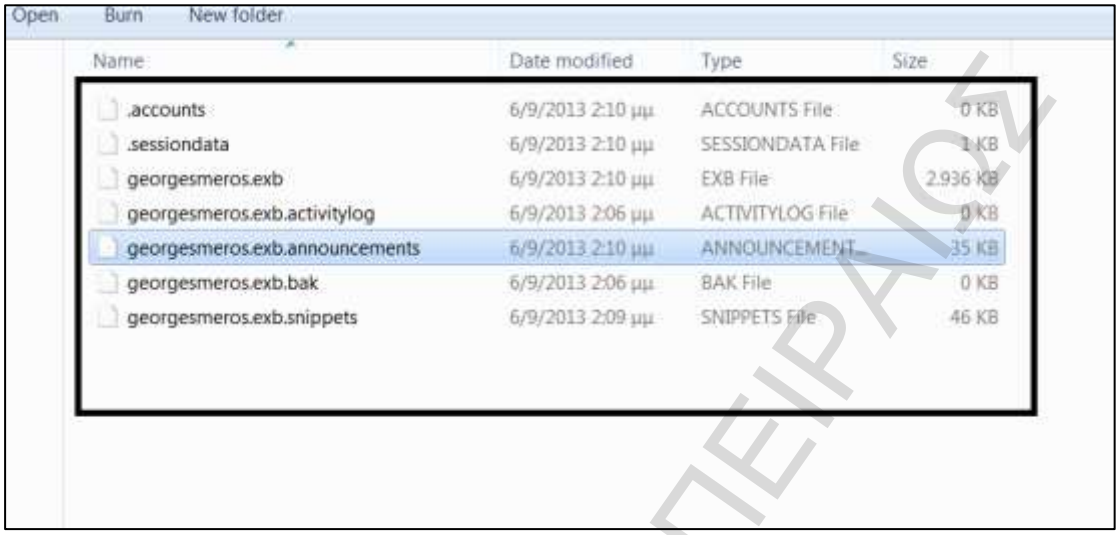
```
14:09:44 [2700] 67% Creating server note "pdf file", resource count: 1
14:09:58 [2700] 67% * guid={c99742ff-c5f6-45c6-9ac1-5e0ee72c76f2}
14:09:58 [2700] 67% * rsrc={84f187ef-12af-4d81-8cd7-59357eed4839}, note={c99742ff-c5f6-45c6-9ac1-
5e0ee72c76f2}
14:09:58 [2700] 67% * updateCount: 25 --> 26
14:09:58 [2700] 67% * updateCount: 26 --> 27
```

Πίνακας 7-5:Καταχώριση του αρχείου καταγραφής συμβάντων(3)

```
14:09:58 [2700] 89% Creating server note "image", resource count: 1
14:10:01 [2700] 89% * guid={193d376b-a3be-426f-8681-ac4a6492267c}
14:10:01 [2700] 89% * rsrc={3161c1e3-bb2e-44a4-87d3-33a75d895bdf}, note={193d376b-a3be-426f-8681-
ac4a6492267c}
14:10:01 [2700] 89% * updateCount: 27 --> 28
14:10:01 [2700] 89% * updateCount: 28 --> 29
14:10:01 [2700] 100% * saved updateCount: 29
```

7.4.3 Εξέταση της βάσης δεδομένων της εφαρμογής

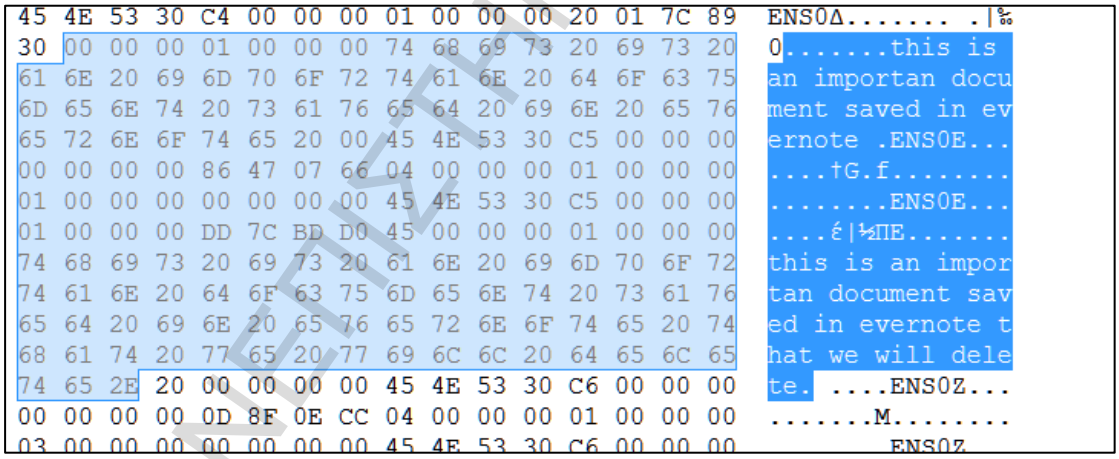
Στο υποκεφάλαιο αυτό θα εξετάσουμε τα αρχεία που βρίσκονται στον φάκελο 'Databases'.



Εικόνα 7-4: Παρουσίαση των SQL βάσεων δεδομένων του Evernote

georgesmeros.exb.snippets

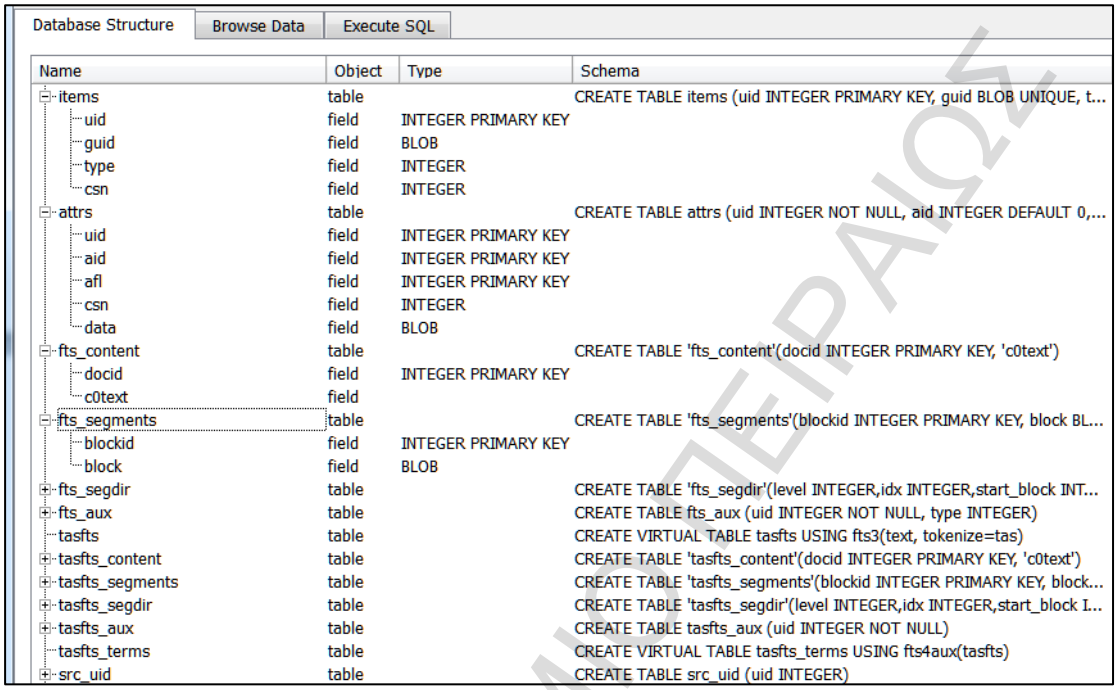
Το αρχείο αυτό το εξετάζουμε με την χρήση του hexeditor. Περιέχει-όπως υποδηλώνει και ο τίτλος-αποσπάσματα από τα «notes» του λογαριασμού. Εδώ μπορέσαμε να ανακαλύψουμε έναν «note» μόνο.



Εικόνα 7-5: Περιεχόμενα του georgesmeros.exb.snippets

georgesmeros.exb

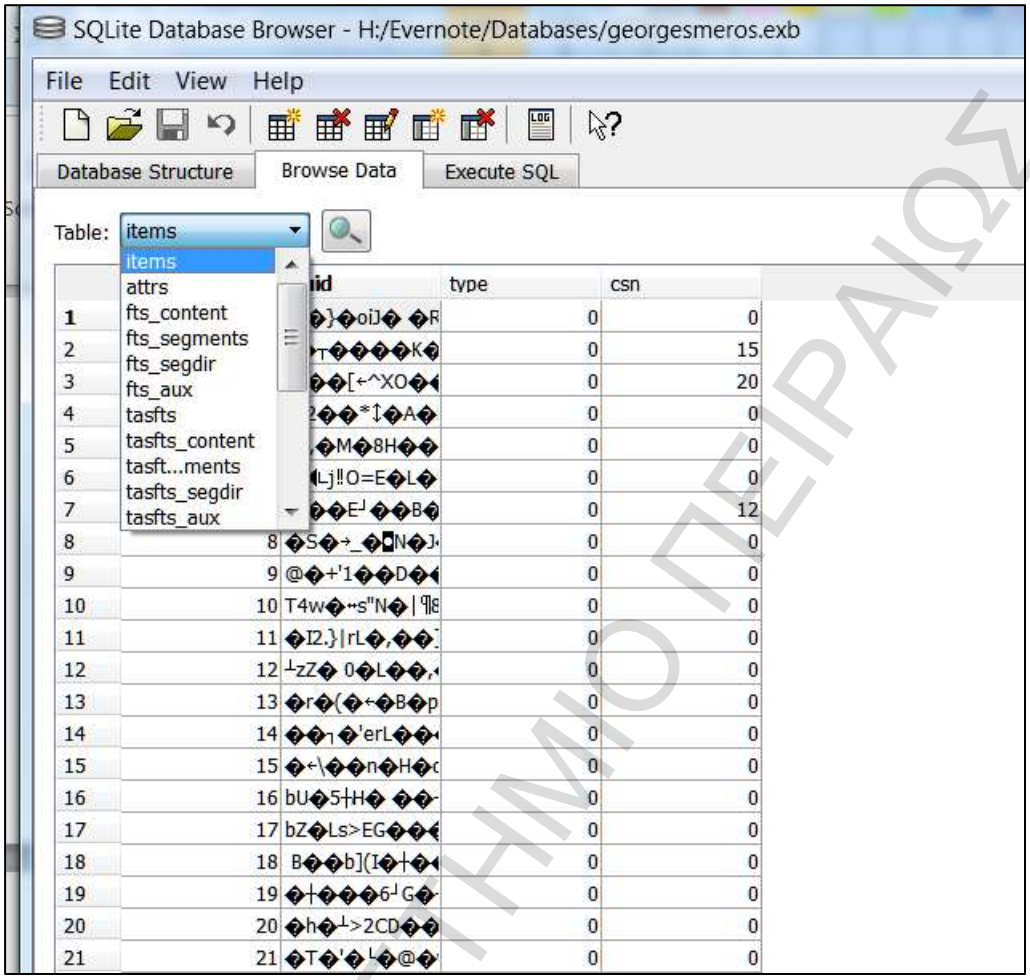
Πρόκειται για μια SQL βιβλιοθήκη για την εξέταση της οποίας χρησιμοποιούμαι το πρόγραμμα SQLite Database Browser. Στην εικόνα που ακολουθούν φαίνεται ο τρόπος δομής της βιβλιοθήκης αυτής.



Name	Object	Type	Schema
items	table		CREATE TABLE items (uid INTEGER PRIMARY KEY, guid BLOB UNIQUE, t...
uid	field	INTEGER PRIMARY KEY	
guid	field	BLOB	
type	field	INTEGER	
csn	field	INTEGER	
attrs	table		CREATE TABLE attrs (uid INTEGER NOT NULL, aid INTEGER DEFAULT 0,...
uid	field	INTEGER PRIMARY KEY	
aid	field	INTEGER PRIMARY KEY	
afl	field	INTEGER PRIMARY KEY	
csn	field	INTEGER	
data	field	BLOB	
fts_content	table		CREATE TABLE 'fts_content'(docid INTEGER PRIMARY KEY, 'c0text')
docid	field	INTEGER PRIMARY KEY	
c0text	field		
fts_segments	table		CREATE TABLE 'fts_segments'(blockid INTEGER PRIMARY KEY, block BL...
blockid	field	INTEGER PRIMARY KEY	
block	field	BLOB	
fts_segdir	table		CREATE TABLE 'fts_segdir'(level INTEGER,idx INTEGER,start_block INT...
fts_aux	table		CREATE TABLE fts_aux (uid INTEGER NOT NULL, type INTEGER)
tasfts	table		CREATE VIRTUAL TABLE tasfts USING fts3(text, tokenize=tas)
tasfts_content	table		CREATE TABLE 'tasfts_content'(docid INTEGER PRIMARY KEY, 'c0text')
tasfts_segments	table		CREATE TABLE 'tasfts_segments'(blockid INTEGER PRIMARY KEY, block...
tasfts_segdir	table		CREATE TABLE 'tasfts_segdir'(level INTEGER,idx INTEGER,start_block I...
tasfts_aux	table		CREATE TABLE tasfts_aux (uid INTEGER NOT NULL)
tasfts_terms	table		CREATE VIRTUAL TABLE tasfts_terms USING fts4aux(tasfts)
src_uid	table		CREATE TABLE src_uid (uid INTEGER)

Εικόνα 7-6: Δομή της βάσης δεδομένων georgesmeros.exb

Στην συνέχεια περιηγούμαστε στα δεδομένα της βιβλιοθήκης όπου έχουμε την δυνατότητα να εξετάσουμε όλα τα tables της βιβλιοθήκης αυτής.



Εικόνα 7-7: Περιεχόμενα της βάσης δεδομένων georgesmeros.exb

Θα επικεντρώσουμε την έρευνα μας στα ακόλουθα tables:

- Resourse_attr
- Note_attr
- Fts_content
- Atttrs

Resourse_attr

Εδώ βρίσκουμε πληροφορίες για τα δύο αρχεία που επισυνάψαμε. Συγκεκριμένα μπορούμε να ανακαλύψουμε την προέλευση των αρχείων αυτών, το μέγεθος τους και τις τιμές κατακερματισμού για καθένα από αυτά τα αρχεία. Αυτές οι τιμές κατακερματισμού ταυτίζονται με τις αρχικές. Τέλος δεν καταφέραμε να ερμηνεύσουμε τα δεδομένα στο κελί «date created» σε κάποια χρήσιμη πληροφορία.

	source_url	date_created							size	hash
27		5117.463171296							2041	0e2d61050811670832d80ed457203343
54		5117.463171296							2176	4914ced8925f9adcc1c58ab87813c81f
300		5117.463171296							6310	53df38a9b4999d2f9ababedaae41d3b0
27		5117.463171296							1871	836fc57702fc08596a5b6d74e54b33cc
27		5117.463171296							2191	908ca278561900d6620da9a8b06ecbaf
27		5117.463171296							2143	950bf3517b1e7f23bc40066853a23f7e
27		5117.463171296							2147	b67f7aa40af6651ce07e39f6b522e96d
27		5117.463171296							2636	bb54c12582d7d1793fb860ae27fe9daa
27		5117.463171296							2064	c7dbb1ce10ff3dfe7c0a485d904d0d23
	file://E:\Testingfiles\002021.pdf	5117.463611111						0	753418	d076bb50e1724b39f86b04111a75f624
675	file://E:\Testingfiles\002098.jpg	5117.463726852						0	115561	b417b165ff13812b4d7a2c35a71ca88f

Εικόνα 7-8:Περιεχόμενα του Resourse_attr

Note_attr

Στο table αυτό ανακαλύπτουμε όλα τις σημειώσεις που δημιουργήσαμε στον λογαριασμό μας. Για την ακρίβεια βρίσκουμε τον τίτλο που δώσαμε σε κάθε σημείωση.

	title	au	last_edited_by	notebook	notebook_uid	t	date_created
196	this is an importan document			georgesmeros's	194		735117.456041667
198	Getting Started			georgesmeros's	194		735107.407488426
209	txt file			georgesmeros's	194		735117.463414352
211	pdf file			georgesmeros's	194		735117.463576389
215	image			georgesmeros's	194		735117.463703704

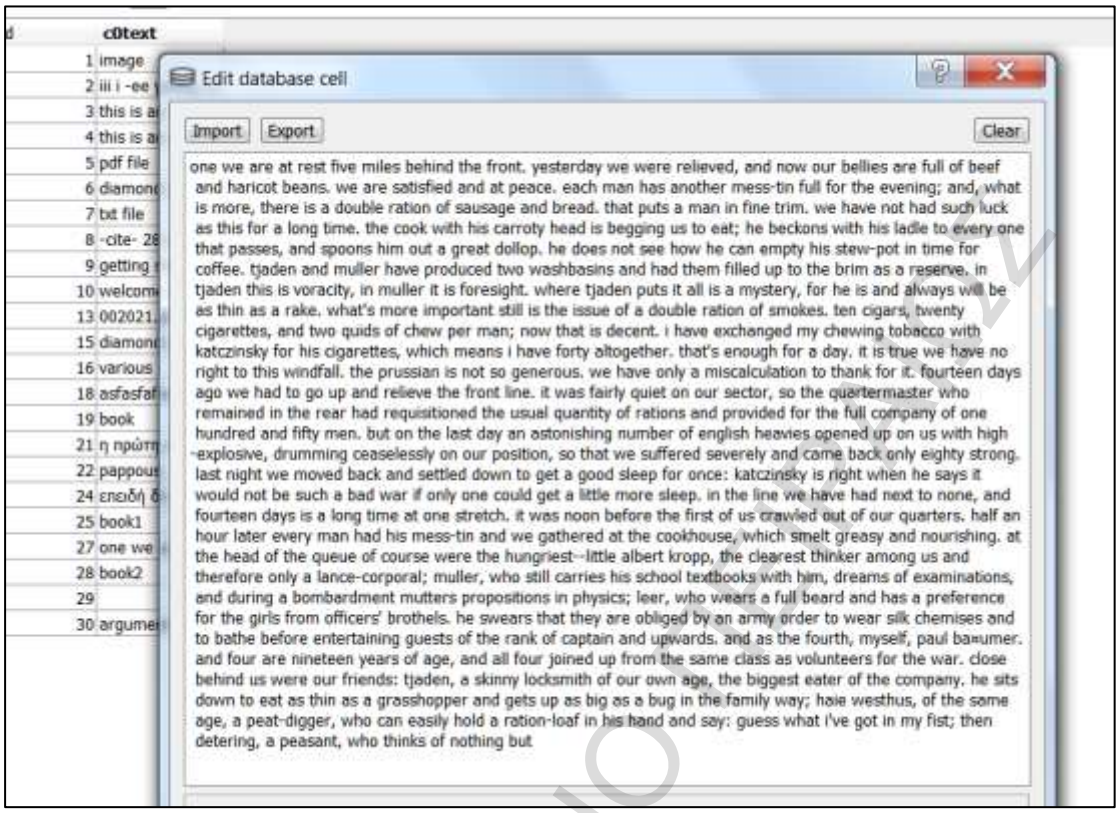
Εικόνα 7-9: Περιεχόμενα του Note_attr

Fts_content

Μέχρις στιγμής ανακαλύψαμε τα αρχεία που επισυνάψαμε και τις σημειώσεις που δημιουργήσαμε. Επομένως στόχος είναι να βρούμε το περιεχόμενο τους. Πλοηγούμαστε στο table Fts_content. Εκεί κάνοντας διπλό click' σε κάθε καταχώρηση ανοίγουμε ένα καινούργιο παράθυρο με το περιεχόμενο της κάθε σημείωσης.

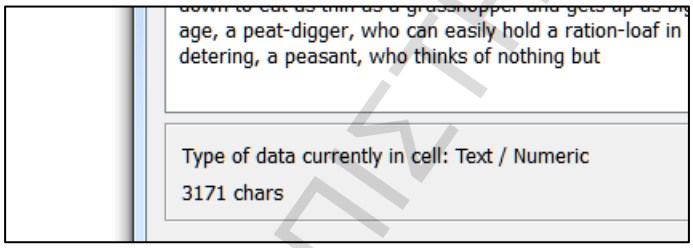
cid	c0text
1	image
2	iii i -ee young sir
3	this is an importa
4	this is an importa
5	pdf file
6	diamond sawblac
7	txt file
8	-cite- 28 usc cha
9	getting started
10	welcome to ever
13	002021.pdf
15	diamond sawblac
16	various
18	asfasfafasfasfa a
19	book
21	η πρώτη σκέψη τ
22	pappous
24	επειδή δν είμαι σ
25	book1
27	one we are at re
28	book2
29	
30	arguments are a

Εικόνα 7-10: Περιεχόμενα του Fts_content



Εικόνα 7-11: Ανακάλυψη των περιεχομένων των σημειώσεων

Στο παράθυρο αυτό μπορούμε να βρούμε και τον αριθμό των λέξεων της κάθε σημειώσεως.

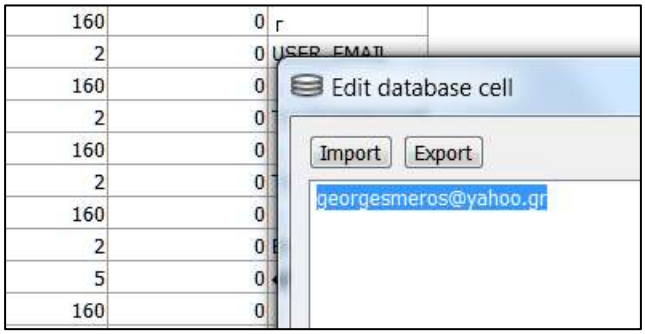


Εικόνα 7-12: Ανακάλυψη του αριθμού των λέξεων των σημειώσεων

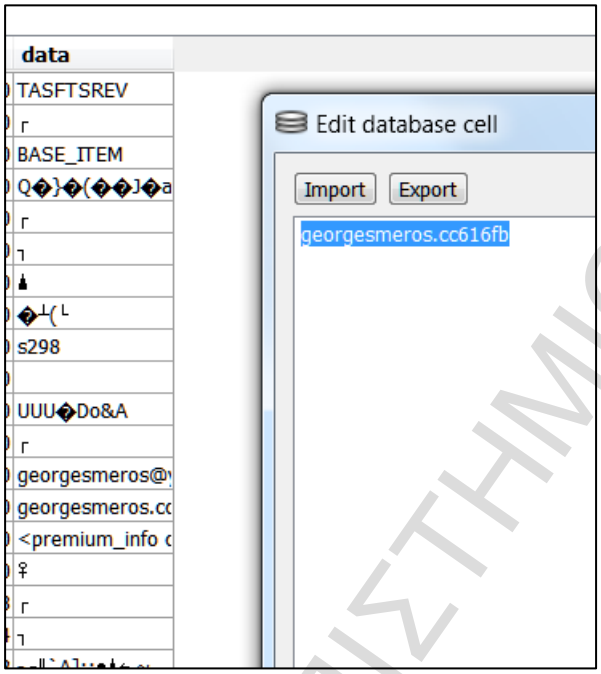
Τα περιεχόμενα των κελιών αυτών ταυτίζονται με τα περιεχόμενα των σημειώσεων που δημιουργήσαμε. Αξίζει να επισημάνουμε ότι δεν μπορέσαμε να ανακαλύψουμε κάποια περαιτέρω πληροφορία για την εικόνα που χρησιμοποιήσαμε στην έρευνα μας.

Atttrs

Στο table αυτό ανακαλύψαμε την διεύθυνση ηλεκτρονικού ταχυδρομείου με την οποία σχετίζεται ο λογαριασμός αυτός καθώς επίσης και την ηλεκτρονική διεύθυνση Evernote.



Εικόνα 7-13:Ανακάλυψη του email του χρήστη



Εικόνα 7-14: Ανακάλυψη της ηλεκτρονικής διεύθυνσης Evernote

Συνοψίζοντας, στον πίνακα που ακολουθεί παραθέτουμε τα ευρήματα μας από την ανάλυση των αρχείων του Evernote.

Πίνακας 7-6: Χρήση του λογισμικού του Evernote

Όνομα αρχείου	Ευρήματα
Αρχεία καταγραφής συμβάντων (Logs)	Πληροφορίες για: ➢ την ενημέρωση της υπηρεσίας ➢ τα αρχεία που συγχρονίστηκαν(ώρα, όνομα αρχείου, id)
Databases ➢ georgesmeros.exb	Πληροφορίες για: ➢ τα αρχεία που επισυνάψαμε (μέγεθος, τιμή κατακερματισμού, προέλευση), ➢ τις σημειώσεις που δημιουργήσαμε ➢ και το περιεχόμενο τους

7.4.4 Εξέταση της μνήμης Ram

Με την χρήση του hexeditor θα εξετάσουμε τα περιεχόμενα της μνήμης RAM. Αρχικά βρίσκουμε πολλές αναφορές στο Evernote, όμως εμείς θέλουμε να βρούμε συγκεκριμένες πληροφορίες που να μας αποκαλύπτουν τις ενέργειες που κάναμε με την εφαρμογή αυτή.

Αρχικά όπως φαίνεται και με την εικόνα που ακολουθεί βρίσκουμε ,όχι μόνο, το όνομα του χρήστη αλλά και την ώρα που έγινε η είσοδος στην υπηρεσία του Evernote.

```
0D 0A 31 34 3A 30 36 3A 31 38 20 5B 32 35 39 36   ..14:06:18 [2596
5D 20 53 65 74 20 74 68 65 20 73 79 6E 63 20 73   ] Set the sync s
65 72 76 69 63 65 20 75 72 6C 20 74 6F 20 22 77   ervice url to "w
77 77 2E 65 76 65 72 6E 6F 74 65 2E 63 6F 6D 22   ww.evernote.com"
0D 0A 31 34 3A 30 36 3A 34 30 20 5B 31 36 32 34   ..14:06:40 [1624
5D 20 30 25 20 41 75 74 68 65 6E 74 69 63 61 74   ] 0% Authenticat
69 6E 67 20 75 73 65 72 20 22 67 65 6F 72 67 65   ing user "george
73 6D 65 72 6F 73 40 79 61 68 6F 6F 2E 67 72 22   smeros@yahoo.gr"
0D 0A 31 34 3A 30 36 3A 34 34 20 5B 32 35 39 36   ..14:06:44 [2596
5D 20 4F 70 65 6E 65 64 20 64 61 74 61 62 61 73   ] Opened databas
```

Εικόνα 7-15: Πληροφορίες σχετικά με την είσοδο του χρήστη

Στην συνέχεια βρίσκουμε κάποιες γεωγραφικές συντεταγμένες. Συγκεκριμένα βρίσκουμε 5 ζευγάρια γεωγραφικού μήκους και πλάτους της μορφής:

Πίνακας 7-7: Δείγμα των συντεταγμένων που ανακτήσαμε

Lat:38°1'58.2816" Long: 23° 47' 22.8942"

```
50 50 52 4F 58 49 4D 41 54 45 3C 2F 6C 6F  >APPROXIMATE</lo
74 69 6F 6E 5F 74 79 70 65 3E 0A 20 20 20  cation_type>.
59 65 77 70 6F 72 74 3E 0A 20 20 20 20 3C  <viewport>.    <
75 74 68 77 65 73 74 3E 0A 20 20 20 20 20  southwest>.
51 74 3E 33 37 2E 39 34 38 38 31 38 31 3C  <lat>37.9488181<
51 74 3E 0A 20 20 20 20 20 3C 6C 6E 67 3E  /lat>.     <lng>
2E 36 38 36 39 38 36 32 3C 2F 6C 6E 67 3E  23.6869862</lng>
20 20 20 3C 2F 73 6F 75 74 68 77 65 73 74  .    </southwest
20 20 20 20 3C 6E 6F 72 74 68 65 61 73 74  >.    <northeast
20 20 20 20 20 3C 6C 61 74 3E 33 38 2E 30  >.     <lat>38.0
38 35 36 33 3C 2F 6C 61 74 3E 0A 20 20 20  328563</lat>.
3C 6C 6E 67 3E 32 33 2E 37 38 39 36 39 32    <lng>23.789692
2F 6C 6E 67 3E 0A 20 20 20 20 3C 2F 6E 6F  5</lng>.    </no
58 65 61 73 74 3E 0A 20 20 20 3C 2F 76 69  rtheast>.   </vi
70 6F 72 74 3E 0A 20 20 20 3C 62 6F 75 6E  ewport>.   <boun
3E 0A 20 20 20 20 3C 73 6F 75 74 68 77 65  ds>.    <southwe
3E 0A 20 20 20 20 20 3C 6C 61 74 3E 33 37  st>.     <lat>37
34 38 38 31 38 31 3C 2F 6C 61 74 3E 0A 20  .9488181</lat>.
20 20 3C 6C 6E 67 3E 32 33 2E 36 38 36 39     <lng>23.6869
32 3C 2F 6C 6E 67 3E 0A 20 20 20 20 3C 2F  862</lng>.    </
75 74 68 77 65 73 74 3E 0A 20 20 20 20 3C  southwest>.    <
72 74 68 65 61 73 74 3E 0A 20 20 20 20 20  northeast>.
51 74 3E 33 38 2E 30 33 32 38 35 36 33 3C  <lat>38.0328563<
51 74 3E 0A 20 20 20 20 20 3C 6C 6E 67 3E  /lat>.     <lng>
2E 37 38 39 36 39 32 35 3C 2F 6C 6E 67 3E  23.7896925</lng>
20 20 20 3C 2F 6E 6F 72 74 68 65 61 73 74  .    </northeast
20 20 20 3C 2F 62 6F 75 6E 64 73 3E 0A 20  >.   </bounds>.
2F 67 65 6F 6D 65 74 72 79 3E 0A 20 3C 2F   </geometry>. </
```

Εικόνα 7-16: Δείγμα των συντεταγμένων που ανακτήσαμε

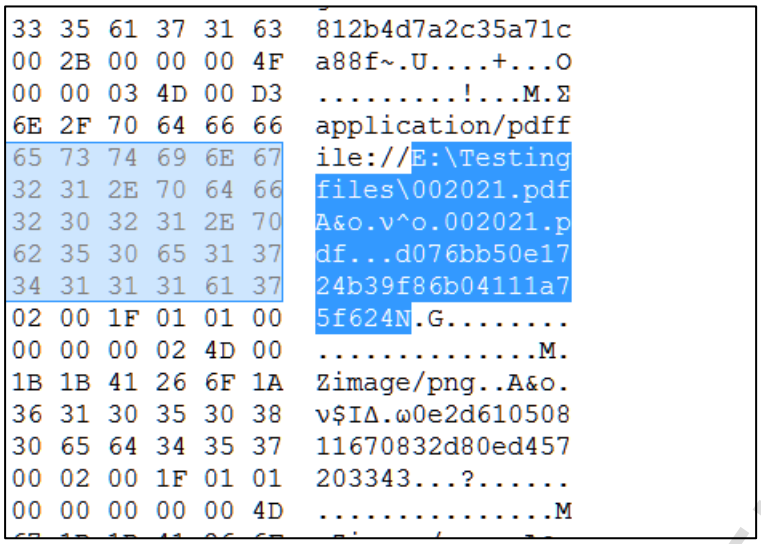
Στην εικόνα που ακολουθεί βλέπουμε τα μέρη στα οποία αντιστοιχούν οι συντεταγμένες αυτές. Το Evernote κατόρθωσε να προσδιορίσει σε αποδεκτά πλαίσια την τοποθεσία που διεξάγεται η έρευνα.

Εικόνα 7-17: Παρουσίαση των συντεταγμένων στον χάρτη

Στην συνέχεια θα χρησιμοποιήσουμε τα ευρήματα μας από τα προηγούμενα στάδια της έρευνας. Αρχικά ψάχνοντας με βάση τις καταλήξεις των αρχείων ανακαλύψαμε όλα τα αρχεία που ανεβάσαμε καθώς και τις αντίστοιχες τιμές κατακερματισμού.

```
                ................
02 00 4F        ....}.Y....!...O
4D 00 D7        .........!...M.X
A3 66 69        image/jpeg.X.ffi
6E 67 66        le://E:\Testingf
70 67 41        iles\002098.jpgA
2E 6A 70        &o.vm›.002098.jp
66 31 33        g.fib417b165ff13
37 31 63        812b4d7a2c35a71c
00 00 4F        a88f~.U....+...O
4D 00 D3        .........!...M.Σ
```

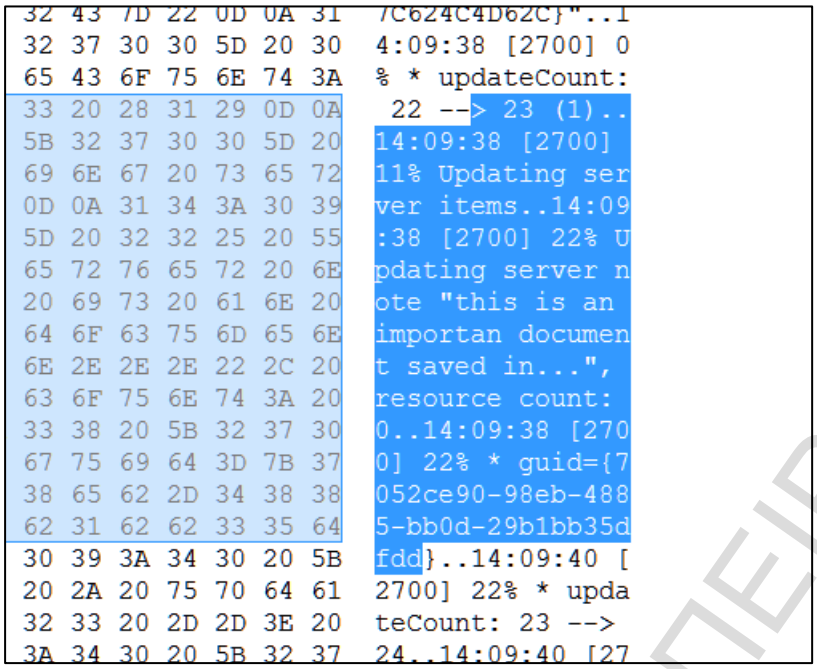
Εικόνα 7-18: Όνομα και διεύθυνση του αρχείου που διακινήσαμε



Εικόνα 7-19: Όνομα και τιμή κατακερματισμού του αρχείου που διακινήσαμε

Αξίζει να σημειώσουμε ότι δεν βρήκαμε καμία αναφορά στο αρχείο 002052.txt αλλά ούτε και στο τιμή κατακερματισμού του. Τέλος ψάχνοντας στην μνήμη RAM με βάση τους κωδικούς κατακερματισμού των αρχείων που ανεβάσαμε καταφέραμε επιτυχώς να τα ανακαλύψουμε ξανά.

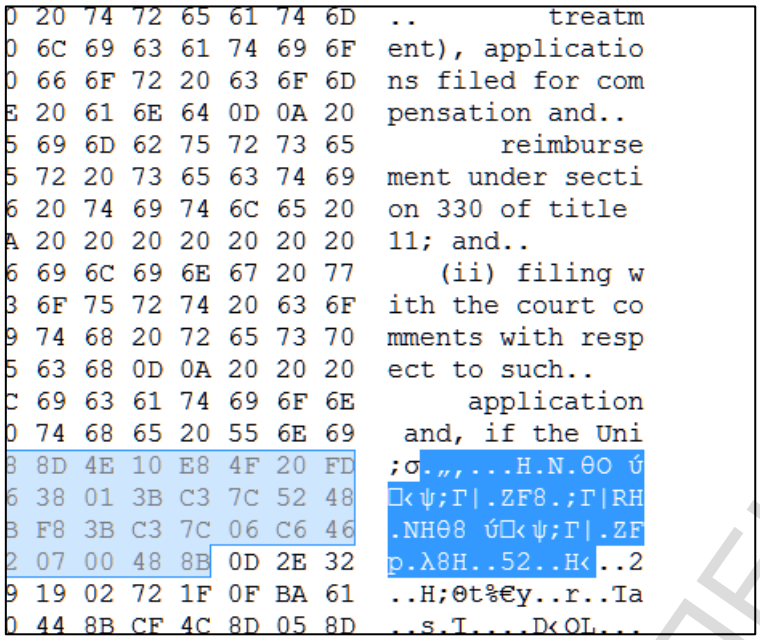
Στο υποκεφάλαιο αυτό θα χρησιμοποιήσουμε τα id που ανακαλύψαμε στο υποκεφάλαιο 7.4.1 . Με την χρήση των id των σημειώσεων που δημιουργήσαμε καταφέραμε επιτυχώς να ανακαλύψουμε στην μνήμη RAM τα logs από τον συγχρονισμό του Evernote με τον εξυπηρετητή της εφαρμογής.



Εικόνα 7-20: Εύρεση των αρχείων log στην μνήμη RAM

Παρατηρούμε ότι πρόκειται για τις ίδιες καταχωρίσεις που βρήκαμε και στα αρχεία καταγραφής συμβάντων της εφαρμογής.

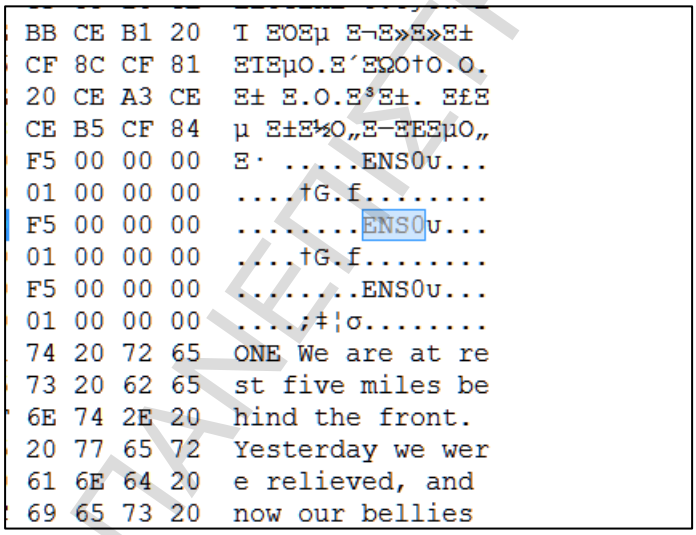
Στο επόμενο στάδιο της έρευνας μας θα επιχειρήσουμε να ανακαλύψουμε το περιεχόμενο των «notes». Αρχικά θα επικεντρωθούμε στο αρχείο 002052.txt.Ψάχνοντας στην μνήμη RAM όντως βρίσκουμε τα περιεχόμενα του ωστόσο η ροή του κειμένου διακόπτεται από διάφορα «σκουπίδια». Έτσι η διαδικασία ανάκτησης του αρχείου 002052.txt είναι επίπονη και χρονοβόρα αλλά εφικτή.



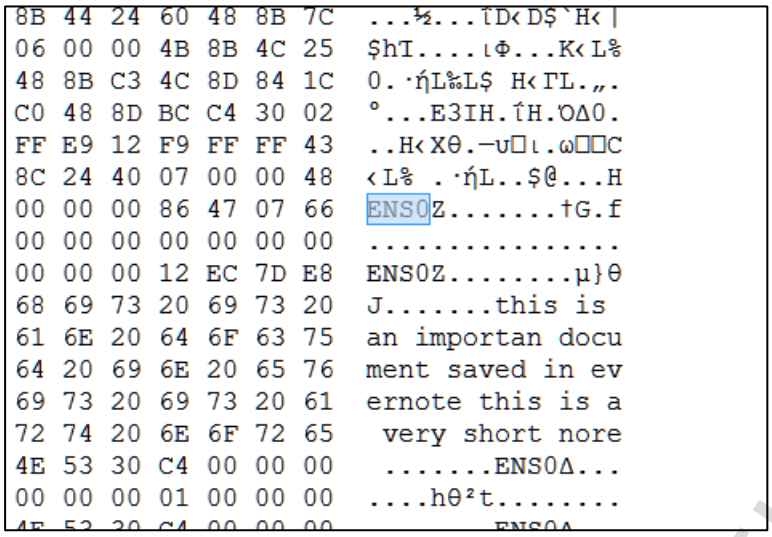
Εικόνα 7-21: Απόσπασμα του περιεχομένου του αρχείου 002052.txt

Το ίδιο ισχύει και για το αρχείο 002021.pdf.

Έπειτα θα επικεντρωθούμε στην ανακάλυψη των απλών σημειώσεων που δημιουργήσαμε. Παρατηρούμε ότι αν ψάξουμε εξονυχιστικά την μνήμη μπορούμε να βρούμε τα περιεχόμενα όλων των σημειώσεων .Ωστόσο για να αυτοματοποιήσουμε την διαδικασία θα προσπαθήσουμε να διακρίνουμε κάποιο κοινό μοτίβο ή στοιχείο. Πράγματι αν παρατηρήσουμε θα ανακαλύψουμε ότι όλα αρχίζουν και τελειώνουν με την λέξη *ENS0*.



Εικόνα 7-22: Εύρεση ενός μοτίβου για την ευκολότερη ανακάλυψη των σημειώσεων(1)



Εικόνα 7-23: Εύρεση ενός μοτίβου για την ευκολότερη ανακάλυψη των σημειώσεων(2)

Τέλος ανακαλύψαμε ότι οι σημειώσεις που είναι στα ελληνικά είναι σε μη αναγνώσιμη μορφή.

Συνοψίζοντας, ερευνώντας την μνήμη RAM καταφέραμε να ανακαλύψουμε τις εξής πληροφορίες:

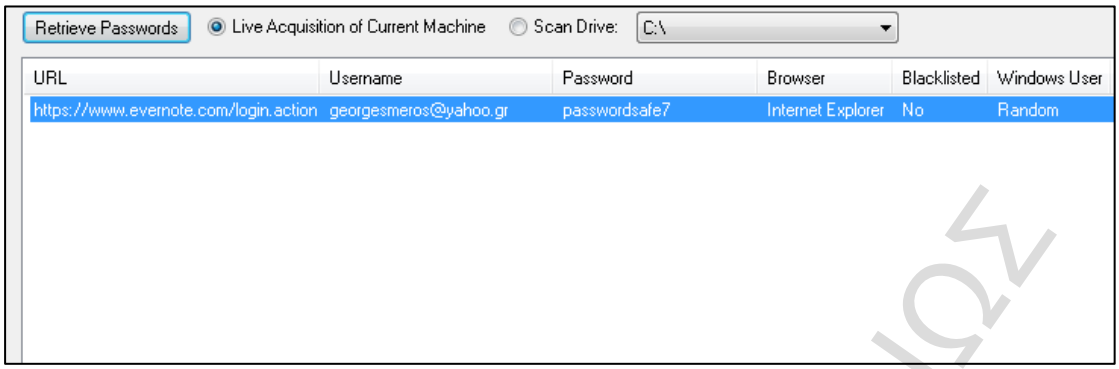
- Τα αρχεία καταγραφής του συγχρονισμού της υπηρεσίας
- Τα αρχεία που επισυνάψαμε στις σημειώσεις (εκτός από το αρχείο .txt).
- Τα περιεχόμενα των πρωτοαναφερθέντων αρχείων
- Γεωγραφικές συντεταγμένες που προσδιορίζουν επαρκώς την τοποθεσία πρόσβασης.
- Τα περιεχόμενα των σημειώσεων.
- Να ανακαλύψουμε ένα μοτίβο ώστε να διευκολύνουμε την διαδικασία ανεύρεσης σημειώσεων.

7.5. Πρόσβαση στην εφαρμογή μέσω περιηγητή

Το επόμενο βήμα στην έρευνα μας είναι να εξετάσουμε τα αποδεικτικά στοιχεία που δημιουργούνται από την πρόσβαση στο Evernote μέσω ενός περιηγητή .Για να το πετύχουμε αυτό θα ακολουθήσουμε την μεθοδολογία που δημιουργήσαμε στο κεφάλαιο 6. Να επισημάνουμε ότι καθώς πρόκειται για μια εφαρμογή για την δημιουργία σημειώσεων στα πλαίσια της έρευνας μας, πέραν της διακίνησης αρχείων, είτε δημιουργήσαμε καινούργιες σημειώσεις είτε απλώς επεξεργαστήκαμε τις ήδη υπάρχοντες.

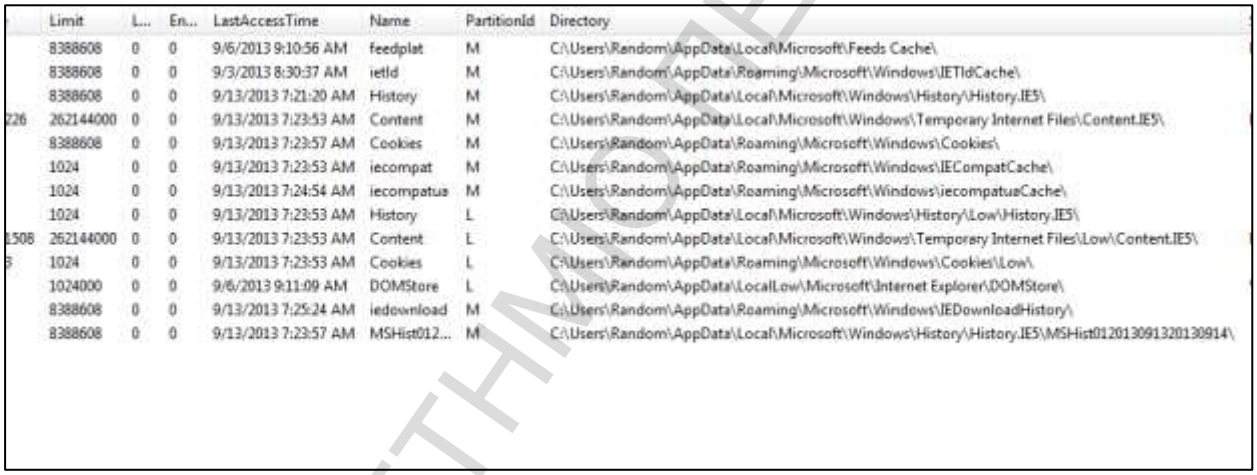
7.5.1 Χρήση του Internet Explorer

Στο υποκεφάλαιο αυτό θα χρησιμοποιήσουμε ένα Vm με εγκατεστημένο τον Internet Explorer. Αρχικά με την χρήση του OSForensics ανακαλύπτουμε και το όνομα χρήστη αλλά και τον κωδικό πρόσβασης στην εφαρμογή Evernote.



Εικόνα 7-24: Εύρεση του ονόματος χρήστη και του συνθηματικού

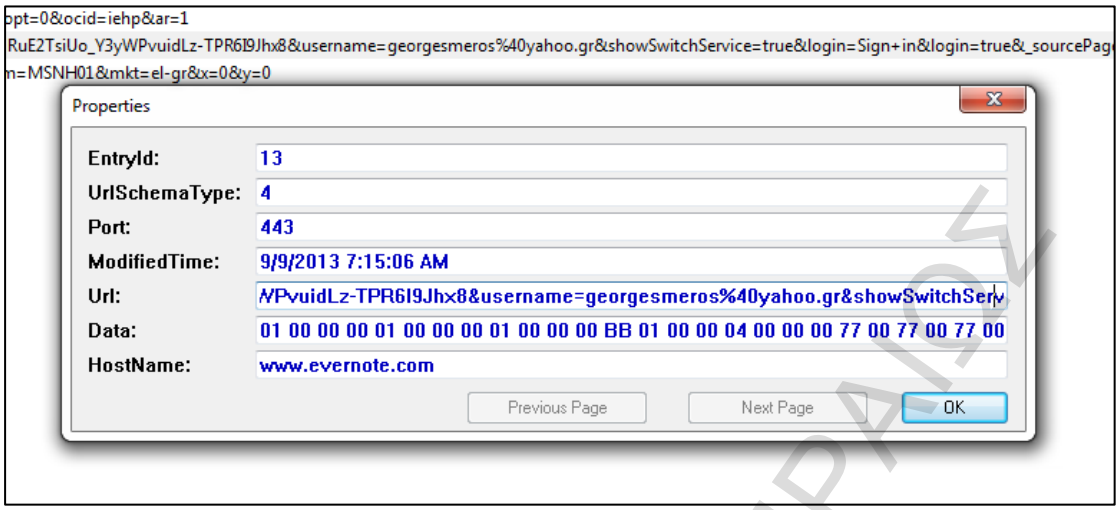
Στην συνέχεια θα εξετάσουμε τις SQL βάσεις δεδομένων του Internet Explorer. Ακολουθώντας την μεθοδολογία που έχουμε προσδιορίσει στο υποκεφάλαιο ,αποκτούμε μια συνολική εικόνα των αρχείων που πρέπει να εξετάσουμε.



Εικόνα 7-25: Συνοπτική παρουσίαση των βάσεων δεδομένων που θα εξετάσουμε

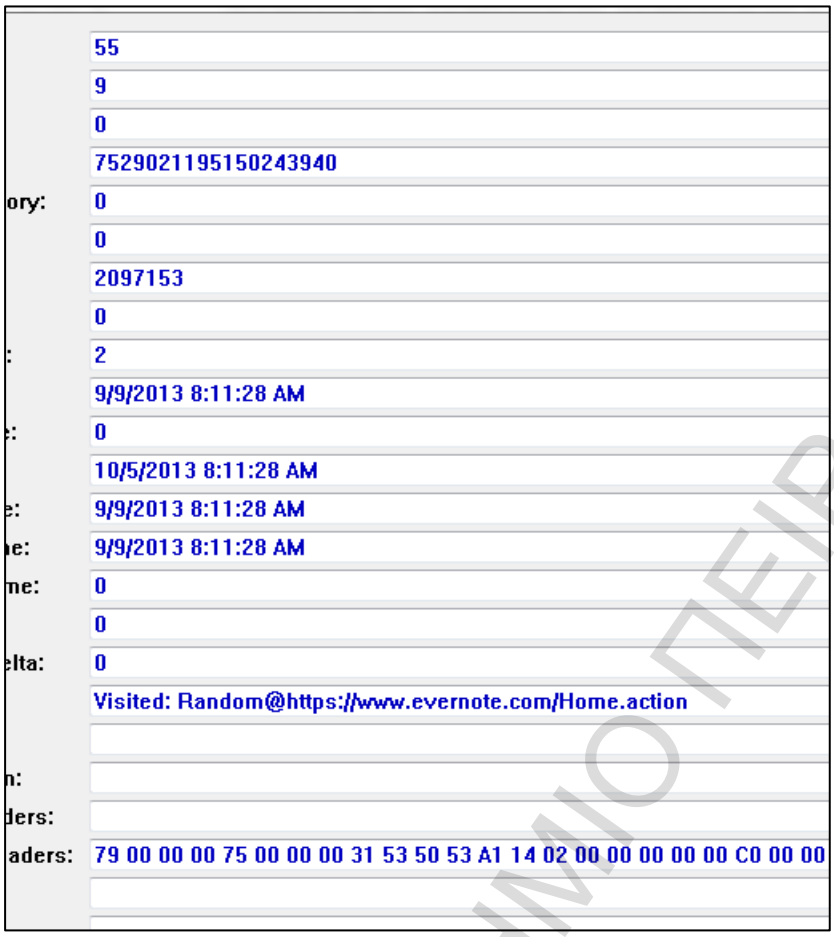
COOKIES

Αρχικά θα εξετάσουμε τα Cookies. Όπως φαίνεται από την εικόνα που ακολουθεί καταφέραμε να ανακαλύψουμε το Cookie που δημιουργείται από την είσοδο μας στην υπηρεσία αυτή.



Εικόνα 7-26: Cookie από την επίσκεψη μας στο ιστότοπο Evernote

Επίσης εξετάζοντας το Ιστορικό του περιηγητή καταφέραμε να επιβεβαιώσουμε ότι όντως επισκεφθήκαμε την ιστοσελίδα του Evernote.

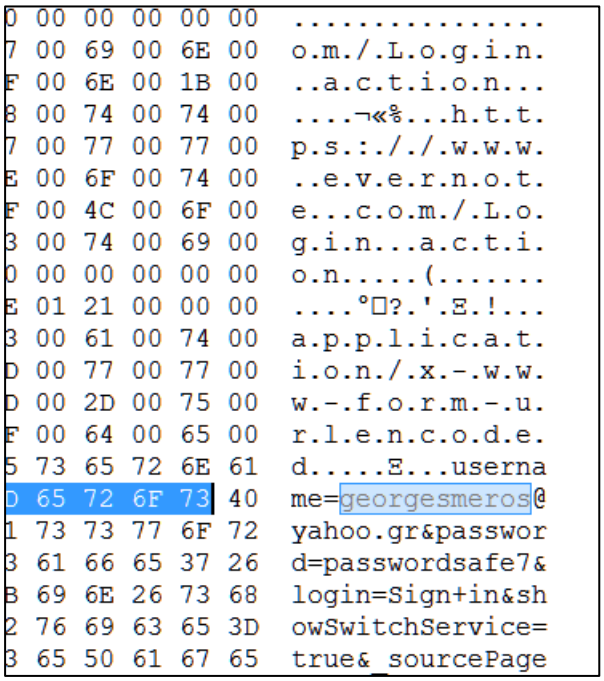


Εικόνα 7-27: Δείγμα από το Ιστορικό του Internet Explorer

Συνοψίζοντας με την εξέταση του περιηγητή Internet Explorer καταφέραμε να ανακαλύψουμε στοιχεία που υποδηλώνουν την χρήση του Evernote. Ανάμεσα σε αυτά τα στοιχεία βρίσκονται το όνομα χρήστη και το συνθηματικό για την πρόσβαση στην υπηρεσία αυτή. Ωστόσο δεν καταφέραμε να ανακαλύψουμε κάτι σχετικό με την διακίνηση των αρχείων που κάναμε.

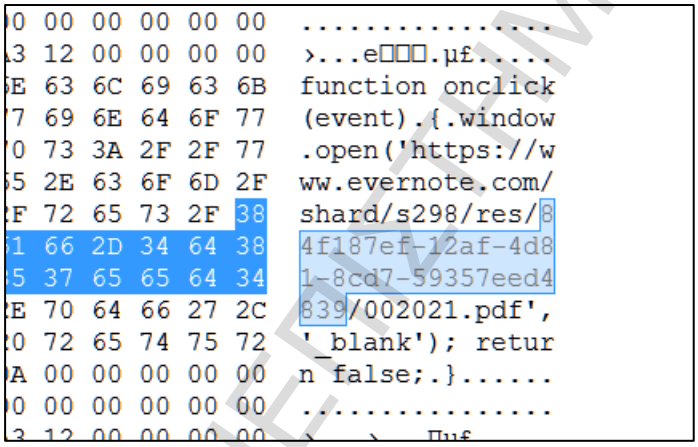
Ram

Στην μνήμη RAM μπορούμε εύκολα να βρούμε το όνομα χρήστη και το συνθηματικό για την πρόσβαση στο Evernote.



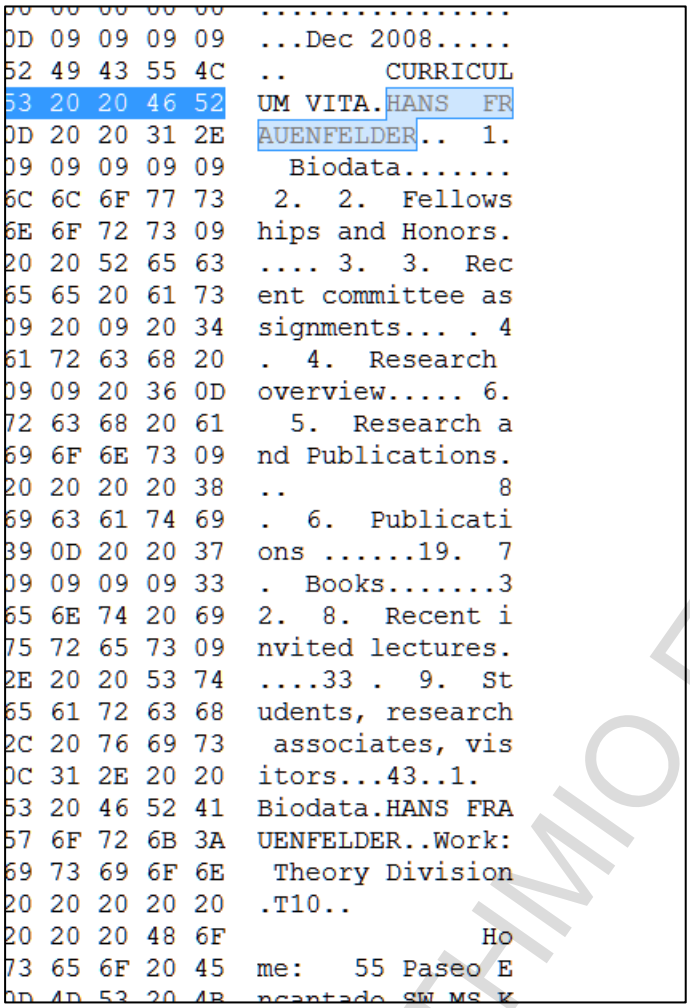
Εικόνα 7-28: Εύρεση του ονόματος του χρήστη και του συνθηματικού

Στην συνέχεια βρίσκουμε στην μνήμη το όνομα του αρχείο που «κατεβάσαμε». Να τονίσουμε ότι πέραν από το όνομα του αρχείου καταφέραμε να ανακαλύψουμε και το recourse id που είχε.



Εικόνα 7-29: Εύρεση του αρχείου που διακινήσαμε

Στο σενάριο όπου «ανεβάσαμε» μέσω του Evernote ένα αρχείο καταφέραμε να ανακαλύψουμε τόσο τα περιεχόμενα του αρχείου αυτού στην μνήμη όσο και το όνομα του αρχείου .



Εικόνα 7-30: Εύρεση των περιεχομένων του αρχείου που διακινήσαμε

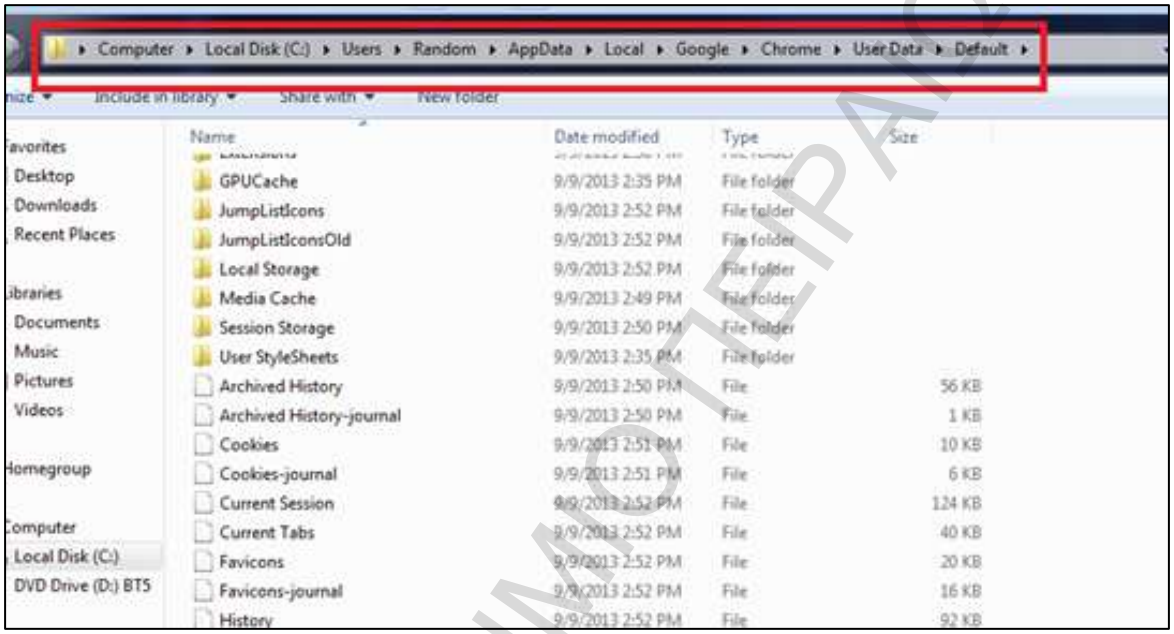
Συνοψίζοντας, μετά την χρήση του Internet Explorer, καταφέραμε να ανακαλύψουμε τα εξής

- πληροφορίες σχετικά με τον λογαριασμό του χρήστη,
- τις ημερομηνίες πρόσβασης στην υπηρεσία,
- τα αρχεία που μετέφερε (στην μνήμη RAM)
- το περιεχόμενο των αρχείων στην περίπτωση που «ανέβασε» τα αρχεία στο
- Evernote(μνήμη RAM)

7.5.2 Χρήση του Google Chrome

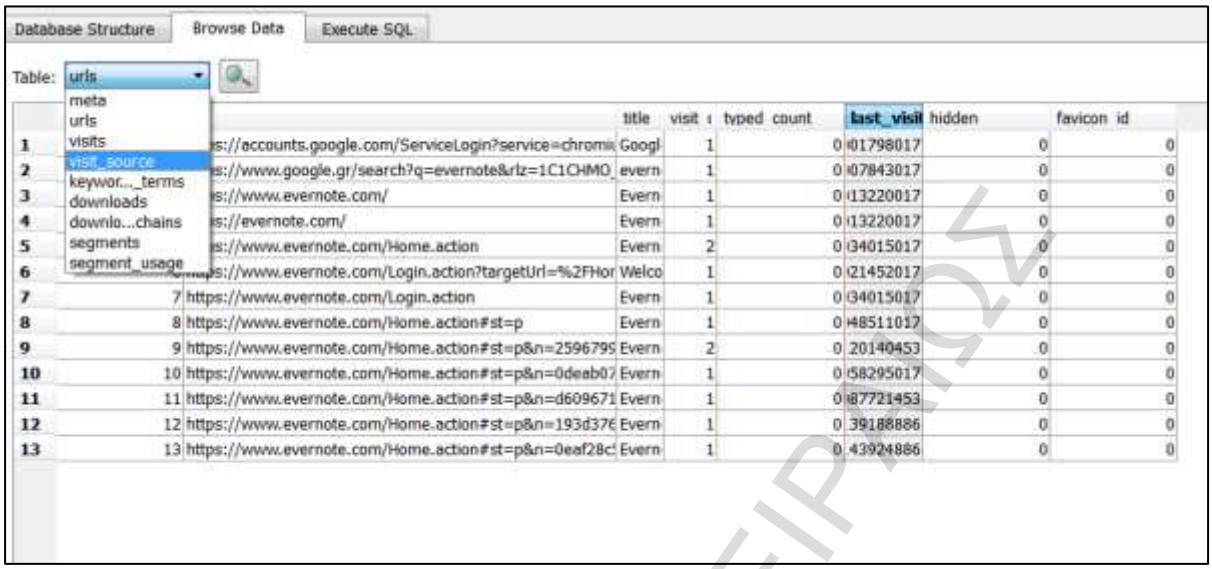
Χρησιμοποιώντας το OSForensics δεν καταφέρνουμε να ανακαλύψουμε το όνομα χρήστη ή το συνθηματικό του λογαριασμού.

Στην συνέχεια, σύμφωνα με το υποκεφάλαιο 6.11.2,πλοηγούμαστε στην τοποθεσία *C:\Users\Random\ AppData\Local\Google\Chrome\Random\Default.* Εδώ θα εξετάσουμε τις SQL βάσεις δεδομένων του περιηγητή.



Εικόνα 7-31: Παρουσίαση των, προς εξέτασιν, αρχείων

Ακολουθώντας την μεθοδολογία που προσδιορίσαμε στο υποκεφάλαιο ,με την χρήση του SQLite Database Browser εξετάζουμε τα περιεχόμενα των αρχείων αυτών. Στο αρχείο 'History' βρίσκουμε πληροφορίες όχι μόνο για τα τις διευθύνσεις που επισκεφθήκαμε αλλά και για τυχόν αρχεία που «κατεβάσαμε».

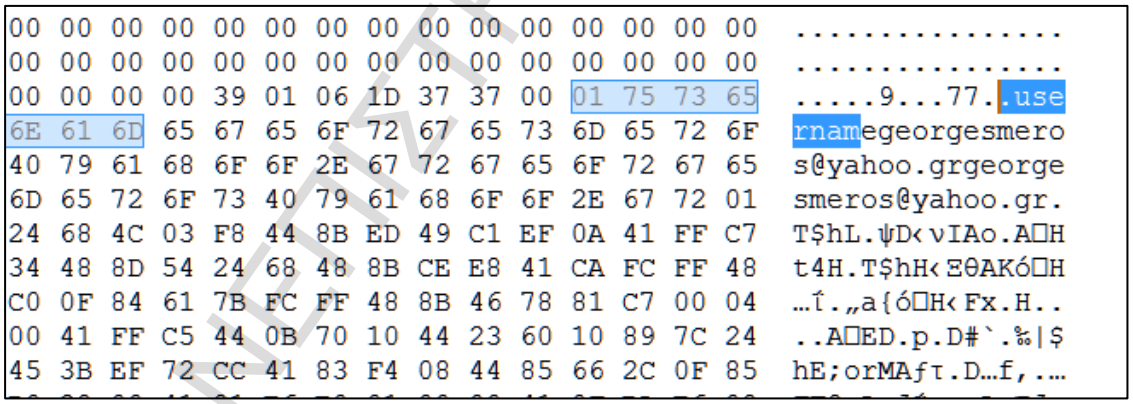


Εικόνα 7-32: Ανακάλυψη των διευθύνσεων

Έτσι καταφέραμε να ανακαλύψουμε με επιτυχία τα αρχεία που «κατεβάσαμε». Στην συνέχεια εξετάζοντας τα αρχεία Cookies και Logins βρίσκουμε δεδομένα που αποδεικνύουν ότι όντως χρησιμοποιήσαμε τον Chrome για να αποκτήσουμε πρόσβαση στην εφαρμογή Evernote. Τέλος δεν μπορέσαμε να βρούμε κάποια άλλη πληροφορία που να αποκαλύπτει τις ενέργειες που κάναμε.

RAM

Εξετάζοντας την μνήμη RAM καταφέραμε να ανακαλύψουμε το όνομα χρήστη που χρησιμοποιήσαμε για την πρόσβαση στην εφαρμογή



Εικόνα 7-33: Ανακάλυψη του ονόματος χρήστη

Επίσης καταφέραμε να ανακαλύψουμε τα αρχεία που «ανεβάσαμε» και «κατεβάσαμε».

Συνοψίζοντας, όπως και στον Internet Explorer, βρήκαμε πληροφορίες σχετικά με τα αρχεία που διακινήσαμε αλλά τίποτα που να σχετίζεται με τις σημειώσεις που δημιουργήσαμε.

7.6. Διαγραφή αρχείων

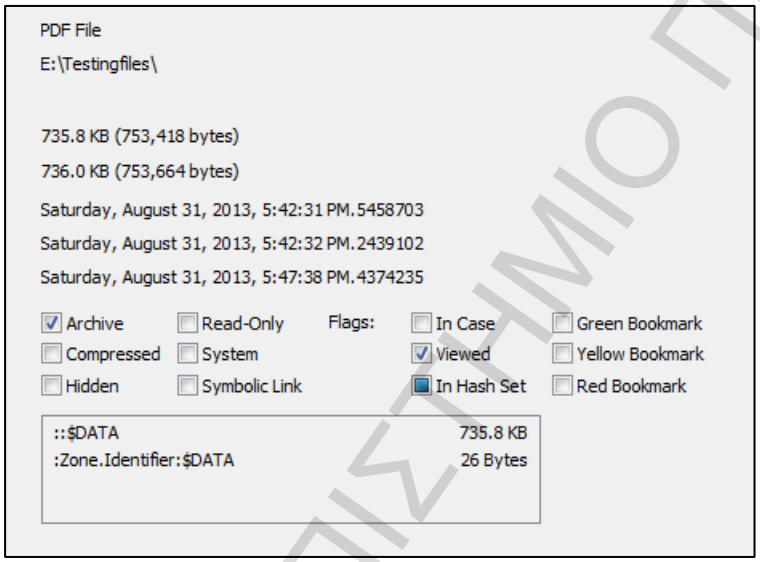
Όταν διαγράφουμε ένα «note»-είτε μέσω του λογισμικού της εφαρμογής, είτε μέσω ενός περιηγητή-το «note» αποθηκεύεται προσωρινά στον φάκελο 'Trash'.Όσο παραμένει στον φάκελο αυτόν, είναι δυνατή η εύρεση του στην SQL βάση δεδομένων της εφαρμογής. Όταν διαγράψουμε την σημείωση και από τον φάκελο 'Trash' τότε χάνουμε κάθε δυνατότητα ανάκτησης κάποιας πληροφορίας για αυτό.

7.7. Μεταδεδομένα αρχείων

Στα πλαίσια της έρευνας μας εξετάσαμε αν η μετακίνηση των αρχείων μέσω της εφαρμογής του Evernote επιφέρει αλλαγές στις ιδιότητες τους. Η μετακίνηση των αρχείων («ανέβασμα»,«κατέβασμα») επιφέρει αλλαγές στις ιδιότητες

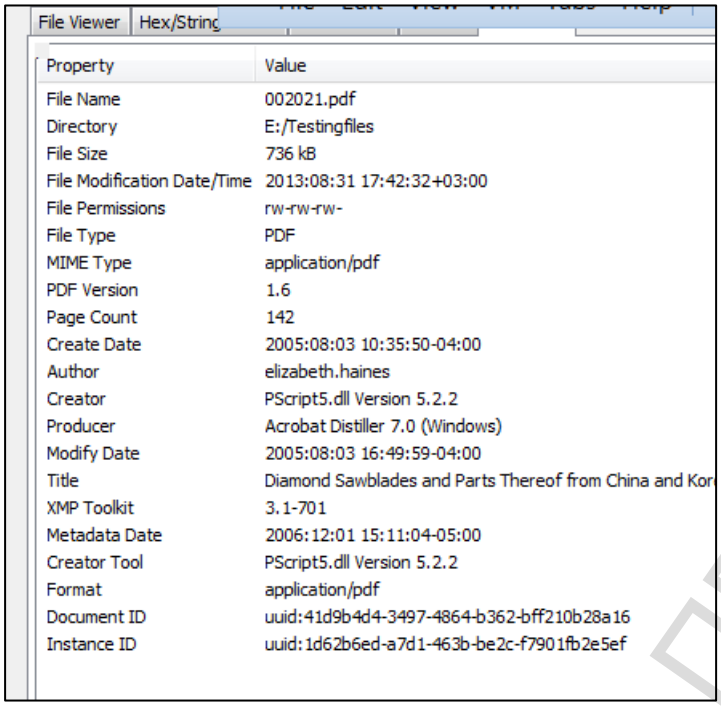
- Date created
- Date accessed
- Date modified

Συγκεκριμένα οι ιδιότητες αυτές των αρχείων παίρνουν την τιμή της ημερομηνίας που «κατέβηκαν» στον υπολογιστή.



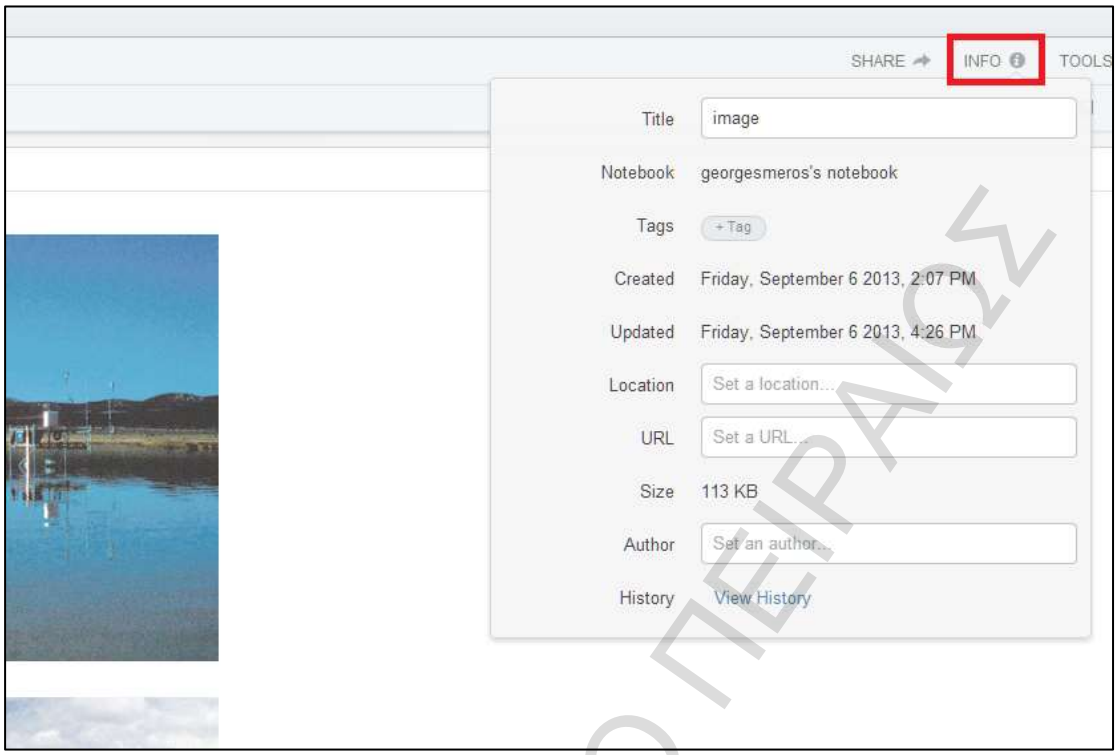
Εικόνα 7-34: Αλλαγή των ημερομηνιών του αρχείου

Τα αρχεία διατήρησαν αναλλοίωτα τις τιμές κατακερματισμού τους αφού δεν επιχειρήσαμε κάποια αλλαγή στο περιεχόμενο τους. Τέλος οποιαδήποτε άλλη πληροφορία έχει το αρχείο-Author,Creator,κ.α- παραμένει και αυτή αναλλοίωτη.



Εικόνα 7-35: Μεταδεδομένα του αρχείου

Τέλος εξετάζοντας, είτε μέσω του λογισμικού της εφαρμογής είτε μέσω κάποιου περιηγητή, τις σημειώσεις που έχουμε δημιουργήσει μπορούμε να ανακαλύψουμε την ημερομηνία δημιουργίας τους και της πιο πρόσφατης επεξεργασίας τους.



Εικόνα 7-36: Πληροφοριών των σημειώσεων

7.8. Απεγκατάσταση Evernote

Τέλος αναλύσαμε την συμπεριφορά του Evernote κατά την διαδικασία της απεγκατάστασης του.Στο πρώτο σενάριο απεγκαταστήσαμε το πρόγραμμα μέσω του Πίνακα Ελέγχου του λειτουργικού συστήματος. Με τον τρόπο αυτό βρήκαμε πληθώρα αναφορών του προγράμματος Evernote στην Registry των Windows ενώ και ο φάκελος "Evernote" παρέμεινε ανέπαφος.

Στο δεύτερο σενάριο για την απεγκατάσταση του Evernote χρησιμοποιήσαμε το πρόγραμμα CC Cleaner. Αφού απεγκαταστήσαμε το Evernote χρησιμοποιήσαμε την επιλογή του Registry Scan για να αφαιρέσουμε τυχόν εναπομείναντες αναφορές στο Evernote από την Registry των Windows .Σε αυτό το σενάριο βρήκαμε λιγότερες αναφορές στο Evernote στην Registry ωστόσο ο φάκελος "Evernote" παρέμεινε ανέπαφος.

Πίνακας 7-8: Αναφορές στην Registry

HKEY_USERS\S-1-5-21-2531412380-2784069389-2677724388-1000\Software\Evernote\Evernote3,"1/1/1601, 3:00 HKEY_USERS\S-1-5-21-2531412380-2784069389-2677724388-1000\Software\Evernote\Evernote5,"1/1/1601, 3:00

Τέλος στο τρίτο σενάριο συνδυάσαμε το CC Cleaner με το Eraser.Καταφέραμε και σβήσαμε εντελώς τον φάκελο 'Evernote' ωστόσο συνέχισαν να υπάρχουν εναπομείναντες αναφορές στο 'Evernote' στην Registry των Windows.

Πίνακας 7-9: Αναφορές στην Registry μετά την χρήση του CC CLeaner

HKEY_CURRENT_USER\Software\Eraser,"1/1/1601, 3:00 HKEY_CURRENT_USER\Software\Evernote,"1/1/1601, 3:00

Συνοψίζοντας μετά την απεγκατάσταση του Evernote μπορούμε με ασφάλεια να υποστηρίξουμε ότι ο ερευνητής μπορεί να ανακαλύψει δεδομένα που αποδεικνύουν την χρήση του-στην χειρότερη περίπτωση- και στην καλύτερη να ανακαλύψει και τα ίδια τα αρχεία του Evernote.

Πίνακας 7-10: Απεγκατάσταση Evernote

Σενάριο	Ευρήματα
Σενάριο 1: Απλή απεγκατάσταση	Αναφορές στην Registry Άθικτος ο φάκελος ΄Evernote΄
Σενάριο 2:Χρήση CC Cleaner	Αναφορές στην Registry(λιγότερες από το σενάριο 1) Άθικτος ο φάκελος ΄Evernote΄
Σενάριο 3:Χρήση CC cleaner και Eraser	Αναφορές στην Registry

7.9. Παρουσίαση

Ανακεφαλαιώνοντας, εξετάσαμε το Evernote για να προσδιορίσουμε τα ψηφιακά δεδομένα που δημιουργούνται από την χρήση του. Με βάση την έρευνα που κάναμε ανακαλύψαμε ότι ο ερευνητής μπορεί εύκολα να προσδιορίσει αν έχει χρησιμοποιηθεί η υπηρεσία αυτή. Ακόμα και αν έχει απεγκατασταθεί υπάρχουν υπολείμματα στο λειτουργικό σύστημα του υπολογιστή(Registry) ενώ και τα αρχεία που εγκαθιστά πρέπει να αφαιρεθούν χειροκίνητα.

Επίσης εξετάσαμε τα προαναφερθέντα αρχεία. Καταφέραμε να προσδιορίσουμε όλες τις δραστηριότητες που έκανε ο χρήστης:

- συγχρονισμός λογαριασμού,
- επισύναψη αρχείων (καθώς και τα metadata τους)
- συγγραφή σημειώσεων.
- Περιεχόμενο των σημειώσεων και επισυνημμένων αρχείων

Ακόμα, εξετάζοντας την μνήμη RAM καταφέραμε επιπροσθέτως να ανακαλύψουμε γεωγραφικές συντεταγμένες που σχετίζονται με την τοποθεσία διεξαγωγής της έρευνας καθώς και να προσδιορίσουμε ένα μοτίβο για τον ευκολότερο εντοπισμό των σημειώσεων.

Τέλος, ερευνήσαμε τα ψηφιακά δεδομένα που παράγονται από την πρόσβαση στο Evernote μέσω κάποιου προγράμματος περιήγησης. Συγκεκριμένα καταφέραμε να ανακαλύψουμε :

- Το όνομα του χρήστη
- Τα αρχεία που διακίνησε
- Ώρα και ημερομηνία που συνδέθηκε στην υπηρεσία

Στον πίνακα που ακολουθεί παρουσιάζονται συνοπτικά τα ευρήματα μας.

Πίνακας 7-11: Αποτελέσματα της δικανικής εξέτασης του Evernote

Υλισμικό	**Ευρήματα**
Διεύθυνση εγκατάστασης Διεύθυνση δεδομένων εφαρμογής	Program Files (x86)\Evernote\ C:\Users\Random\AppData\Local\Evernote\Evernote
Αρχεία προς εξέταση • georgesmeros.exb.snippets • logs • georgesmeros.exb	Πληροφορίες για: • την ενημέρωση της υπηρεσίας • τα αρχεία που συγχρονίστηκαν (ώρα ,όνομα αρχείου, id) • τα αρχεία που επισυνάψαμε (μέγεθος,διεύθυνση προέλευσης, τιμή κατακερματισμού), • τις σημειώσεις που δημιουργήσαμε και το περιεχόμενο τους
RAM	• Γεωγραφικές συντεταγμένες • Όνομα χρήστη και ημερομηνία εισόδου στην υπηρεσία • Όνομα/περιεχόμενο αρχείων που μετακινήθηκαν • Περιεχόμενο των σημειώσεων και αναγνώριση μοτίβου για ευκολότερη ανακάλυψη τους
Απεγκατάσταση	Αναφορές στην Registry Άθικτα τα δεδομένα της εφαρμογής. (χρήση ειδικού προγράμματος για την διαγραφή τους)
Πρόσβαση μέσω Browser	**Ευρήματα**
Εξέταση των αρχείων του περιηγητή	• Όνομα αρχείων που κατεβάσαμε • Ημερομηνία εισόδου • Όνομα/κωδικός χρήστη
RAM	• Όνομα/περιεχόμενο αρχείων που ανεβάσαμε • Όνομα αρχείων που κατεβάσαμε • Όνομα/κωδικός χρήστη
Metadata	**Ευρήματα**
• Date created • Date accessed • Date modified	Οι ιδιότητες αυτές των αρχείων παίρνουν την τιμή της ημερομηνίας που «κατέβηκαν» στον υπολογιστή.
Διαγραφή «Σημειώσεων»	**Ευρήματα**
	Προσωρινή αποθήκευση στον δικτυακό φάκελο ‘Trash’ Διαγραφή από τον φάκελο ‘Trash’ σημαίνει και οριστική διαγραφή της σημειώσεως.

Κεφάλαιο 8: Ψηφιακή Εγκληματολογική Ανάλυση του SpiderOak

8.1. Εισαγωγή

Το SpiderOak είναι ένα online εργαλείο, βασισμένο στην τεχνολογία cloud, που μας επιτρέπει την δημιουργία αντιγράφων ασφαλείας. Η εφαρμογή μέσω της οποίας έχουμε πρόσβαση στην υπηρεσία αυτή είναι διαθέσιμη για Windows, Linux, Android και IOS. Το SpiderOak επιτρέπει στο χρήστη να δημιουργήσει αντίγραφα ασφαλείας κάθε φακέλου του υπολογιστή του.

Το SpiderOak μας παρέχει την δυνατότητα να χρησιμοποιήσουμε την τεχνολογία cloud, διατηρώντας το δικαίωμα της ιδιωτικότητας. Όλα τα αρχεία κρυπτογραφούνται τοπικά στον υπολογιστή , και στη συνέχεια μεταφέρονται στους διακομιστές του SpiderOak .Οι τυχόν αλλαγές που κάνουμε στα αρχεία και τους φακέλους συγχρονίζονται με τις τοπικές αποκρυπτογραφημένες εκδόσεις πριν «μεταφερθούν» στους διακομιστές του SpiderOak.

Το SpideOak, εφαρμόζοντας την πολιτική προστασίας προσωπικών δεδομένων "Zero Knowledge", με την τοπική κρυπτογράφηση των δεδομένων δεν έχει την δυνατότητα να ξέρει τι αποθηκεύουμε. Ταυτόχρονα, όμως πρέπει να επισημάνουμε ότι αν χάσουμε τον κωδικό πρόσβασης δεν μπορούμε να τον ανακτήσουμε είτε αυτόν είτε τα αρχεία που κρυπτογραφήσαμε με αυτόν.

Το πιο σημαντικό, όμως, είναι ότι ποτέ τα κλειδιά δεν αποθηκεύονται με την μορφή απλού κειμένου στον διακομιστή του SpiderOak. Είναι κρυπτογραφημένα με 256 bit AES, χρησιμοποιώντας ένα κλειδί δημιουργημένο από τον αλγόριθμο PBKDF2 (χρησιμοποιώντας sha-256), με 16384 γύρους (rounds), και 32 bytes τυχαίων δεδομένων (salt). Η προσέγγιση αυτή αποτρέπει τις επιθέσεις brute-force και τις επιθέσεις με την χρήση βάσεων δεδομένων συνθηματικών (SpiderOak, 2013).

Το SpiderOak Hive αποτελεί έναν εύκολο τρόπο συγχρονισμού των δεδομένων μεταξύ διαφορετικών συσκευών. Απλά ,μέσω του «drag and drop» των αρχείων στον φάκελο Hive, μπορούμε να μοιραστούμε αρχεία με όλες τις συσκευές που είναι συνδεδεμένες στον λογαριασμό μας (SpiderOak, n.d.).

Το SpiderOak προσφέρει δύο τύπους λογαριασμών, μια δωρεάν έκδοση 2 GB και μια πληρωμένη συνδρομή με αυξημένη χωρητικότητα.

8.2. Σκοπός/Στόχος

Ο σκοπός της παρούσας έρευνας είναι να προσδιορίσουμε τα υπολείμματα δεδομένων σε έναν υπολογιστή με Windows 7 μετά την χρήση του SpiderOak, όπως το όνομα χρήστη, ο κωδικός πρόσβασης, τα αρχεία που αποθηκεύτηκαν στο λογαριασμό, και τα σχετικά με αυτά τα αρχεία metadata. Επίσης στα πλαίσια της έρευνας χρησιμοποιούμε αντιδικανικές διαδικασίες για την σύγκριση της αρχικής και της τελικής κατάστασης του συστήματος.

8.3. Ανάλυση του SpiderOak στο περιβάλλον των Windows 7

8.3.1 Προετοιμασία

Για την συλλογή των δεδομένων που απαιτούνται για να απαντήσουμε στις ερωτήσεις της έρευνας μας δημιουργήσαμε μια εικονική μηχανή. Ακολουθώντας την μεθοδολογία που προσδιορίσαμε στο κεφάλαιο 6 χρησιμοποιήσαμε το SpiderOak για την διακίνηση αρχείων. Συγκεκριμένα «κατεβάσαμε» και «ανεβάσαμε» 4 αρχεία αντίστοιχα. Αξίζει να επισημάνουμε ότι συνδέσαμε τον λογαριασμό μας στο SpiderOak με δυο υπολογιστικά συστήματα(PCno1,PCVM).

Για την προετοιμασία της έρευνας του SpiderOak, εκτός από το λογισμικό που αναλύσαμε στο κεφάλαιο 6, χρησιμοποιήσαμε επίσης:

- SpiderOak version 5.0.3
- Microsoft Word 2010
- Internet explorer 10
- Google Chrome Version 29.0.1547.66
- CCleaner v3.17.1689
- Eraser
- SQLite Database Browser 2.0 b1
- ESEDatabaseView v1.07

Τέλος στα πλαίσια της προετοιμασίας της έρευνας μας έχουμε χρησιμοποιήσει την λειτουργία δημιουργίας υπογραφών του OSFORENSICS πριν και μετά την εγκατάσταση του SpiderOak ώστε να ανακαλύψουμε με ακρίβεια και αποτελεσματικότητα τις αλλαγές που έγιναν στο λειτουργικό σύστημα της εικονικής μηχανής.

8.3.2 Αναγνώριση και Συλλογή

Στο πλαίσιο αυτής της έρευνας, εντοπίστηκαν τα μέσα που περιέχουν τις πληροφορίες που απαιτούνται για τη διεξαγωγή της ανάλυσης. Πρόκειται για την μνήμη RAM της εικονικής μηχανής και τον σκληρό δίσκο του VM. Ακολουθώντας τις διαδικασίες που προσδιορίσαμε στο κεφάλαιο 6,αποκτήσαμε με δικανικά αποδεκτό τρόπο τα περιεχόμενα της μνήμης RAM και του σκληρού δίσκου της προς εξέτασιν εικονικής μηχανής.

8.3.3 Διατήρηση

Για την έρευνα αυτή δημιουργήσαμε ένα δικανικό αντίγραφο των δυο αρχείων που αποκτήσαμε στο στάδιο της συλλογής και της ανάκτησης. Για να το πετύχουμε αυτό χρησιμοποιήσαμε το πρόγραμμα Access Data FTK Imager.

8.3.4 Ανάλυση

Στο στάδιο αυτό χρησιμοποιήσαμε μια σειρά από εργαλεία ,όπως το OSFORENSICS. Αρχικά θέλουμε να προσδιορίσουμε τις αλλαγές που γίνονται στο λειτουργικό των Windows με την εγκατάσταση και την απεγκατάσταση του SpiderOak. Θέλουμε να δούμε αν μπορούμε να ανακαλύψουμε ότι χρησιμοποιήθηκε το πρόγραμμα αυτό ακόμα και αν έχει απεγκατασταθεί από το λειτουργικό σύστημα.

Για αυτό τον λόγο χρησιμοποιούμαι το OSFORENSICS και την επιλογή της δημιουργίας και σύγκρισης υπογραφών. Στον φάκελο '*C:\Program Files\SpiderOak*' είναι εγκατεστημένα τα αρχεία που είναι απαραίτητα για την εκτέλεση της εφαρμογής.

Στον φάκελο '*C:\Users\ Username\AppData\Roaming\SpiderOak*' αποθηκεύονται τα αρχεία Logs καθώς και οι SQL βάσεις δεδομένων της εφαρμογής.

Πίνακας 8-1: Συνοπτική παρουσίαση των προς εξέτασιν αρχείων του SpiderOak

C:\Users\Random\AppData\Roaming\SpiderOak_maintain_branding.flag, C:\Users\Random\AppData\Roaming\SpiderOak_maintain_shortcuts.flag, C:\Users\Random\AppData\Roaming\SpiderOak\backup_system_ignore_this_folder.lock, C:\Users\Random\AppData\Roaming\SpiderOak\config.txt, C:\Users\Random\AppData\Roaming\SpiderOak\dirhash.db, C:\Users\Random\AppData\Roaming\SpiderOak\exclude.txt, C:\Users\Random\AppData\Roaming\SpiderOak\fs_queue.db, C:\Users\Random\AppData\Roaming\SpiderOak\local.dat, C:\Users\Random\AppData\Roaming\SpiderOak\oak_20130910111337.log, 13, C:\Users\Random\AppData\Roaming\SpiderOak\oak_20130910112000.log, C:\Users\Random\AppData\Roaming\SpiderOak\objectdb.fs, C:\Users\Random\AppData\Roaming\SpiderOak\objectdb.fs.index, C:\Users\Random\AppData\Roaming\SpiderOak\objectdb.fs.lock, C:\Users\Random\AppData\Roaming\SpiderOak\objectdb.fs.tmp,

C:\Users\Random\AppData\Roaming\SpiderOak\pandora_sqliite_database, C:\Users\Random\AppData\Roaming\SpiderOak\prefs.dat, C:\Users\Random\AppData\Roaming\SpiderOak\shell_extension_log.txt, C:\Users\Random\AppData\Roaming\SpiderOak\snapshot.db, C:\Users\Random\AppData\Roaming\SpiderOak\spider_20130910111337.log, C:\Users\Random\AppData\Roaming\SpiderOak\spider_20130910112001.log,

Η εγκατάσταση του προγράμματος επιφέρει αλλαγές και στην Registry του λειτουργικού συστήματος.

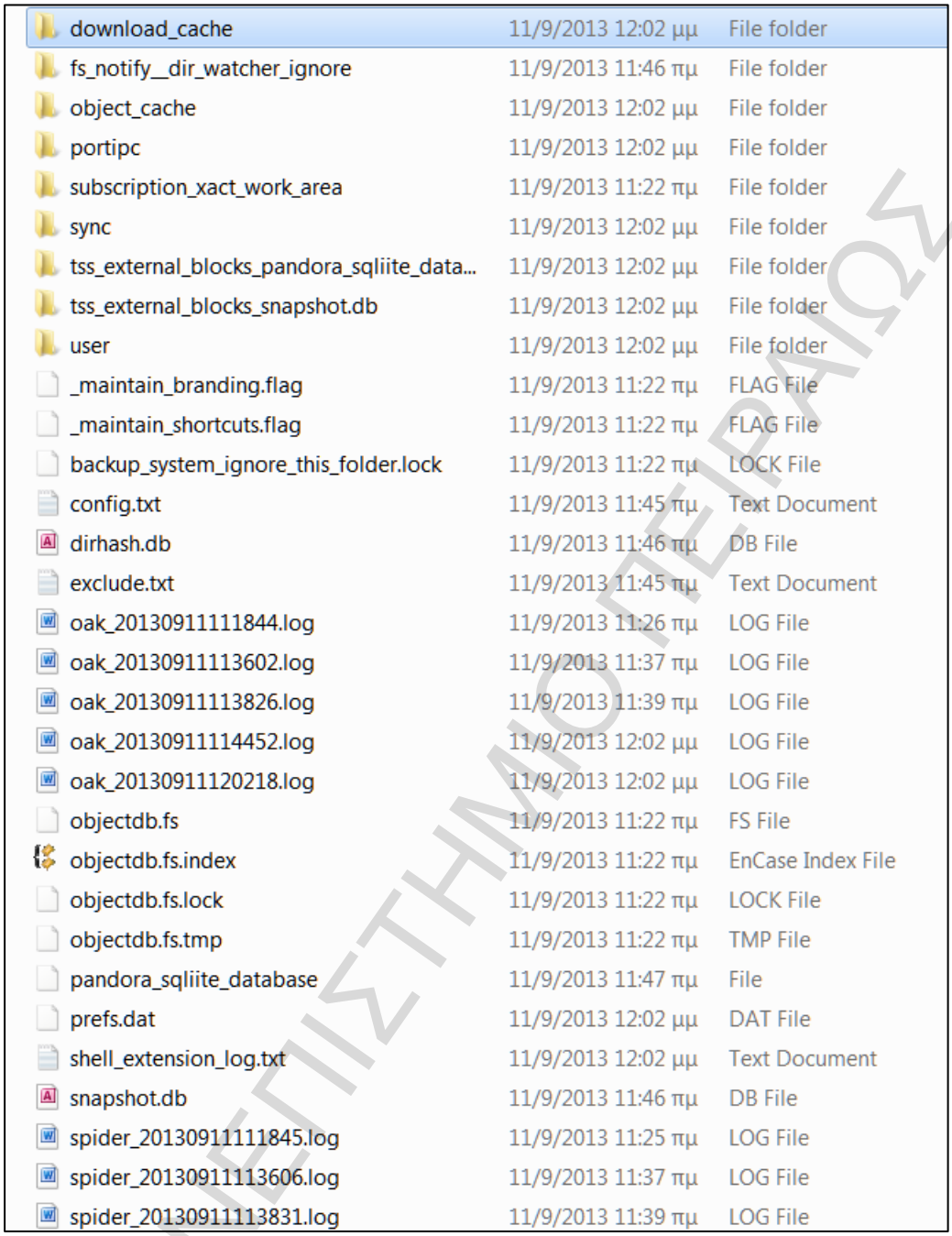
Πίνακας 8-2: Αλλαγές στην Registry των Windows

HKEY_CURRENT_USER\Software\SpiderOak, HKEY_CURRENT_USER\Software\Classes\LocalSettings\Software\Microsoft \Windows\Shell\MuiCache\C:\program files\SpiderOak\SpiderOak.exe, HKEY_CURRENT_USER\Software\SpiderOak\ShowIconOverlay HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SpiderOak.PropertySetStora HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\ E30A16E5E9E9DF0448388C6555CB76BB\SpiderOakApplication

8.4. «Ανέβασμα» αρχείων μέσω του SpiderOak Hive

Στο σενάριο αυτό θα εξετάσουμε τις πληροφορίες που μπορούμε να ανακαλύψουμε μετά την διακίνηση αρχείων μέσω της λειτουργίας SpiderOak Hive. Συγκεκριμένα στο πρώτο σενάριο θα «ανεβάσουμε» τα αρχεία μας στον φάκελο Hive και στο δεύτερο σενάριο θα συγχρονίσουμε τον λογαριασμό μας και θα «κατεβάσουμε» τα αρχεία από τον διακομιστή της υπηρεσίας στο υπολογιστικό μας σύστημα.

Όπως προαναφέραμε στην τοποθεσία:*C:\Users\Random\AppData\Roaming\SpiderOak* βρίσκουμε τα αρχεία που δημιουργούνται από την χρήση της εφαρμογής.



Εικόνα 8-1: Παρουσίαση των προς εξέτασιν αρχείων

Στην έρευνα μας αρχικά θα επικεντρωθούμε στα αρχεία Log. Πρόκειται για αρχεία που μπορούμε να τα επεξεργαστούμε με οποιαδήποτε εφαρμογή επεξεργασίας κειμένου (Textpad,Word). Στην περίπτωση μας θα χρησιμοποιήσουμε το πρόγραμμα Microsoft Word.

Αρχικά καταφέραμε να ανακαλύψουμε

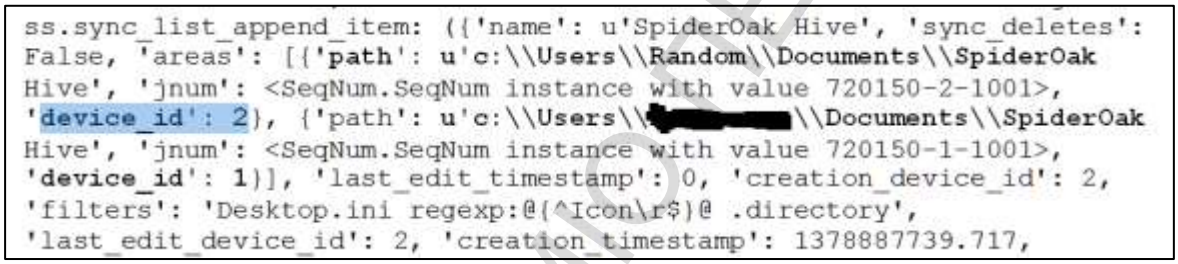
- τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας-PCno1 και PCVM-
- τις ημερομηνίες πρόσβασης στις δυο συσκευές
- και την τοποθεσία αποθήκευσης των αρχείων

Πίνακας 8-3: Συσκευές συσχετισμένες με τον λογαριασμό μας

2013-09-11 11:19:00,707 DEBUG oak status: signal: sc.reply_setup_devices: ([{u'sysplatform': u'win32', u'last_login': 1378814990.0,
u'creation_time': 1378656645.0, u'name': u'**PCno1', u'device_id': 1**}, {u'sysplatform': u'win32', u'last_login': 1378822757.0,
u'creation_time': 1378800956.0, u'name': **u'PCVM', u'device_id': 2}**],)

Πίνακας 8-4: Ημερομηνία εισόδου στον λογαριασμό μας

2013-09-11 11:22:12,401 DEBUG oak status: set space_usage to {'by_device': [{'device_id': 2, 'storage_used': 0, 'device_desc': u'PCVM'}, {'device_id': 1, 'storage_used': 1637856, 'device_desc': u'PCno1'}], 'size_of_all_files': 1690251, 'by_category': {'Documents': 1637856}}



Εικόνα 8-2: Διεύθυνση των φακέλων αποθήκευσης των αρχείων

Στην συνέχεια ανακαλύψαμε το όνομα των αρχείων που διακινήσαμε, την ημερομηνία που έλαβαν χώρα οι ενέργειες αυτές ,καθώς και το μέγεθος των αρχείων.

Πίνακας 8-5: Όνομα αρχείου και ημερομηνία διακινήσεως του(1)

2013-09-11 11:45:33,174 DEBUG oak status: signal: ss.currently_building_fs_entry: (('new_file', u'c:\\Users\\Random\\Documents\\SpiderOak Hive\\002021.pdf', u'c:\\Users\\Random\\Documents\\SpiderOak Hive', 753418),)
2013-09-11 11:45:33,174 DEBUG oak

Πίνακας 8-6: Όνομα αρχείου και ημερομηνία διακινήσεως του(2)

ss.currently_building_fs_entry: (('new_file', u'c:\\Users\\Random\\Documents\\SpiderOak Hive\\002052.txt', u'c:\\Users\\Random\\Documents\\SpiderOak Hive', 95225),)
2013-09-11 11:45:33,267 DEBUG oak

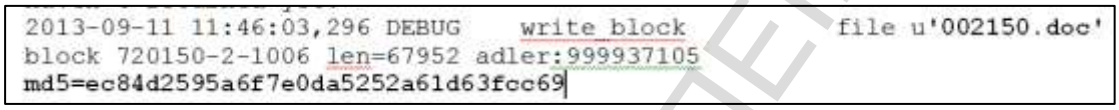
Πίνακας 8-7: Όνομα αρχείου και ημερομηνία διακινήσεως του(3)

2013-09-11 11:45:33,299 DEBUG oak status: signal: ss.currently_building_fs_entry: (('new_file', u'c:\\Users\\Random\\Documents\\SpiderOak Hive\\002098.jpg', u'c:\\Users\\Random\\Documents\\SpiderOak Hive', 115561),)

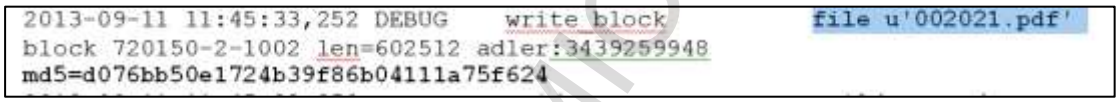
Πίνακας 8-8: Όνομα αρχείου και ημερομηνία διακινήσεως του(4)

ss.currently_building_fs_entry: (('new_file', u'c:\\Users\\Random\\Documents\\SpiderOak Hive\\002150.doc', u'c:\\Users\\Random\\Documents\\SpiderOak Hive', 256000),) 2013-09-11 11:46:03,265 DEBUG oak status: signal: ss.updated_status_bar: ()

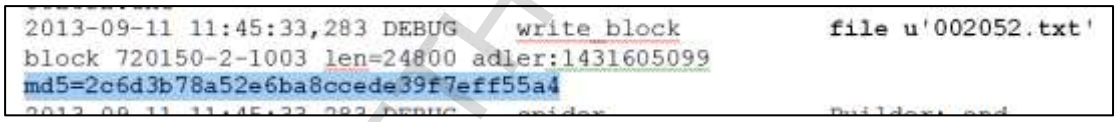
Ακόμα καταφέραμε να ανακαλύψουμε και το md5hash value των αρχείων που διακινήσαμε.



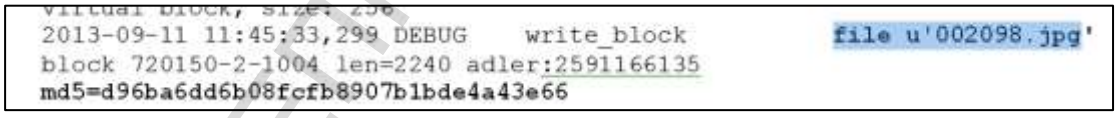
Εικόνα 8-3: MD5 αρχείου(1)



Εικόνα 8-4: MD5 αρχείου(2)



Εικόνα 8-5: MD5 αρχείου(3)



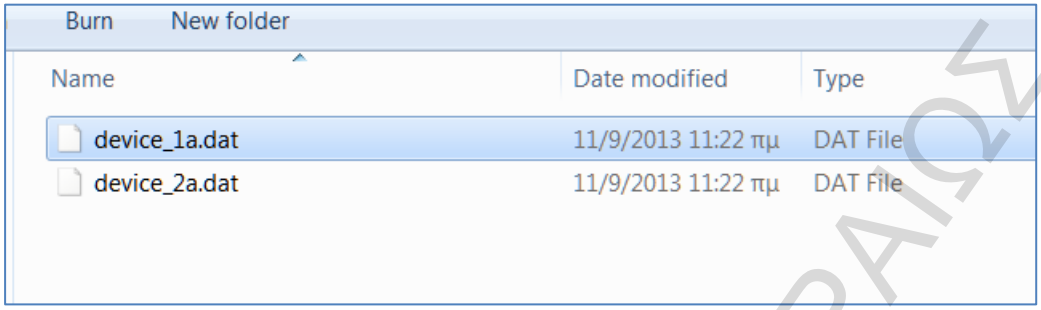
Εικόνα 8-6: MD5 αρχείου(4)

Συνοψίζοντας με την εξέταση των Log αρχείων του SpiderOak καταφέραμε να ανακαλύψουμε τα εξής:

- τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας
- την διεύθυνση αποθήκευσης των αρχείων και στις δύο συσκευές
- τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος,md5hash)
- την ώρα και ημερομηνία διακίνησης των αρχείων

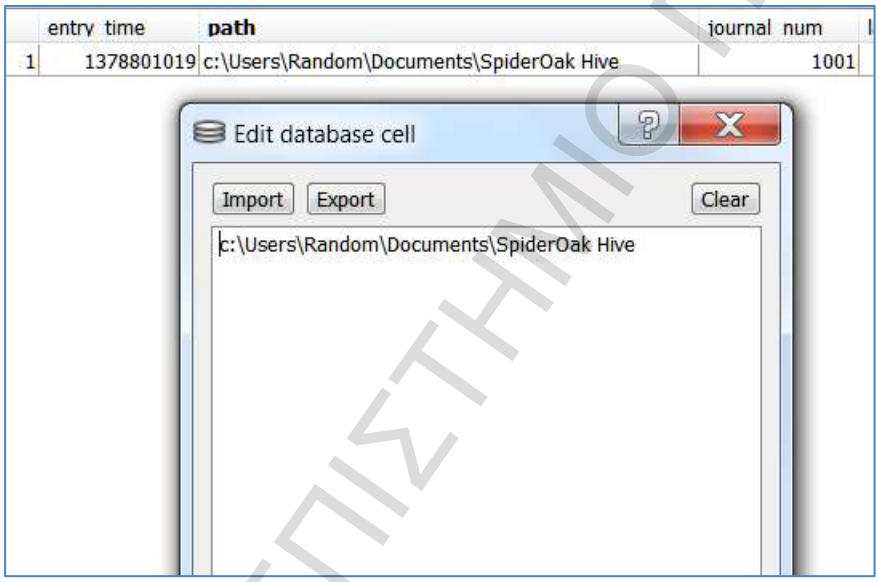
8.4.1 Εξέταση των βάσεων δεδομένων του SpiderOak

Στο υποκεφάλαιο αυτό θα εξετάσουμε τις βάσεις δεδομένων του SpiderOak.Αρχικά εξετάζουμε τον φάκελο object_cache.



Εικόνα 8-7: Περιεχόμενα φακέλου object_cache

Εδώ βρίσκουμε πληροφορίες για τις συσκευές που συνδέονται με τον λογαριασμό μας. Για την ακρίβεια ανακαλύπτουμε το «path» του φακέλου όπου αποθηκεύουμε τα αρχεία.



Εικόνα 8-8: Φάκελος αποθήκευσης αρχείων

Το επόμενο αρχείο που θα εξετάσουμε είναι η SQL βάση δεδομένων pandora_sqliite_database, ακλουθώντας την μεθοδολογία του κεφαλαίου 6.

Εξετάζοντας το table version_reference ανακαλύπτουμε όλα τα αρχεία που είναι αποθηκευμένα στον φάκελο Hive.

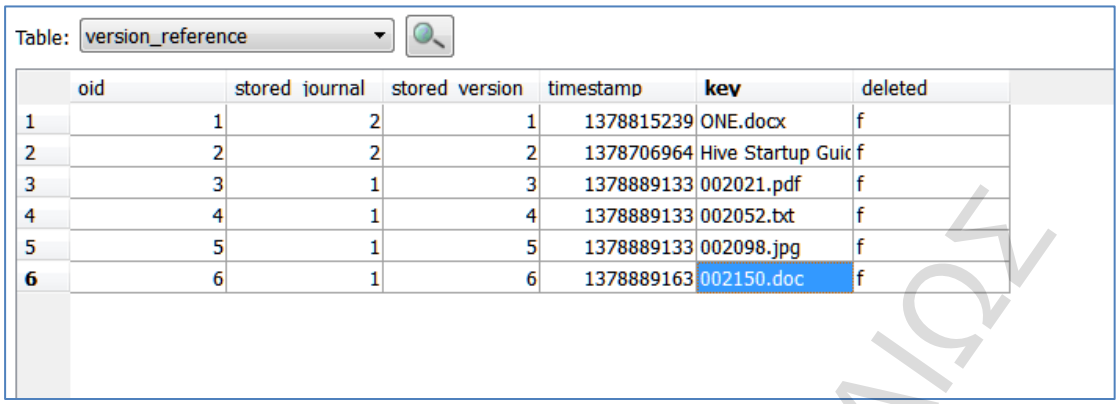


Table: version_reference

	oid	stored journal	stored version	timestamp	key	deleted
1	1	2	1	1378815239	ONE.docx	f
2	2	2	2	1378706964	Hive Startup Guic	f
3	3	1	3	1378889133	002021.pdf	f
4	4	1	4	1378889133	002052.txt	f
5	5	1	5	1378889133	002098.jpg	f
6	6	1	6	1378889163	002150.doc	f

Εικόνα 8-9: Ανακάλυψη αρχείων

Συνοψίζοντας με την εξέταση των SQL και Log αρχείων καταφέραμε να ανακαλύψουμε τα εξής:

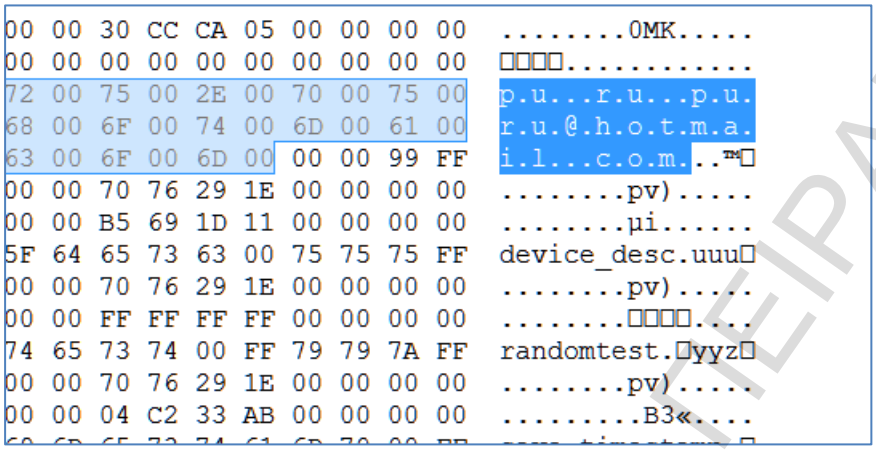
Πίνακας 8-9: Χρήση του λογισμικού του SpiderOak

Όνομα Αρχείου	Ευρήματα
Αρχεία Log	Πληροφορίες για : • τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας • την διεύθυνση αποθήκευσης των αρχείων και στις δύο συσκευές • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος,md5hash) • την ώρα και ημερομηνία διακίνησης των αρχείων
Databases • object_cache • pandora_sqliite_database	Πληροφορίες για: • τις συσκευές με τις οποίες συνδέεται ο λογαριασμός μας • το «path» του φακέλου όπου αποθηκεύουμε τα αρχεία • τα αρχεία που είναι αποθηκευμένα στον φάκελο Hive • Timestamps σχετικές με τον χρόνο δημιουργίας τους

8.4.2 Εξέταση της μνήμης Ram

Ερευνώντας τα περιεχόμενα της Ram με τον όρο SpiderOak βρίσκουμε πολλές αναφορές στην εφαρμογή αυτή. Στην προσπάθεια μας να βρούμε περισσότερες πληροφορίες για τον χρήστη της εφαρμογής αυτής και παίρνοντας υπόψιν τα προηγούμενα ευρήματα μας κάνουμε search με τον όρο «device».

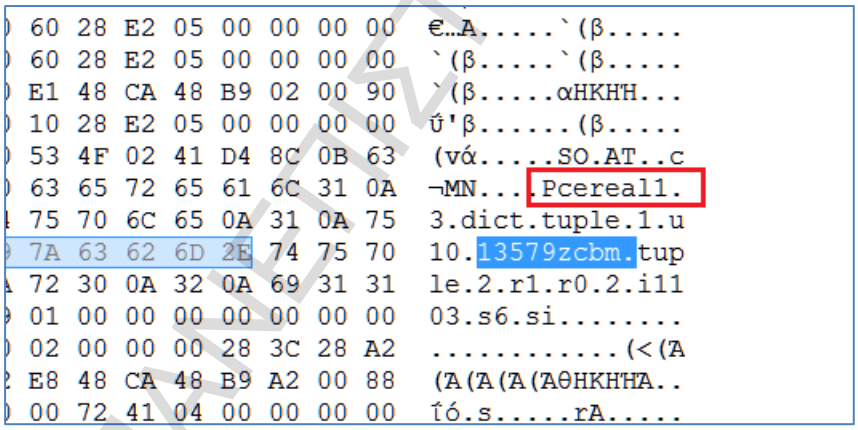
Καταφέρνουμε να ανακαλύψουμε το εξής:



Εικόνα 8-10: Εύρεση ονόματος χρήστη και e-mail.

Έτσι ανακαλύψαμε το όνομα του λογαριασμού και την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό αυτό. Περαιτέρω έρευνα με τον όρο «randnomtest» μας επιβεβαιώνει ότι αυτό είναι το όνομα του λογαριασμού.

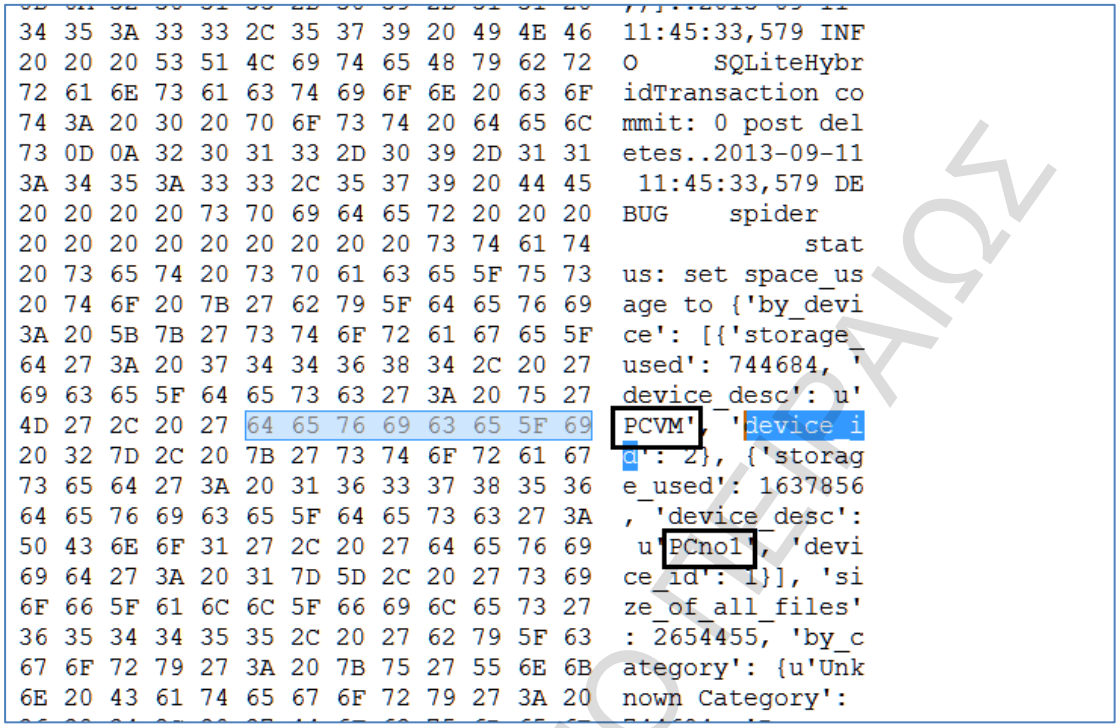
Ακόμα καθώς στο σενάριο μας χρησιμοποιήσαμε τον κωδικό πρόσβασης για να εισέλθουμε στην υπηρεσία του SpiderOak, καταφέραμε να τον ανακτήσουμε στην μνήμη.



Εικόνα 8-11: Εύρεση κωδικού

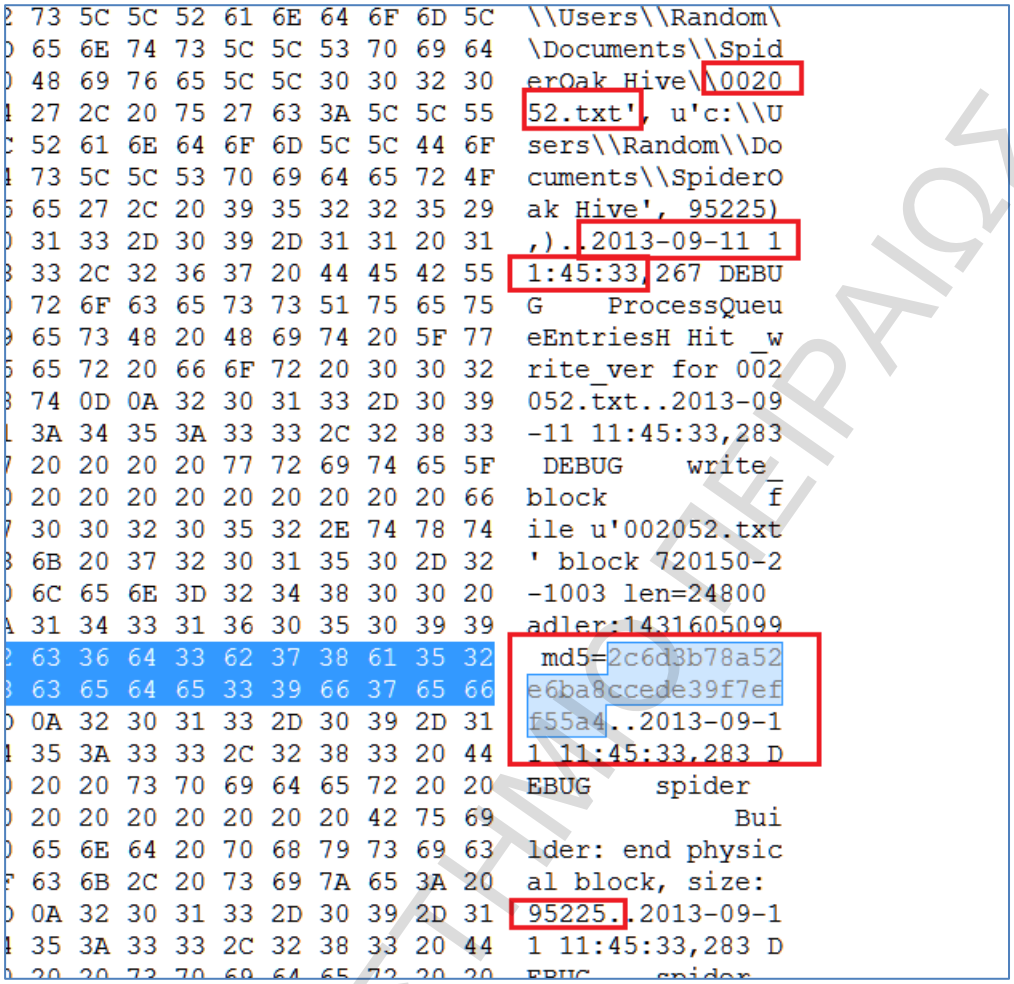
Παρατηρούμε ότι πριν το συνθηματικό βρίσκεται η ακολουθία χαρακτήρων «Pcereal1».Στα σενάρια μας ανακαλύψαμε ότι πάντα η ακολουθία αυτή χαρακτήρων προηγείται του συνθηματικού. Έτσι ανακαλύψαμε ένα μοτίβο που διευκολύνει την έρευνα μας για την υπηρεσία αυτή.

Επίσης μπορέσαμε να ανακαλύψουμε τις συσκευές που είναι συσχετισμένες με τον λογαριασμό μας.



Εικόνα 8-12: Συσκευές σχετιζόμενες με τον λογαριασμό μας

Επίσης καταφέραμε να ανακαλύψουμε τα αρχεία που «ανεβάσαμε», το μέγεθος τους, την ημερομηνία που έγινε η διακίνηση αυτή καθώς και την τιμή κατακερματισμού τους.



Εικόνα 8-13: Εύρεση πληροφοριών για τα αρχεία που διακινήσαμε

Στον πίνακα που ακολουθεί συνοψίζονται τα ευρήματα μας.

Πίνακας 8-10: Μνήμη RAM (χρήση λογισμικού του SpiderOak)

Αρχείο	Ευρήματα
RAM	Πληροφορίες για: • το όνομα του λογαριασμού και την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό αυτό • τον κωδικό πρόσβασης για να εισέλθουμε στην υπηρεσία του SpiderOak(πριν το συνθηματικό βρίσκεται η ακολουθία χαρακτήρων «Pcereal1») • τις συσκευές που είναι συσχετισμένες με τον λογαριασμό μας. • τα αρχεία που «ανεβάσαμε» • το μέγεθος, το md5hash και την ώρα και ημερομηνία που «ανεβάσαμε» τα αρχεία αυτά.

8.5. Συγχρονισμός και «κατέβασμα» αρχείων

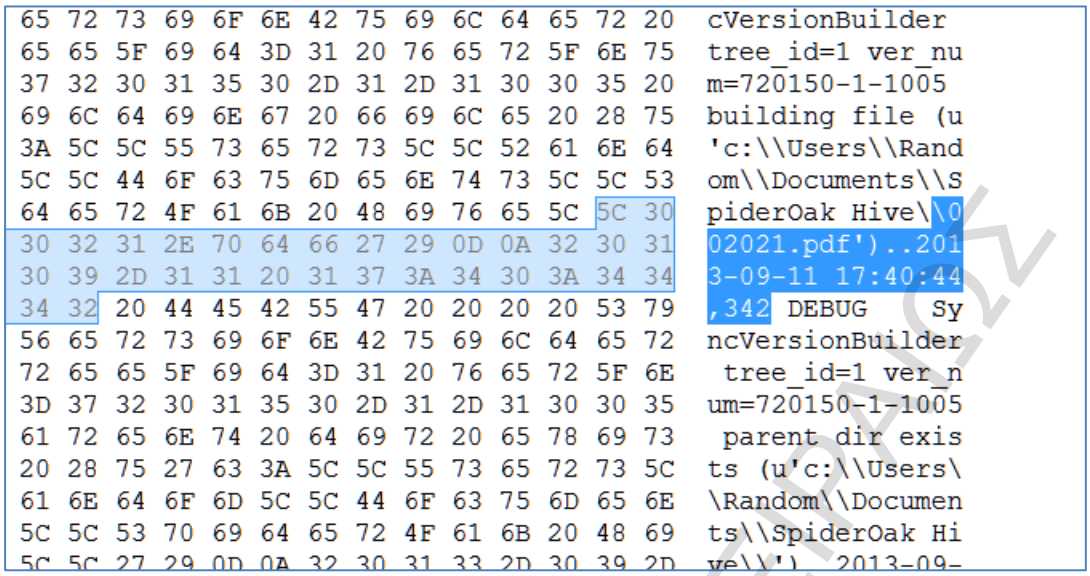
Όταν χρησιμοποιούμε το SpiderOak σε ένα υπολογιστικό σύστημα τότε η εφαρμογή αυτή ακλουθεί μια διαδικασία .Πρώτα συγχρονίζεται με τον διακομιστή της υπηρεσίας και στην συνέχεια μπορούμε να προβούμε στις ενέργειες που επιθυμούμε.

Στα πλαίσια της έρευνας μας ελέγξαμε τις ψηφιακές αποδείξεις που δημιουργούνται από τις εξής ενέργειες:

- Αυτόματος συγχρονισμός της υπηρεσίας SpiderOak και «κατέβασμα» των αρχείων στον φάκελο Hive από τον διακομιστή του SpiderOak.
- «Μεταφορά» των αρχείων σε μια εξωτερική συσκευή USB.

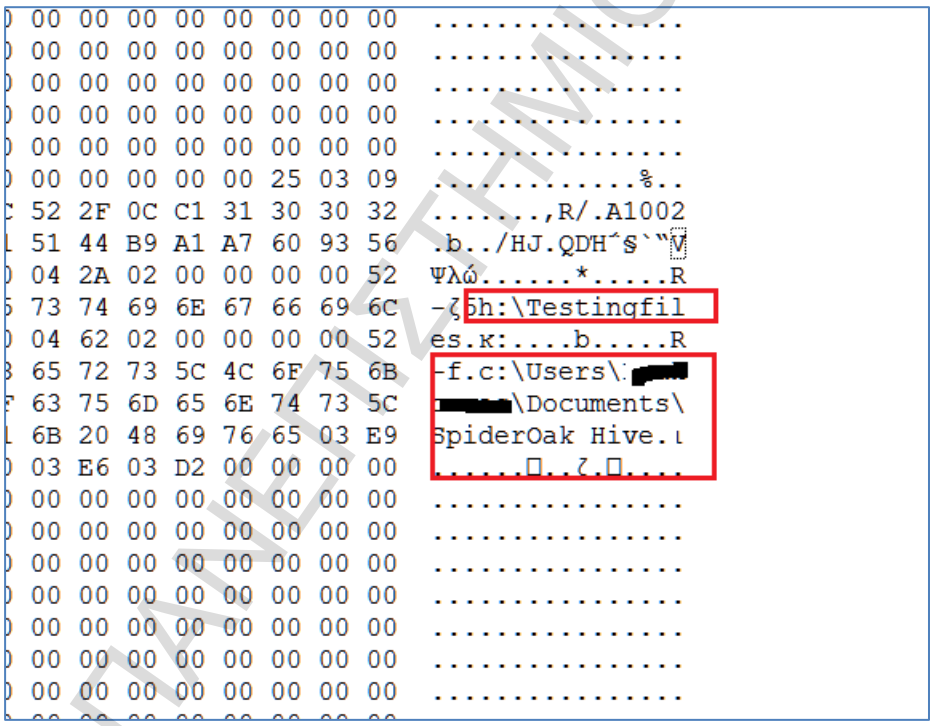
Μέτα την ολοκλήρωση του 1^{ου} βήματος εξετάσαμε τα περιεχόμενα της μνήμης RAM και τα περιεχόμενα των databases της εφαρμογής.

Με την εξέταση της μνήμης ανακαλύψαμε πληροφορίες σχετικά με το όνομα των αρχείων και την ημερομηνία που έγινε ο συγχρονισμός.



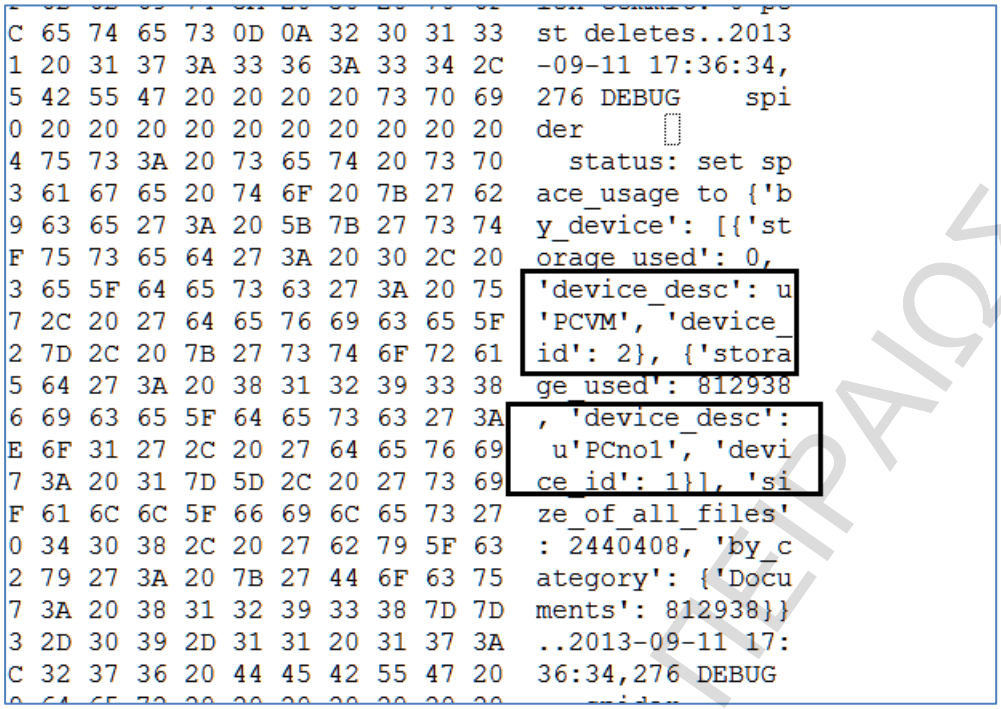
Εικόνα 8-14: Όνομα και ημερομηνία διακίνησης αρχείων

Ακόμα καταφέραμε να ανακαλύψουμε τις τοποθεσίες που σχετίζονται με τα αρχεία που διακινήσαμε. Συγκεκριμένα τα αρχεία ανέβηκαν από τον φάκελο Testingfiles μιας USB συσκευής(H:) και αποθηκεύτηκαν στον φάκελο SpiderOak/Hive του υπολογιστή Pcno1.



Εικόνα 8-15: Ανακάλυψη προέλευσης και προορισμού των αρχείων

Τέλος καταφέραμε να ανακαλύψουμε και τα υπολογιστικά συστήματα που είναι συνδεδεμένα με τον λογαριασμό μας.

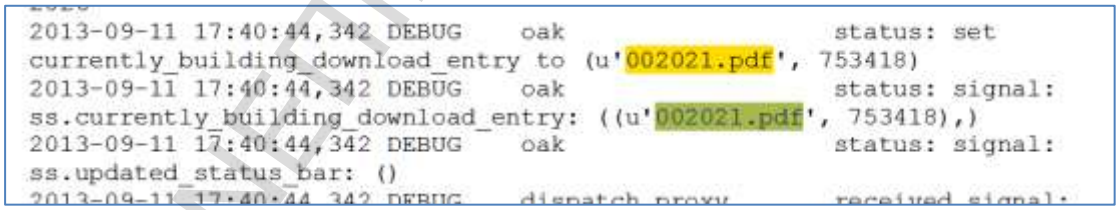


Εικόνα 8-16: Ανακάλυψη των συσχετισμένων υ/ων

Στην συνέχεια εξετάσαμε τις databases της εφαρμογής ακολουθώντας την διαδικασία που περιγράψαμε στο κεφάλαιο 6. Συνοπτικά ,τα αποτελέσματα μας -εξαιρουμένου των πληροφοριών που σχετίζονται με τα αρχεία που διακινήθηκαν-είναι ίδιες με το υποκεφάλαιο 8.4.1.

Όσον αφορά τα αρχεία, βρήκαμε τα ονόματα των αρχείων που κατεβάσαμε και τις ώρες που σχετίζονται με τις ενέργειες αυτές .Ωστόσο δεν μπορέσαμε να ανακαλύψουμε τις τιμές των md5 values τους.

Παρομοίως με την εξέταση των αρχείων Log της εφαρμογής τα ευρήματα μας διαφέρουν με αυτά του υποκεφαλαίου 8.4.1 στο γεγονός ότι ανακαλύψαμε λιγότερες πληροφορίες σχετικά με τα αρχεία που κατεβάσαμε (δεν βρήκαμε το md5hash).



Εικόνα 8-17: Εξέταση των αρχείων Log

Στον επόμενο πίνακα συνοψίζουμε τα ευρήματα μας για το σενάριο αυτό.

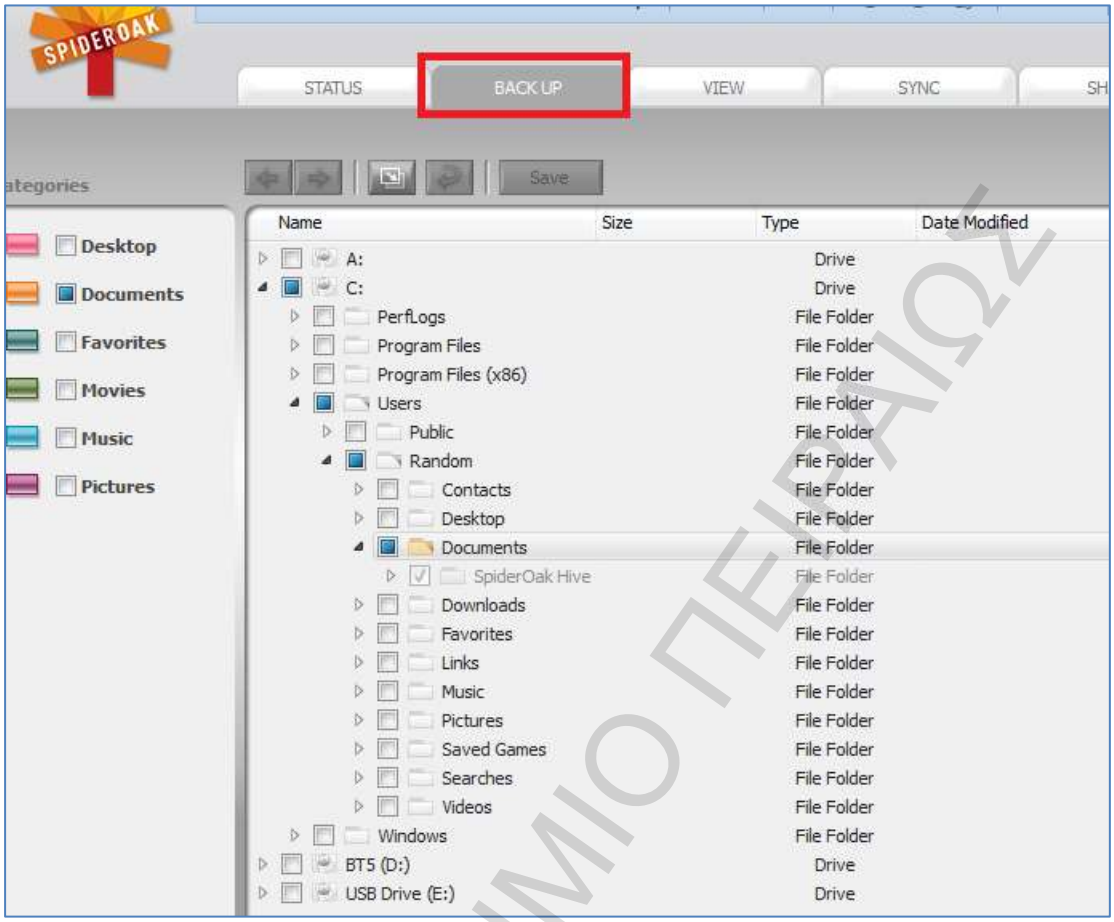
Πίνακας 8-11: «Κατέβασμα» αρχείων (χρήση λογισμικού του SpiderOak)

Αρχείο	Ευρήματα
Αρχεία Log	Πληροφορίες για : • τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας • την διεύθυνση αποθήκευσης των αρχείων και στις δύο συσκευές • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος) • την ώρα και ημερομηνία διακίνησης των αρχείων
Databases • object_cache • pandora_sqliite_database	Πληροφορίες για: • τις συσκευές με τις οποίες συνδέεται ο λογαριασμός μας • το «path» του φακέλου όπου αποθηκεύουμε τα αρχεία • τα αρχεία που είναι αποθηκευμένα στον φάκελο Hive • Timestamps σχετικές με τον χρόνο δημιουργίας τους
RAM	Πληροφορίες για: • τις συσκευές που είναι συσχετισμένες με τον λογαριασμό μας. • τα αρχεία που «κατεβάσαμε» • το μέγεθος και την ώρα και ημερομηνία που «κατεβάσαμε» τα αρχεία αυτά. • Το πλήρες «path» της διεύθυνσης προελεύσεως και προορισμού των αρχείων

8.6. Χρήση της λειτουργίας δημιουργίας αντιγράφων ασφαλείας της εφαρμογής SpiderOak.

Στο σενάριο αυτό θα χρησιμοποιήσουμε την λειτουργία ‘BACK UP’ του SpiderOak. Σκοπός της έρευνας μας είναι να προσδιορίσουμε τις ψηφιακές αποδείξεις που δημιουργούνται με την ενέργεια μας αυτή και αφορούν μόνο τα αρχεία για τα οποία δημιουργήσαμε αντίγραφα ασφαλείας.

Στην εικόνα που ακολουθεί παρουσιάζουμε το περιβάλλον της λειτουργίας ‘BACK UP’ της εφαρμογής.



Εικόνα 8-18: Περιβάλλον της εφαρμογής SpiderOak

Εξετάζοντας τα αρχεία Log καταφέρνουμε να ανακαλύψουμε τα δεδομένα που κάναμε back up,το μέγεθος τους καθώς και την ημερομηνία και ώρα που έλαβε χώρα αυτή η ενέργεια .Δεν μπορέσαμε όμως να βρούμε κάποια άλλη πληροφορία για αυτά τα αρχεία όπως π.χ. την τιμή κατακερματισμού τους.

```
2013
2013-09-12 10:25:58,503 DEBUG    oak                    status: set
currently_building_fs_entry to ('new_file',
u'e:\\Testingfiles\\002150.doc', u'e:\\Testingfiles', 256000)
2013-09-12 10:25:58,503 DEBUG    oak                    status: signal:
ss.currently_building_fs_entry: (('new_file',
u'e:\\Testingfiles\\002150.doc', u'e:\\Testingfiles', 256000),)
2013-09-12 10:25:58,503 DEBUG    oak                    status: signal:
ss.updated_status_bar: ()
```

Εικόνα 8-19: Πληροφορίες για τα αρχεία που διακινήσαμε

Στο επόμενο βήμα εξετάσαμε τις SQL βάσεις δεδομένων τις εφαρμογές. Η έρευνα μας ταυτίζεται με την έρευνα που κάναμε στο υποκεφάλαιο 8.4. ,όπως και τα ευρήματα μας.

Αρχικά πλοηγούμαστε στα αρχεία της object_cache.Εκεί ανακαλύπτουμε επιπροσθέτως και την USB συσκευή από την οποία κάναμε το back up.

e: tree_2_entries

oid	entry_time	path	journal_num	last
1	1378801019	c:\Users\Random\Documents\SpiderOak Hive	1001	
2	1378970757	e:\Testingfiles	1002	

Εικόνα 8-20: Τοποθεσίες προέλευσης και προορισμού των αρχείων

Τέλος εξετάζοντας την βάση δεδομένων pandora_sqliite_database ανακαλύπτουμε τα αρχεία που κάναμε back up καθώς και το μέγεθος τους.

e: version_reference

oid	stored_journa	stored_versio	timestamp	key	deleted
1	3	1	1378970757	002021.pdf	f
2	3	2	1378970757	002052.txt	f
3	3	3	1378970757	002098.jpg	f
4	3	4	1378970757	002150.doc	f

Εικόνα 8-21: Εύρεση αρχείων που διακινήσαμε

stored_block

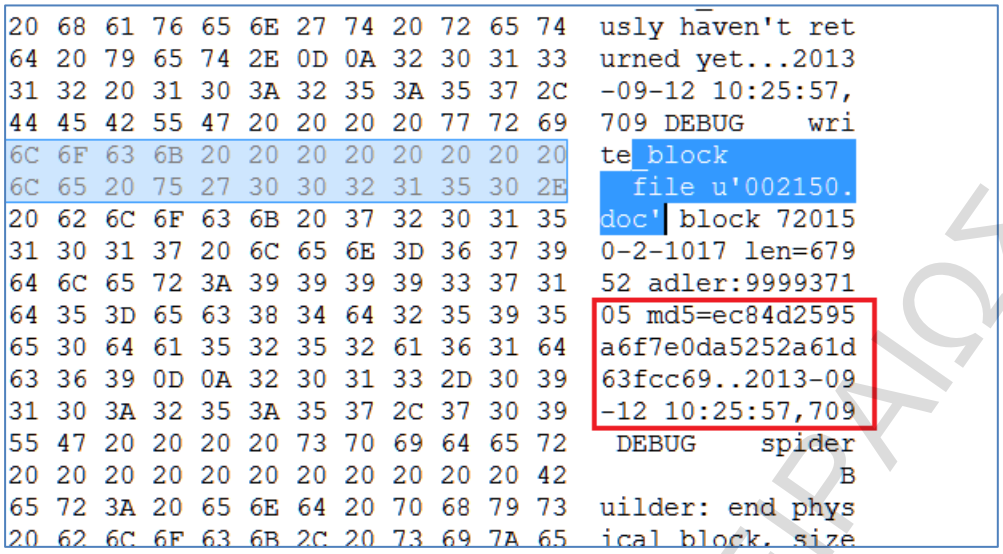
oid	user_id	device_id	block_id	md5_hash	storesize	blocksize
1	720150	2	1013	v P rK9 k	602544	753418
2	720150	2	1014	,m;x .k	24832	95225
3	720150	2	1015	k k	2272	2048
4	720150	2	1016	%Ĺ	113744	113513
5	720150	2	1017	YZo~ %	67984	256000

Εικόνα 8-22: Μέγεθος αρχείων που διακινήσαμε

Αντιστοιχίζοντας τα object id των δυο tables βρίσκουμε το μέγεθος των αρχείων.

8.6.1 Εξέταση της μνήμης RAM

Εξετάζοντας την RAM καταφέραμε να ανακαλύψουμε τα αρχεία που διακινήσαμε, το μέγεθος τους, το md5hash και την ώρα και ημερομηνία που έλαβε χώρα το back up τους.



Εικόνα 8-23: Πληροφορίες για τα αρχεία

Συνοψίζοντας τα ευρήματα μας στο σενάριο αυτό είναι τα εξής:

Πίνακας 8-12: Χρήση της λειτουργίας 'Back up' του SpiderOak

Αρχείο	Ευρήματα
Αρχεία Log	Πληροφορίες για : • τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος) • την ώρα και ημερομηνία που έλαβε χώρα το back up
Databases • object_cache • pandora_sqliite_database	Πληροφορίες για: • τις συσκευές με τις οποίες συνδέεται ο λογαριασμός μας • το «path» του φακέλου όπου αποθηκεύουμε τα αρχεία • το «path» του φακέλου από όπου προέρχονται τα αρχεία • τα αρχεία που κάναμε back up • Το μέγεθος των αρχείων
RAM	Πληροφορίες για: • τις συσκευές που είναι συσχετισμένες με τον λογαριασμό μας • τα αρχεία που κάναμε back up • το μέγεθος και την ώρα και ημερομηνία που κάναμε το back up • Το πλήρες «path» της διεύθυνσης προελεύσεως και προορισμού των αρχείων

8.6.2 «Κατέβασμα» των αντιγράφων ασφαλείας

Στο σενάριο αυτό θα «κατεβάσουμε» στην εικονική μηχανή μας τα αρχεία που κάναμε back up.Εξετάζοντας τα αρχεία Log ανακαλύπτουμε το όνομα των αρχείων, το μέγεθος τους καθώς και την ώρα και την ημερομηνία που τα ανακτήσαμε.

```
0x0000000005EF8A68>], None, [], [None, None, None, None], None, None, [1
2, 3, 4], None)
2013-09-12 11:49:02,568 DEBUG    spider                    status: signal:
ss.download_file_progress: (1, u'002021.pdf', 753418L, 'Done 1 item,
staging 0 items')
2013-09-12 11:49:02,568 DEBUG    spider                    status: signal:
ss.download_file_progress: (1, u'002021.pdf', 753418L, 'Done 1 item,
staging 0 items')
```

Εικόνα 8-24: Ευρήματα στα αρχεία Log

Τα ευρήματα μας όσον αφορά την εξέταση των SQL βάσεων δεδομένων της εφαρμογής είναι τα ίδια με το προηγούμενο σενάριο.

Τέλος εξετάζοντας την μνήμη RAM βρίσκουμε πληροφορίες για τα αρχεία που ανακτήσαμε, το μέγεθος τους καθώς και την ημερομηνία που έγινε η ενέργεια αυτή.

```
5 72 20 20 20 20 20 20 20 20    spider
0 73 74 61 74 75 73 3A 20 73        status: s
0 73 73 2E 64 6F 77 6E 6C 6F  ignal: ss.downlo
5 5F 70 72 6F 67 72 65 73 73  ad_file_progress
5 27 30 30 32 30 32 31 2E 70  : (1, u'002021.p
5 33 34 31 38 4C 2C 20 27 44  df', 753418L, 'D
9 74 65 6D 2C 20 73 74 61 67  one 1 item, stag
9 74 65 6D 73 27 29 0D 0A 32  ing 0 items')..2
0 31 32 20 31 31 3A 34 39 3A  013-09-12 11:49:
0 44 45 42 55 47 20 20 20 20  02,568 DEBUG
0 20 20 20 20 20 20 20 20 20  spider
4 61 74 75 73 3A 20 73 69 67       status: sig
3 2E 64 6F 77 6E 6C 6F 61 64  nal: ss.download
0 72 6F 67 72 65 73 73 3A 20  _file_progress:
0 30 32 30 32 31 2E 70 64 66  (1, u'002021.pdf
4 31 38 4C 2C 20 27 44 6F 6E  ', 753418L, 'Don
```

Εικόνα 8-25: Ευρήματα στην μνήμη RAM

Συνοψίζοντας τα ευρήματα μας στο σενάριο αυτό είναι τα εξής:

Πίνακας 8-13: Διακίνηση των αντιγράφων ασφαλείας

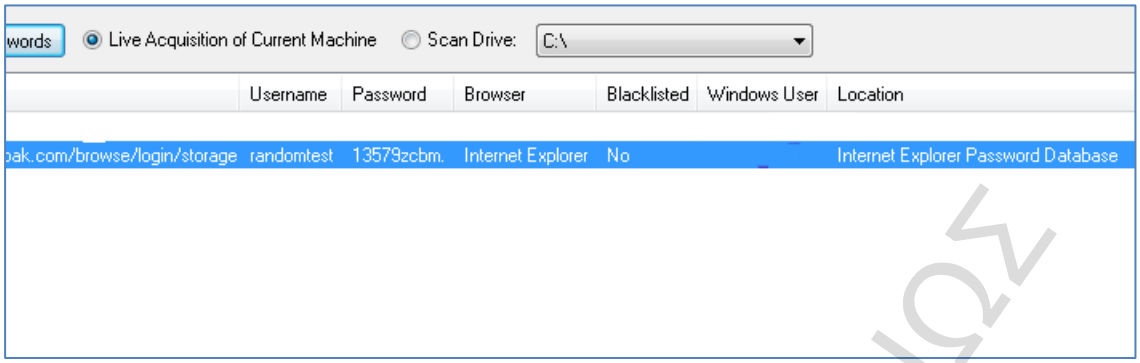
Αρχείο	Ευρήματα
Αρχεία Log	Πληροφορίες για : • τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος) • την ώρα και ημερομηνία που ανακτήσαμε τα αρχεία
Databases • object_cache • pandora_sqliite_database	Πληροφορίες για: • τις συσκευές με τις οποίες συνδέεται ο λογαριασμός μας • το «path» του φακέλου όπου αποθηκεύουμε τα αρχεία • το «path» του φακέλου από όπου προέρχονται τα αρχεία • τα αρχεία που ανακτήσαμε • Το μέγεθος των αρχείων
RAM	Πληροφορίες για: • τις συσκευές που είναι συσχετισμένες με τον λογαριασμό μας • τα αρχεία που ανακτήσαμε • το μέγεθος και την ώρα και ημερομηνία που κάναμε το back up

8.7. Πρόσβαση μέσω Περιηγητή

Το SpiderOak μας δίνει την δυνατότητα να «κατεβάσουμε» τα αρχεία που είναι αποθηκευμένα στον διακομιστή της υπηρεσίας μέσω κάποιου περιηγητή.

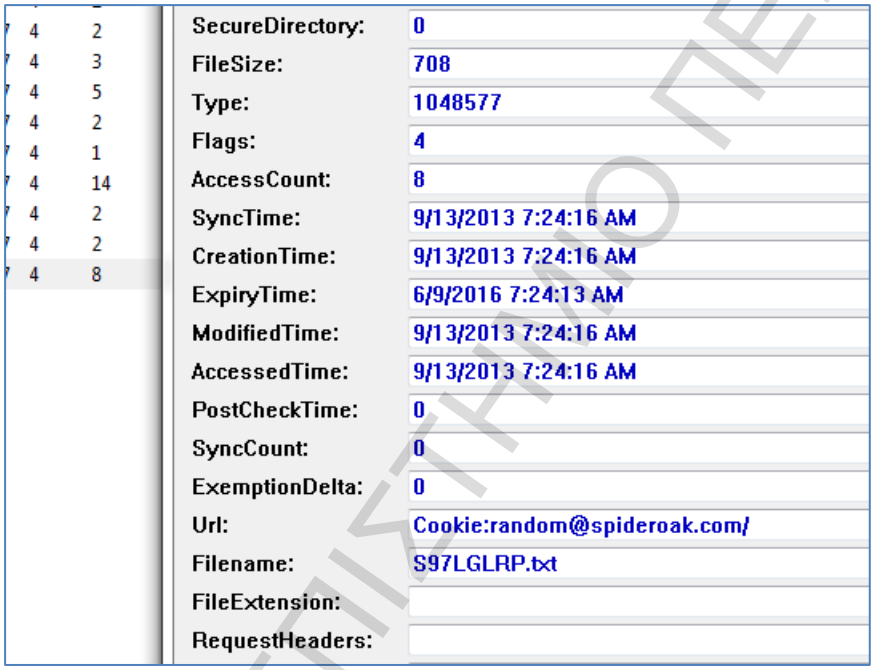
8.7.1 Χρήση του Internet Explorer 10

Με την χρήση του OSForensics και εφόσον έχουμε επιλέξει την αποθήκευση των κωδικών καταφέρνουμε με επιτυχία να ανακαλύψουμε το όνομα του χρήστη και τον κωδικό πρόσβασης.



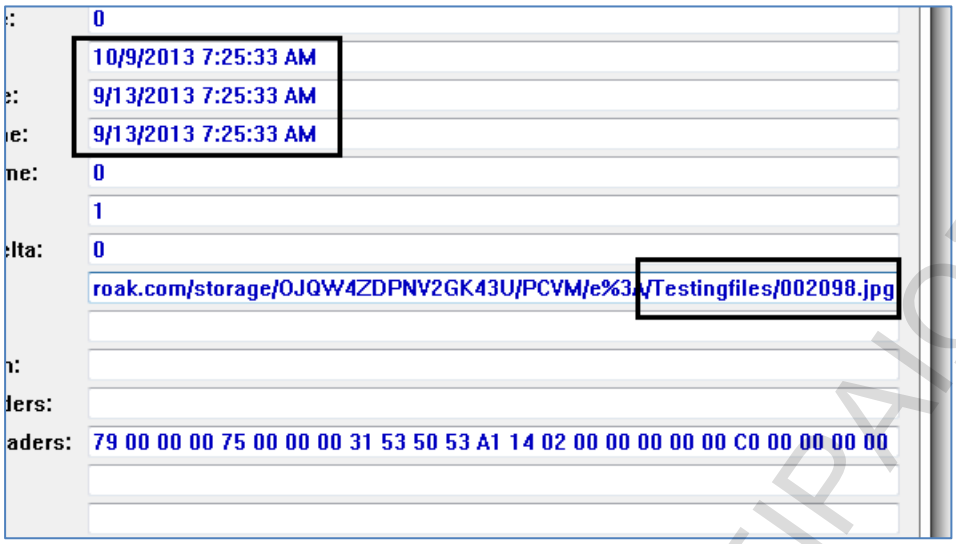
Εικόνα 8-26: Εύρεση κωδικών στον Internet Explorer

Ακολουθώντας την μεθοδολογία που έχουμε προσδιορίσει καταφέραμε να προσδιορίσουμε πολλές αναφορές που αποδεικνύουν την πρόσβαση μας στην εν λόγω υπηρεσία.



Εικόνα 8-27: Cookie του Internet Explorer

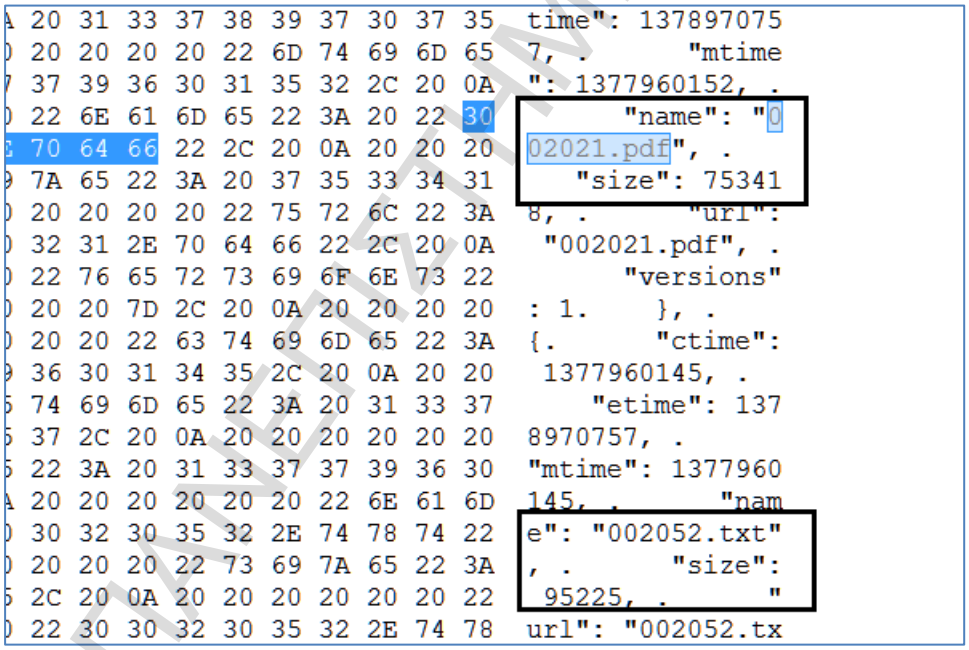
Εξετάζοντας το αρχείο 'Downloads' του Internet Explorer δεν καταφέραμε να ανακαλύψουμε κάποια πληροφορία για τα αρχεία που κατεβάσαμε . Ωστόσο η εξέταση του ιστορικού του περιηγητή μας αποκάλυψε τα αρχεία που κατεβάσαμε καθώς και την ώρα και ημερομηνία που έλαβε χώρα η ενέργεια αυτή.



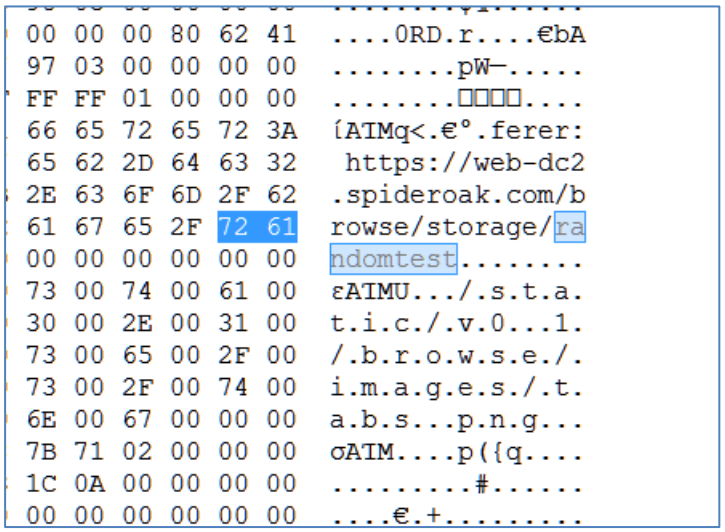
Εικόνα 8-28: Εύρεση αρχείων στο Ιστορικό του IE

RAM

Εξετάζοντας την μνήμη RAM βρήκαμε πληροφορίες για τα αρχεία που «κατεβάσαμε» καθώς και τον λογαριασμό SpiderOak που χρησιμοποιήσαμε.

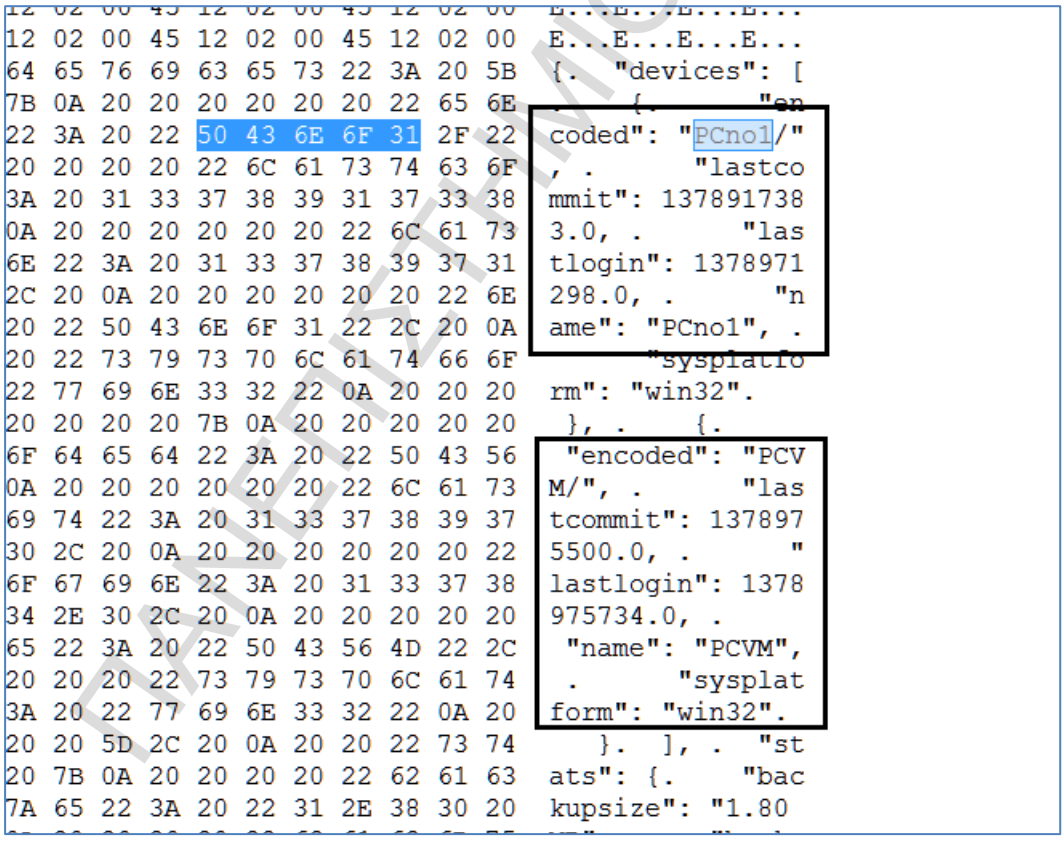


Εικόνα 8-29: Εύρεση αρχείων στην μνήμη RAM



Εικόνα 8-30: Όνομα κατόχου του λογαριασμού

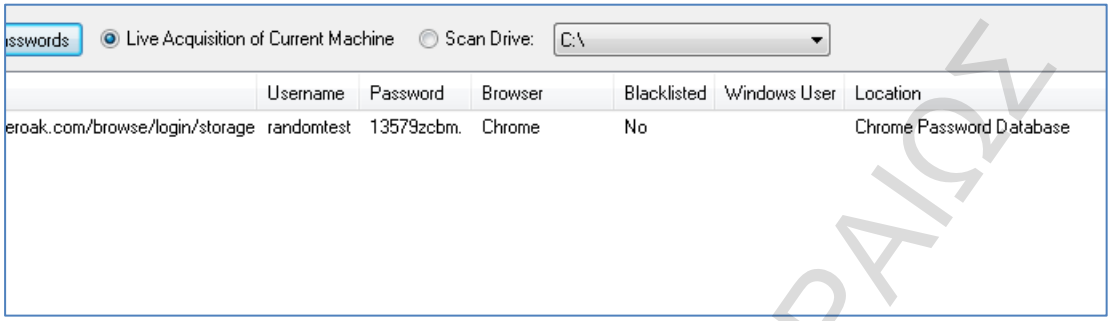
Τέλος ανακαλύψαμε και τις δυο συσκευές με τις οποίες είναι συνδεδεμένος ο λογαριασμός αυτός καθώς και την ημερομηνία που έγινε το τελευταίο Log in-σε μορφή που όμως δεν μπορούμε να αποκωδικοποιήσουμε.



Εικόνα 8-31: Εύρεση συσχετισμένων συσκευών

8.7.2 Χρήση του Google Chrome

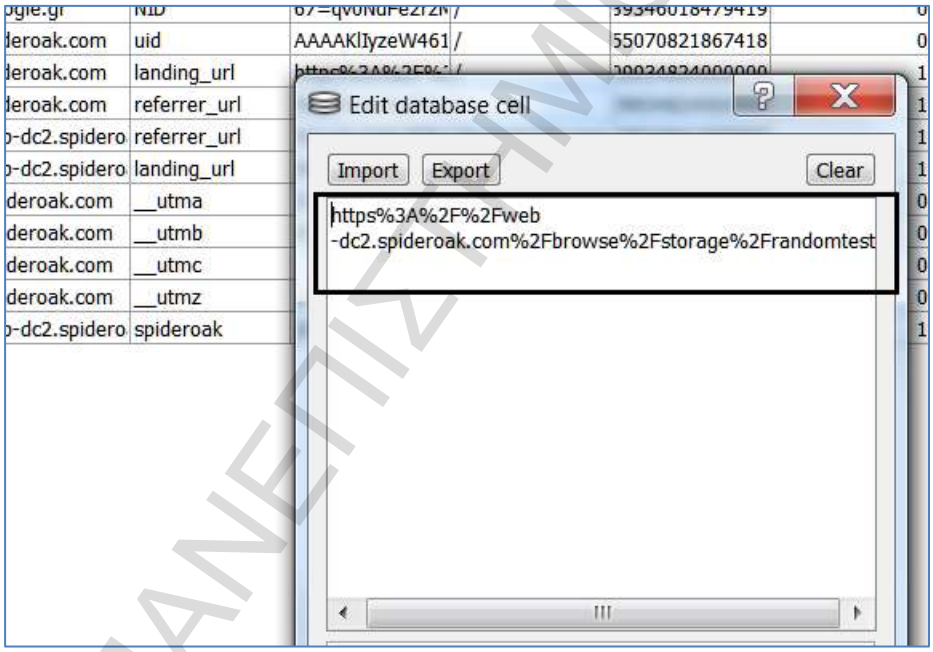
Στο σενάριο αυτό θα χρησιμοποιήσουμε τον περιηγητή Chrome.Αρχικά χρησιμοποιούμαι το OSForensics για την ανακάλυψη των κωδικών πρόσβασης



Εικόνα 8-32: Εύρεση κωδικών πρόσβασης στον Google Chrome

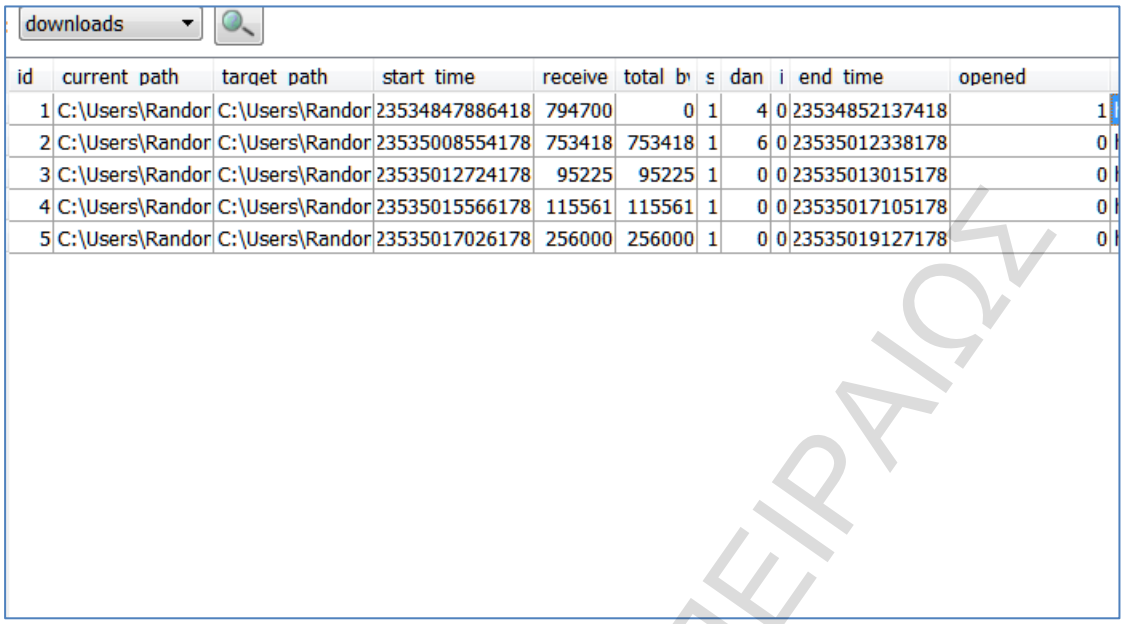
Πλοηγούμαστε στον φάκελο C:\Users\Random\AppData\Local\Google\Chrome\Default.

Το επόμενο βήμα είναι η εξέταση των περιεχόμενα της SQL βάσης δεδομένων History.Εκεί ανακαλύπτουμε το όνομα χρήστη του λογαριασμού SpiderOak.



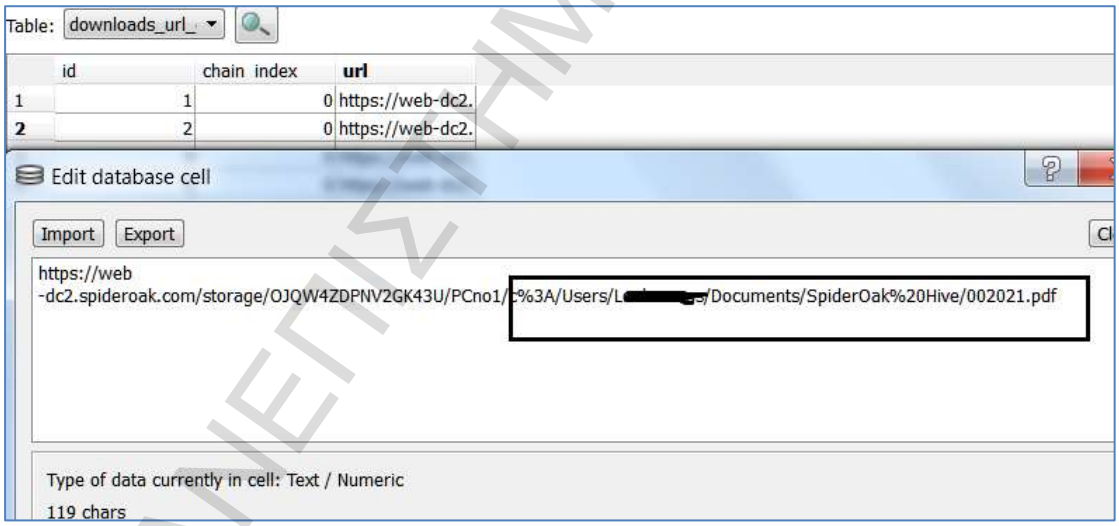
Εικόνα 8-33: Εξέταση Ιστορικού GC

Επίσης στο table downloads ανακαλύπτουμε τα αρχεία που «κατεβάσαμε» στον υπολογιστή μας καθώς και το μέγεθος τους και την ημερομηνία που έλαβε χώρα η ενέργεια αυτή.



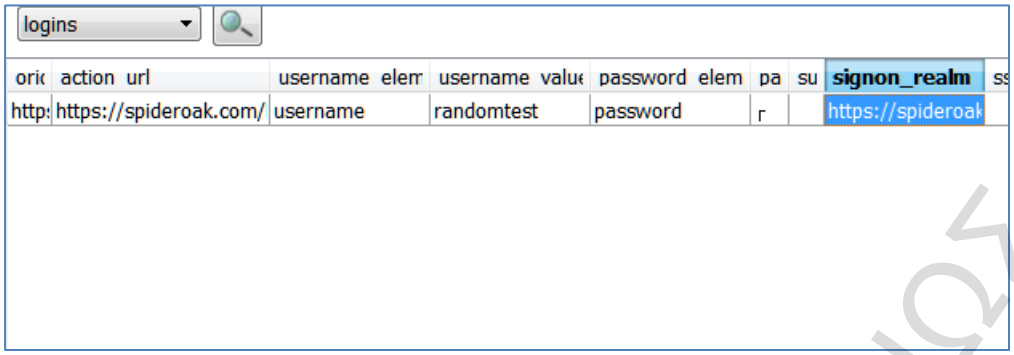
Εικόνα 8-34: Εύρεση αρχείων που κατεβάσαμε

Ακόμα στο table Download_url_chains ανακαλύπτουμε σε ποια συσκευή ήταν αποθηκευμένα τα αρχεία που κατεβάσαμε(PCno1) καθώς και σε ποιόν φάκελο.



Εικόνα 8-35: Εύρεση Υ/η που "ανεβάσαμε" τα αρχεία

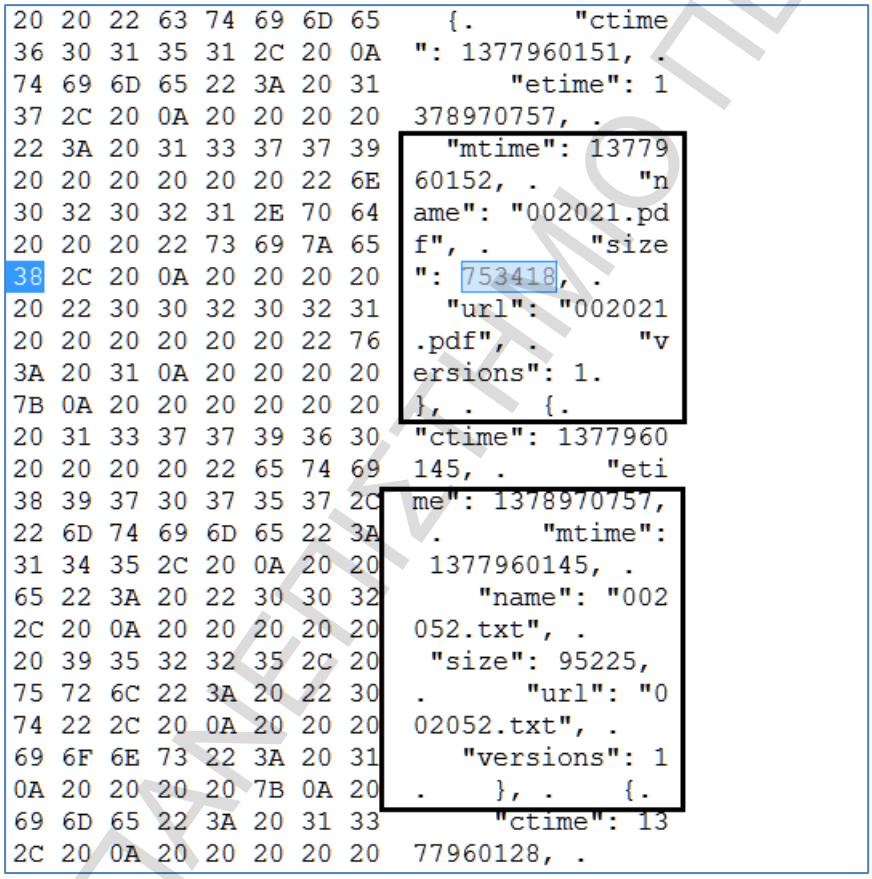
Τέλος εξετάζοντας την βάση δεδομένων Login Data ανακαλύπτουμε το όνομα χρήστη.



Εικόνα 8-36: Όνομα χρήστη

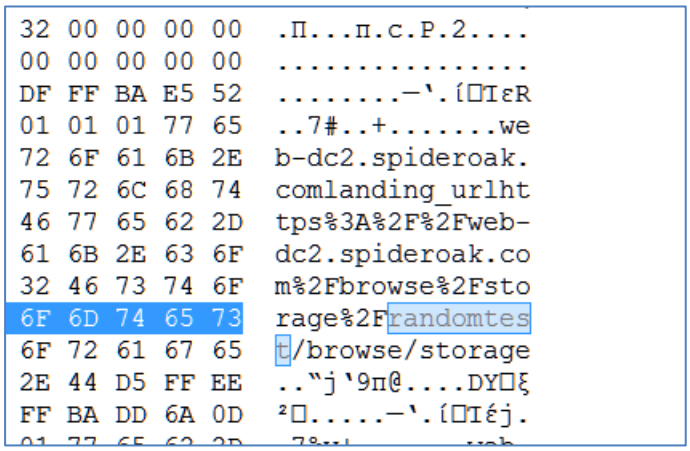
RAM

Στην μνήμη RAM βρήκαμε πληροφορίες για το όνομα των αρχείων που «κατεβάσαμε», το μέγεθος τους καθώς και την ώρα που έλαβε χώρα η ενέργεια αυτή.



Εικόνα 8-37: Πληροφορίες στην μνήμη RAM(1)

Ανακαλύψαμε ακόμα και το όνομα χρήστη.



Εικόνα 8-38: Πληροφορίες στην μνήμη RAM(2)

Μπορούμε να συνοψίσουμε τα ευρήματα μας στον κάτωθι πίνακα.

Πίνακας 8-14: Πρόσβαση στο SpiderOak μέσω περιηγητή

Περιηγητής	Ευρήματα
Internet Explorer • Cookies • History • RAM	Πληροφορίες για : • την πρόσβαση στην υπηρεσία SpiderOak • το όνομα των αρχείων που «κατέβηκαν» και τις ημερομηνίες • το μέγεθος αρχείων • το όνομα χρήστη του λογαριασμού • τις συσκευές συσχετισμένες με τον λογαριασμό
Google Chrome • Cookies • History • RAM	Πληροφορίες για : • την πρόσβαση στην υπηρεσία SpiderOak • το όνομα χρήστη του λογαριασμού • το όνομα αρχείων που «κατέβηκαν», ημερομηνίας και μεγέθους τους • τις συσκευές συσχετισμένες με τον λογαριασμό • την συσκευή αποθήκευσης των αρχεία που κατεβάσαμε(PCno1) καθώς τον φάκελο προέλευσης.

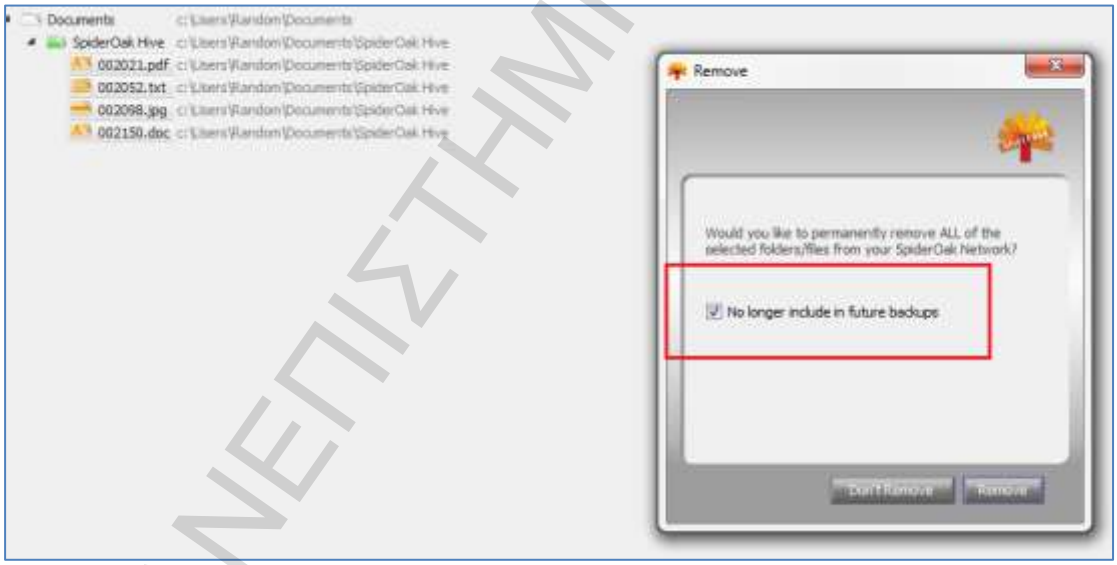
8.8. Διαγραφή αρχείων

Όταν σβήνουμε κάποιο αρχείο στο περιβάλλον της εφαρμογής SpiderOak τότε αυτό αποθηκεύεται στον φάκελο ‘Deleted Items’.

Εικόνα 8-39: Λειτουργία διαγραφής αρχείων

Αυτό οφείλεται στο γεγονός ότι το SpiderOak επιτρέπει ακόμα και αν σβήσουμε τα αρχεία αυτά να είναι διαθέσιμα για τα μελλοντικά back up μας.

Για την πλήρη απομάκρυνση ενός αρχείου από τον αποθηκευτικό χώρο του λογαριασμού μας απαιτείται να αφαιρέσουμε χειροκίνητα το αρχείο και από τον φάκελο 'Deleted Items'.



Εικόνα 8-40: Οριστική διαγραφή αρχείων

Στην περίπτωση που τα αρχεία βρίσκονται αποθηκευμένα στον φάκελο 'Deleted Files',μπορούμε επιτυχώς να ανακτήσουμε πληροφορίες για αυτά. Πρέπει να επισημάνουμε ότι βρίσκουμε πληροφορίες για όλα τα διαγραμμένα αρχεία του λογαριασμού μας.

Πλοηγούμαστε στην SQL βάση δεδομένων pandora_sqliite_database. Επιλέγουμε το table deleted_version_reference

timestamp	key	journal_id	i device	i user id	versic	v	v user id	filesize
1378909744	002098.jpg	1001	2	720150	1007	1	720150	115561
1378909744	002052.txt	1001	2	720150	1006	1	720150	95225
1378909744	002150.doc	1001	2	720150	1008	1	720150	256000
1378909744	002021.pdf	1001	2	720150	1005	1	720150	753418
1378909546	002098.jpg	1001	1	720150	1007	1	720150	115561
1378909546	002052.txt	1001	1	720150	1006	1	720150	95225
1378909546	002150.doc	1001	1	720150	1008	1	720150	256000
1378909546	002021.pdf	1001	1	720150	1005	1	720150	753418

Εικόνα 8-41: Εύρεση διαγραμμένων αρχείων

Στην περίπτωση που αφαιρέσουμε τα αρχεία και από τον φάκελο 'Deleted Files' τότε οι μόνες αναφορές που βρίσκουμε για τα αρχεία αυτά είναι από τα αρχεία Logs της εφαρμογής.

Πίνακας 8-15: Εξέταση αρχείων Log

2013-09-11 19:00:23,447 DEBUG oak status: set verbose_status_text to Purging file 002021.pdf
2013-09-11 19:00:23,447 DEBUG oak status: signal: ss.verbose_status_text: (u'Purging file 002021.pdf',)
2013-09-11 19:00:23,447 DEBUG oak status: signal: ss.updated_status_bar: ()

8.9. Μεταδεδομένα αρχείων

Η διαδικασία της διακίνησης αρχείων μέσω του SpiderOak δεν επηρεάζει τα metadata των αρχείων(Author,Permissions,Date printed,md5hash value κ.α). Αντίθετα αυτό που επηρεάζει είναι την ημερομηνία δημιουργίας(Date Created),την ημερομηνία τροποποίησης (Date Modified) και την ημερομηνία πρόσβασης(Date Accesed) του αρχείου. Οι τρείς αυτές μεταβλητές αποκτούν την τιμή της ημερομηνίας που ολοκληρώθηκε το «κατέβασμα» τους στο υπολογιστικό μας σύστημα.

8.10. Απεγκατάσταση του προγράμματος

Τέλος αναλύσαμε την συμπεριφορά του SpiderOak κατά την διαδικασία της απεγκατάστασης του με την σύγκριση των υπογραφών του συστήματος.

Στο πρώτο σενάριο απεγκαταστήσαμε το πρόγραμμα μέσω του Πινάκα Ελέγχου του λειτουργικού συστήματος .Με τον τρόπο αυτό βρήκαμε πληθώρα αναφορών του προγράμματος SpiderOak στην Registry των Windows ενώ και ο φάκελος " AppData\Roaming\SpiderOak " παρέμεινε ανέπαφος.

Στο δεύτερο σενάριο για την απεγκατάσταση του SpiderOak χρησιμοποιήσαμε το πρόγραμμα CC Cleaner. Αφού απεγκαταστήσαμε το SpiderOak χρησιμοποιήσαμε την επιλογή του Registry Scan για να αφαιρέσουμε τυχόν εναπομείναντες αναφορές του SpiderOak απο την Registry των Windows .Σε αυτό το σενάριο βρήκαμε λιγότερες αναφορές στο SpiderOak στην Registry ωστόσο ο φάκελος 'AppData\ Roaming\SpiderOak' παρέμεινε ανέπαφος.

Πίνακας 8-16: Υπολείμματα στην Registry

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\Background\shellex\ ContextMenuHandlers\SpiderOak HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\shellex\ContextMenuHandlers\SpiderOak

Τέλος στο τρίτο σενάριο συνδυάσαμε το CC Cleaner με το Eraser. Καταφέραμε και σβήσαμε εντελώς τον φάκελο 'SpiderOak' ωστόσο συνέχισαν να υπάρχουν αναφορές του προγράμματος στην Registry των Windows.

Συνοψίζοντας μετά την απεγκατάσταση του SpiderOak μπορούμε με ασφάλεια να υποστηρίξουμε ότι ο ερευνητής μπορεί να ανακαλύψει δεδομένα που αποδεικνύουν την χρήση του-στην χειρότερη περίπτωση- και στην καλύτερη να ανακαλύψει και τα ίδια τα αρχεία του SpiderOak.

Πίνακας 8-17: Απεγκατάσταση του SpiderOak

Σενάριο	Ευρήματα
Σενάριο 1: Απλή απεγκατάσταση	Αναφορές στην Registry Άθικτος ο φάκελος ΄SpiderOak
Σενάριο 2:Χρήση CC Cleaner	Αναφορές στην Registry(λιγότερες απο το σενάριο 1) Άθικτος ο φάκελος SpiderOak
Σενάριο 3:Χρήση CC cleaner και Eraser	Αναφορές στην Registry (ίδιες με το σενάριο 2)

8.11. Παρουσίαση

Πίνακας 8-18: Ευρήματα της δικανικής εξέτασης του SpiderOak

Υλισμικό	
Διεύθυνση εγκατάστασης Διεύθυνση δεδομένων εφαρμογής	C:\Program Files\SpiderOak\SpiderOak.exe C:\Users\Random\AppData\Roaming\SpiderOak
Αρχεία προς εξέταση • Αρχεία Log • object_cache • pandora_sqliite_database	Πληροφορίες για : • τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος) • την ώρα και ημερομηνία που ανακτήσαμε τα αρχεία • το «path» του φακέλου όπου αποθηκεύουμε τα αρχεία • το «path» του φακέλου από όπου προέρχονται τα αρχεία
RAM	Πληροφορίες για : • τις συσκευές που είναι συσχετισμένες με τον λογαριασμό μας • τα αρχεία που ανακτήσαμε • το μέγεθος και την ώρα και ημερομηνία που κάναμε το back up
Απεγκατάσταση	Αναφορές στην Registry Άθικτα τα δεδομένα της εφαρμογής (χρήση ειδικού προγράμματος για την διαγραφή τους).
Πρόσβαση μέσω Περιηγητή	Ευρήματα
Εξέταση του περιηγητή	Όνομα/μέγεθος αρχείων που κατεβάσαμε Ημερομηνία που έλαβε χώρα η διακίνηση των αρχείων Όνομα χρήστη Συσκευές συσχετισμένες με τον λογαριασμό
RAM	Όνομα αρχείων που κατεβάσαμε Όνομα χρήστη Συσκευές συσχετισμένες με τον λογαριασμό
Metadata	
➢ Date Created ➢ Date Modified	αποκτούν την τιμή της ημερομηνίας που ολοκληρώθηκε το «κατέβασμα» των αρχείων στο υπολογιστικό μας σύστημα.
Διαγραφή αρχείων	Ευρήματα
	Προσωρινή αποθήκευση στον φάκελο ‘Deleted Items’ Εύρεση αναφορών στα αρχεία Log.

Κεφάλαιο 9: Ψηφιακή Εγκληματολογική Εξέταση του Box

9.1. Εισαγωγή

Το Box αποτελεί μια εναλλακτική λύση για τους χρήστες που θέλουν να χρησιμοποιήσουν μια υπηρεσία cloud storage.Οι χρήστες έχουν πρόσβαση στην υπηρεσία αυτή και μέσω και κινητών συσκευών (Android,Iphone).

Το Box προσφέρει δωρεάν πρόσβαση σε λογαριασμούς με αποθηκευτικό χώρο 10 GB.Η πληρωμή συνδρομής στην εφαρμογή αυτή δεν αυξάνει μόνο τον διαθέσιμο χώρο αποθήκευσης αλλά και τις παρεχόμενες υπηρεσίες όπως το ιστορικό ενεργειών και τα αρχεία Log.Το Box είναι προσανατολισμένο προς την εταιρική χρήση. Στην εικόνα που ακολουθεί φαίνονται οι υπηρεσίες που προσφέρει η εφαρμογή.

Plans & Pricing	Personal	Starter	Business
Need help deciding? Call us today: 1-877-729-4269 Unlimited users and premier support. Get the Elite Plan.	Free Get 10GB secure storage with 250MB file upload size Sign Up Now	$5/user/month Shared workspace for your team or project Start Free Trial	$15/user/month Content collaboration and user management Start Free Trial
Users	1 User	Min 1 - Max 10	Minimum 3
Online Storage	10 or 100 GB	100 GB	1000 GB
File size limit	250 MB or 5 GB	2 GB	5 GB
Mobile Sync and Share			
Desktop Sync	✔	✔	✔
Mobile Access	✔	✔	✔
OneCloud Apps	✔	✔	✔
SSL and At Rest Encryption	✔	✔	✔
Two-Factor Authentication	✔	✔	✔
Secure Sharing	✔	✔	✔
Office Integration	✔	✔	✔
Edit Documents	✔	✔	✔
Rich File Preview	✔	✔	✔
Search	✔	✔	Full Text
Content Security and Management			
User Management			✔
Audit Logs			✔
Mobile Security Control			✔
Customized Admin Roles			

Εικόνα 9-1: Παρουσίαση υπηρεσιών του Box

Όλοι οι λογαριασμοί, ακόμα και οι δωρεάν, μας επιτρέπουν να μοιραστούμε αρχεία ή φακέλους με ένα σύνδεσμο. Το Box ενσωματώνει επίσης τη δυνατότητα να προσθέσουμε σχόλια στα αρχεία μας. Τέλος μπορούμε να αποκτήσουμε πρόσβαση στην εφαρμογή αυτή είτε μέσω του λογισμικού που μας παρέχει είτε μέσω κάποιου περιηγητή (Box, 2013).

9.2. Σκοπός/Στόχος

Ο σκοπός της παρούσας έρευνας είναι να προσδιορίσουμε τα υπολείμματα δεδομένων σε έναν υπολογιστή με Windows 7 μετά την χρήση του Box, όπως το όνομα χρήστη, ο κωδικός πρόσβασης, τα αρχεία που αποθηκεύτηκαν στο λογαριασμό, και τα σχετικά με αυτά τα αρχεία metadata.Επίσης στα πλαίσια της έρευνας χρησιμοποιούμε αντιδικανικές διαδικασίες για την σύγκριση της αρχικής και της τελικής κατάστασης του συστήματος.

9.3. Ανάλυση της υπηρεσίας Box στο περιβάλλον των Windows 7

9.3.1 Προετοιμασία

Για την συλλογή των δεδομένων που απαιτούνται για να απαντήσουμε στις ερωτήσεις της έρευνας μας δημιουργήσαμε μια εικονική μηχανή. Ακολουθώντας την μεθοδολογία που προσδιορίσαμε στο **κεφάλαιο** χρησιμοποιήσαμε το Box για την δημιουργία σημειώσεων και την επισύναψη 4 αρχείων (.pdf,.txt,.doc,jpeg). Τέλος εξετάσαμε και τις λειτουργίες συγχρονισμού που προσφέρει.

Για την προετοιμασία της έρευνας του Box,εκτός από το λογισμικό που αναλύσαμε στο κεφάλαιο, χρησιμοποιήσαμε επίσης:

- BoxSyncWindows version 1.0.0.0
- CCleaner v3.17.1689
- Eraser
- SQLite Database Browser 2.0 b1
- ESEDatabaseView v1.07
- Internet explorer 10
- Google Chrome Version 29.0.1547.66

Τέλος στα πλαίσια της προετοιμασίας έχουμε χρησιμοποιήσει την λειτουργία δημιουργίας υπογραφών του OSFORENSICS πριν και μετά την εγκατάσταση του Box ώστε να ανακαλύψουμε με ακρίβεια και αποτελεσματικότητα τις αλλαγές που έγιναν στο λειτουργικό σύστημα της εικονικής μηχανής.

9.3.2 Αναγνώριση και Συλλογή

Στο πλαίσιο αυτής της έρευνας, εντοπίστηκαν τα μέσα που θα περιέχουν τις πληροφορίες που απαιτούνται για τη διεξαγωγή της ανάλυσης. Πρόκειται για την μνήμη RAM της εικονικής μηχανής και τον σκληρό δίσκο του VM.Ακολουθώντας τις διαδικασίες που προσδιορίσαμε στο κεφάλαιο 6,ανακτήσαμε με δικανικά αποδεκτό τρόπο την μνήμη RAM και τον σκληρό δίσκο της προς εξέτασιν εικονικής μηχανής.

9.3.3 Διατήρηση

Για την έρευνα αυτή δημιουργήσαμε ένα δικανικό αντίγραφο των δυο αρχείων που αποκτήσαμε στο στάδιο της συλλογής και της ανάκτησης. Για να το πετύχουμε αυτό χρησιμοποιήσαμε το πρόγραμμα Access Data FTK Imager.

9.3.4 Ανάλυση

Στο στάδιο αυτό χρησιμοποιήσαμε μια σειρά από εργαλεία όπως το OSFORENSICS.Αρχικά θέλουμε να προσδιορίσουμε τις αλλαγές που γίνονται στο λειτουργικό των Windows με την εγκατάσταση και την απεγκατάσταση του Box.

Θέλουμε να δούμε δηλαδή αν μπορούμε να ανακαλύψουμε ότι χρησιμοποιήθηκε το πρόγραμμα αυτό ακόμα και αν έχει απεγκατασταθεί από το λειτουργικό σύστημα.

Για αυτό τον λόγο χρησιμοποιούμε το OSFORENSICS και την επιλογή της δημιουργίας και σύγκρισης υπογραφών .Στον πίνακα που ακολουθεί βλέπουμε τα αρχεία που δημιουργήθηκαν με την εγκατάσταση του Box. Στον φάκελο 'C:\Program Files\Box Sync' είναι εγκατεστημένα τα αρχεία που είναι απαραίτητα για το «τρέξιμο» της εφαρμογής.

Πίνακας 9-1: Αρχεία για την εκτέλεση του Box

C:\Program Files\Box Sync_bsddb.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_ctypes.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_ctypes_test.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_elementtree.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_hashlib.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_msi.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_testcapi.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_win32sysloader.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync_winxptheme.pyd,"3/1/2013, 7:12
C:\Program Files\Box Sync\box-left.gif,"3/1/2013, 7:12
C:\Program Files\Box Sync\box-right.gif,"3/1/2013, 7:12
C:\Program Files\Box Sync\box-top.gif,"3/1/2013, 7:12
C:\Program Files\Box Sync\BoxContextMenuHandler.dll,"7/6/2013, 9:20
C:\Program Files\Box Sync\BoxCopyHookHandler.dll,"7/6/2013, 9:20
C:\Program Files\Box Sync\BoxIconOverlayHandler.dll,"7/6/2013, 9:20
C:\Program Files\Box Sync\BoxSync.Config.xml,"3/1/2013, 7:12
C:\Program Files\Box Sync\BoxSync.exe,"7/6/2013, 9:20

Στον φάκελο 'C:\Users\ Username \AppData\Local\Box Sync' αποθηκεύονται τα αρχεία Logs.

Πίνακας 9-2: Αρχεία σχετικά με το Box

C:\Users\Random\AppData\Local\Box Sync\Logs\BoxDualInstaller.log,"16/9/2013, 10:18
C:\Users\Random\AppData\Local\Box Sync\Logs\BoxSyncAutoUpgradeMsiInstaller.log,"16/9/2013, 10:18
C:\Users\Random\AppData\Local\Box Sync\Logs\BoxSyncHelperLog__3.4.25.0_9_16_2013.log,"16/9/2013, 10:20
C:\Users\Random\AppData\Local\Box Sync\Logs\BoxSyncLog__3.4.25.0_9_16_2013.log,"16/9/2013, 10:20
C:\Users\Random\AppData\Local\Box Sync\Logs\emdata.dump,"16/9/2013, 10:20
C:\Users\Random\AppData\Local\Box Sync\Logs\ExceptionReport.log,"16/9/2013, 10:21
C:\Users\Random\AppData\Local\Box Sync\Logs\FileLockUnlockManagerLog__3.4.25.0_9_16_2013.log,"16/9/2013, 10:21
C:\Users\Random\AppData\Local\Box Sync\Logs\MissingItemsInGATRU.temp,"16/9/2013, 10:21
C:\Users\Random\AppData\Local\Box Sync\Logs\NetSparkle.log,"16/9/2013, 10:20
C:\Users\Random\AppData\Local\Box Sync\Logs\SystemInfo.txt,"16/9/2013, 10:20
C:\Users\Random\AppData\Local\Box Sync\Updates\9_16_2013_10_18_13_AM\BoxSyncAutoUpgradeMsiInstaller.log,"16/9/2013, 10:19
C:\Users\Random\AppData\Local\Box Sync\Updates\9_16_2013_10_18_13_AM\BoxSyncInstaller_Win64.msi,"16/9/2013, 10:18

Στην τοποθεσία 'C:\Users\ Username \AppData\Roaming\Box Desktop' είναι εγκαταστημένες οι SQL βάσεις δεδομένων που χρησιμοποιεί η εφαρμογή.

Πίνακας 9-3: SQL βάσεις δεδομένων της εφαρμογής

C:\Users\Random\AppData\Roaming\Box Desktop\LastLoggedInUserInfo.xml,"16/9/2013, 10:21
C:\Users\Random\AppData\Roaming\Box Desktop\UserData(pu.ru.puru@hotmail.com)\ChecksumHashFile.txt,"16/9/2013, 10:21
C:\Users\Random\AppData\Roaming\Box Desktop\UserData(pu.ru.puru@hotmail.com)\lastTwoWayMergeTime(1).txt,"16/9/2013, 10:21
C:\Users\Random\AppData\Roaming\Box Sync\GATRUIssue.yaml,"16/9/2013, 10:21
C:\Users\Random\AppData\Roaming\Box Sync\LastLoggedInUserData.yaml,"16/9/2013, 10:21
C:\Users\Random\AppData\Roaming\Box Sync\syncdb.sqlite3,"16/9/2013, 10:20
C:\Users\Random\AppData\Roaming\Box Sync\SyncSessionData.xml,"16/9/2013, 10:21
C:\Users\Random\AppData\Roaming\Box Sync\trusted_CA_root_certs.pem,"16/9/2013, 10:20
C:\Users\Random\AppData\Roaming\Box Sync\pu.ru.puru@hotmail.com\settings.xml,"16/9/2013, 10:21

Τα αρχεία που διακινούμε αποθηκεύονται στον φάκελο 'C:\Users\Username\Documents\My Box Files\. boxsync'

Πίνακας 9-4: Φάκελος αποθήκευσης αρχείων

C:\Users\Random\Documents\My Box Files\.boxsync,"16/9/2013, 10:21
C:\Users\Random\Documents\My Box Files\Box Sync ReadMe.pdf,"16/9/2013, 10:21
C:\Users\Random\Links\My Box Files.lnk,"16/9/2013, 10:21

Στους πίνακες που ακολουθούν βλέπουμε τις αλλαγές στην Registry του λειτουργικού συστήματος μετά την εγκατάσταση της εφαρμογής Box.

Πίνακας 9-5: Αλλαγές στην Registry(1)

HKEY_CLASSES_ROOT\BoxDesktop.ShellExtensions.ContextMenuHandler. BoxDesktopContextMenu,"1/1/1601, 3:00 HKEY_CLASSES_ROOT\BoxDesktop.ShellExtensions.CopyHookHandler. BoxDesktopCopyHook,"1/1/1601, 3:00

Πίνακας 9-6: Αλλαγές στην Registry(2)

HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers\ BoxDesktop\,"1/1/1601, 3:00 HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers\ BoxDesktop,"1/1/1601, 3:00 HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers\ BoxDesktop\,"1/1/1601, 3:00

9.4. Χρήση του λογισμικού της Εφαρμογής για «ανέβασμα» αρχείων

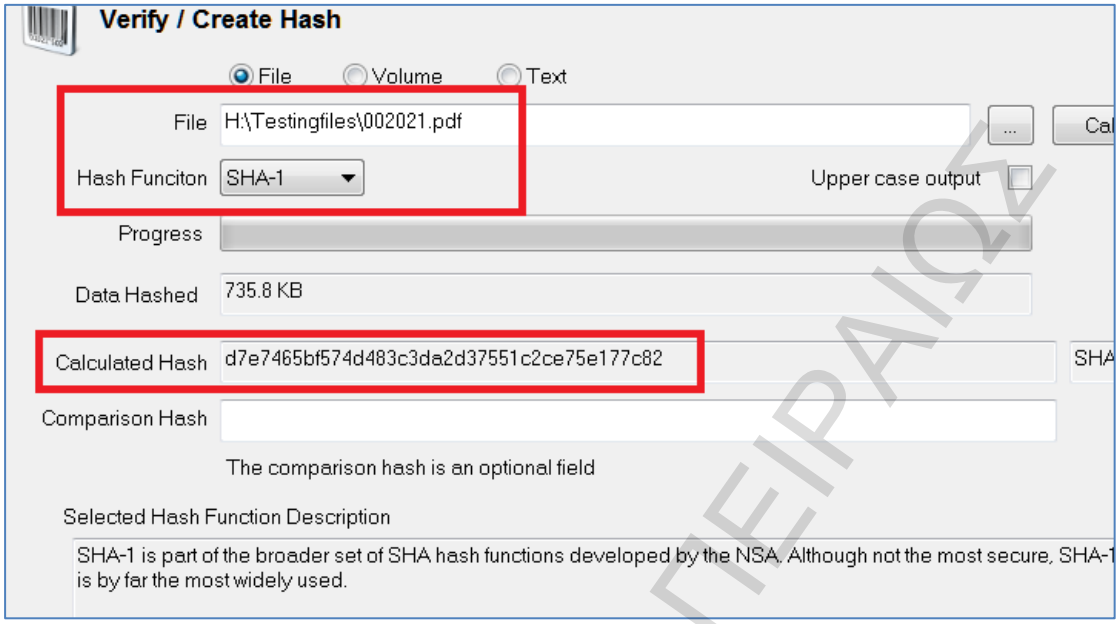
9.4.1 Εξέταση των αρχείων καταγραφής συμβάντων

Στην συνέχεια εξετάζουμε τα αρχεία Log.Βρίσκουμε αναφορές στο αρχείο που ανεβάσαμε καθώς και την ώρα που έλαβα χώρα η ενέργεια αυτή. Παρατηρούμαι όμως ότι η τιμή κατακερματισμού δεν είναι η ίδια με αυτήν που είχαμε υπολογίσει στο κεφάλαιο 6. Αυτό οφείλεται στο γεγονός ότι το Box χρησιμοποιεί την συνάρτηση κατακερματισμού SHA-1.

Πίνακας 9-7: Εξέταση αρχείων Log

[MergeTree:680:_processEvents] sync_progress: "merge, generate actions": safe_actions=[[u"<Box Upload Action(local_node=[<Local File(path='Default Sync Folder**002021.pdf**', nodeID=9,parentID=5, boxID=None, **checksum=d7e7465bf574d483c3da2d37551c2ce75e177c82**, deleted=False, deletedBeforeCurrentSync=False, usedInCurrentSync=True)>], box_node=[None], last_sync_node=[None])>"]]: delete_actions=[[]]: extra_info=[u"<Local Event('File', event_item_type=Created src_path='Default Sync Folder\\002021.pdf', dst_path='', state=Applied)>"]

Εδώ βλέπουμε ότι όντως οι κώδικες κατακερματισμού ταυτίζονται.



Εικόνα 9-2: Χρήση της συνάρτησης SHA-1

Τέλος ανακτούμε και πληροφορίες για το μέγεθος του αρχείου.

```
u'1155935561', u'name': u'Default Sync Folder', u'sequence_id': u'0',
u'type': u'folder'}],
                                        u'total_count': 2},
              u'purged_at': None,
              u'sequence_id': u'0',
              u'sha1': u'd7e7465bf574d483c3da2d37551c2ce75e177c82',
              u'shared_link': None,
              u'size': 753418,
              u'synced': True,
              u'trashed_at': None,
              u'type': u'file'},
 u'type': u'event'}
```

Εικόνα 9-3: Εξέταση αρχείων Log

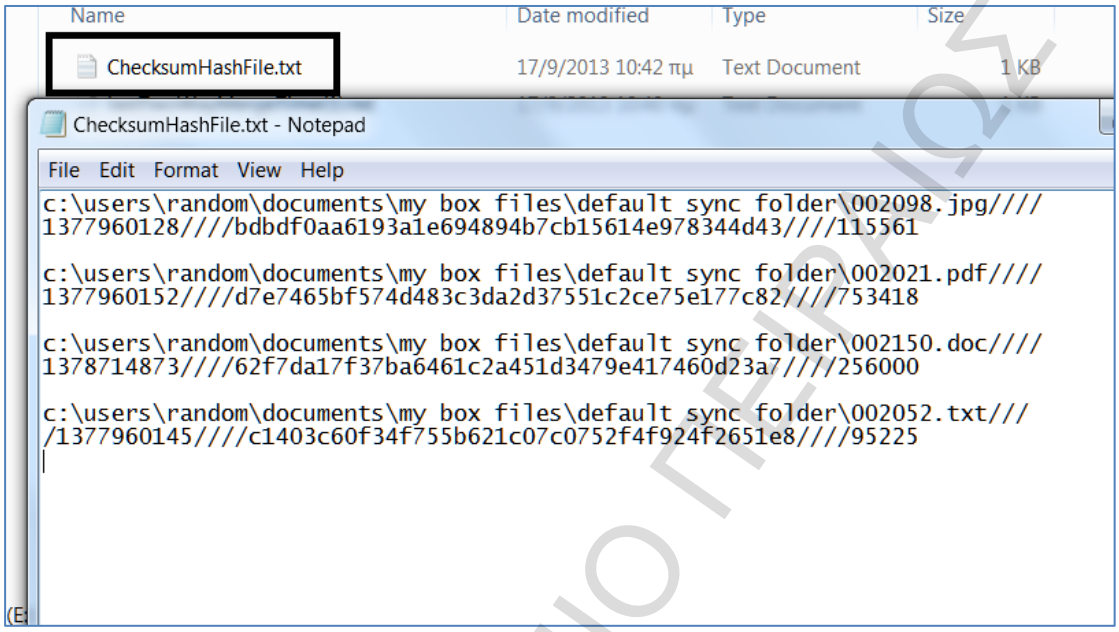
Ακόμα καταφέραμε να ανακαλύψουμε το όνομα του χρήστη ,την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον χρήστη, την ώρα και την ημερομηνία που έγινε το log in καθώς και το ID του λογαριασμού.

Πίνακας 9-8: Εξέταση αρχείων Log

```
u'created_by': {u'id': u'202734963', u'login': u'pu.ru.puru@hotmail.com', u'name':
u'Random random', u'type': u'user'},
        u'description': u'',
        u'etag': u'0',
        u'id': u'10433697451',
        u'item_status': u'active',
        u'modified_at': u'2013-09-17T00:42:15-07:00',
        u'modified_by': {u'id': u'202734963', u'login': u'pu.ru.puru@hotmail.com', u'name':
u'Random random', u'type': u'user'},
```

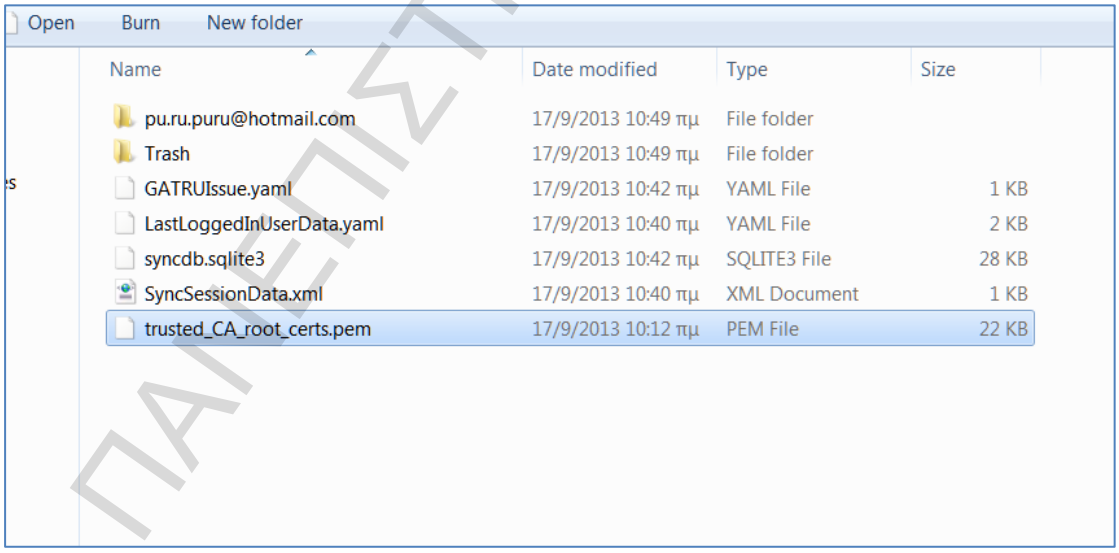
Αξίζει να επισημάνουμε ότι η ημερομηνία στην προηγούμενη εικόνα αναφέρεται στην ημερομηνία δημιουργίας του λογαριασμού.

Στον φάκελο Roaming\Box Desktop βρίσκουμε πληροφορίες για τα αρχεία που ανεβάσαμε ,όπως φαίνεται από την εικόνα που ακολουθεί.



Εικόνα 9-4: Εύρεση πληροφοριών των αρχείων

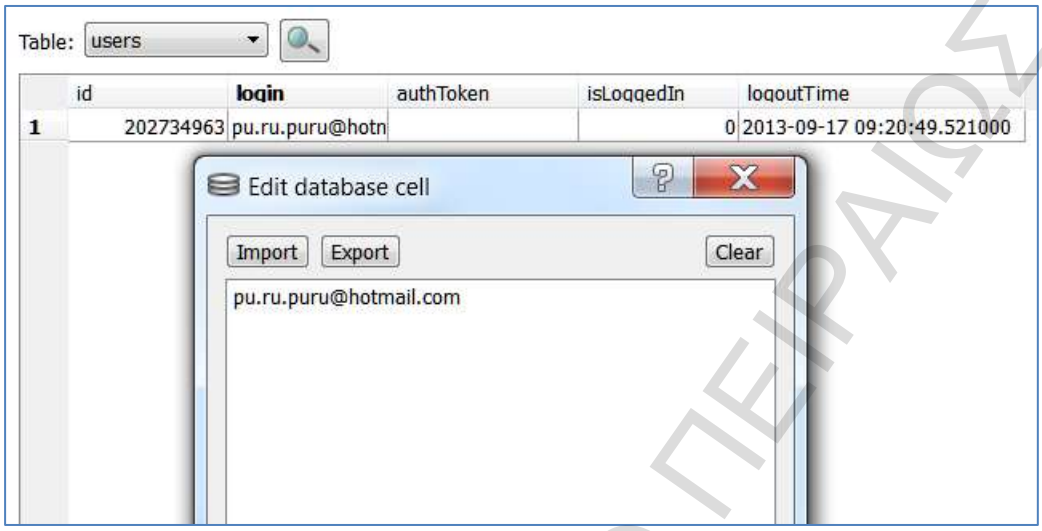
Στην εικόνα που ακολουθεί παρουσιάζονται τα αρχεία που βρίσκονται στον φάκελο Box sync.Οι φάκελοι 'pu.ru.puru@hotmail' και 'Trash' δεν παρέχουν κάποια χρήσιμη πληροφορία στο σενάριο αυτό.



Εικόνα 9-5: Παρουσίαση των προς εξέτασιν αρχείων

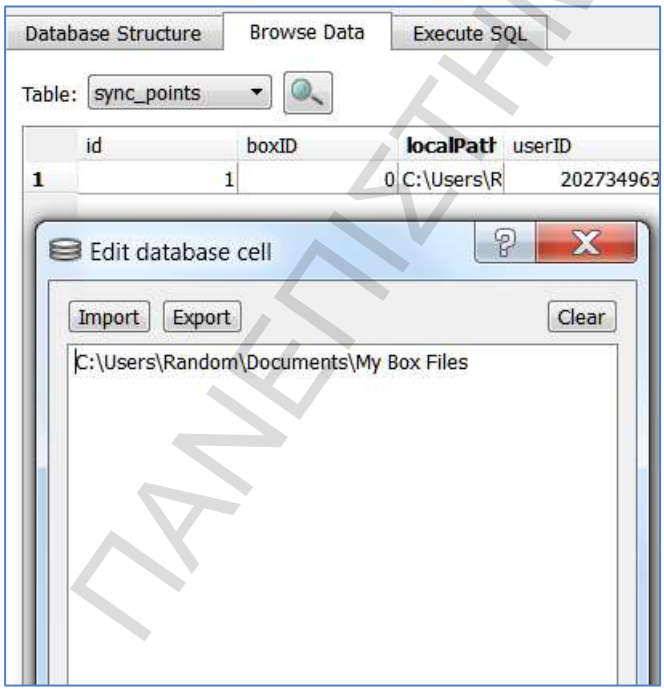
Επόμενο βήμα της έρευνας μας είναι η εξέταση της SQL βάσης δεδομένων της εφαρμογής, του αρχείου δηλαδή Syncdb.sqlite3.

Παρατηρούμαι ότι ανακαλύψαμε με επιτυχία το όνομα του χρήστη αλλά και την τελευταία φορά που κάναμε 'logout'.



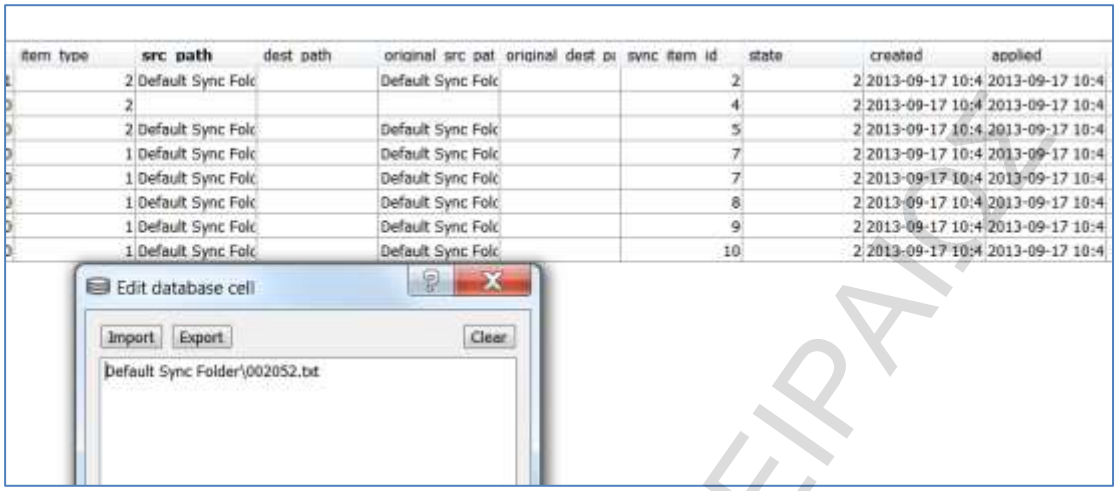
Εικόνα 9-6: Εύρεση διευθύνσεως ηλεκτρονικού ταχυδρομείου

Στην συνέχεια βρίσκουμε την διεύθυνση του φακέλου όπου αποθηκεύονται τα αρχεία που «κατεβάζουμε» τοπικά στον υπολογιστή.



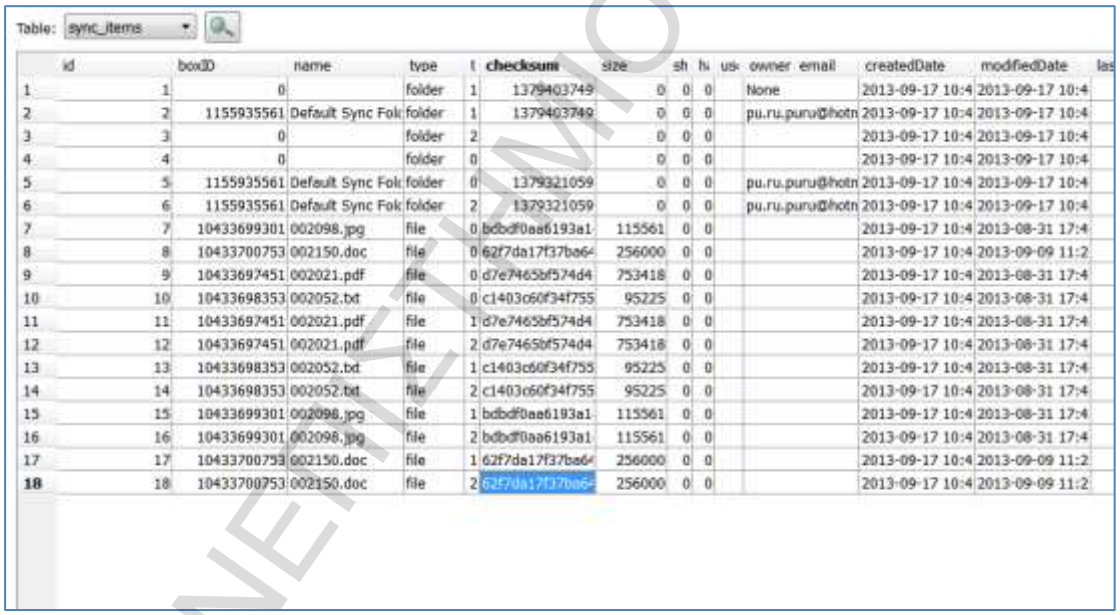
Εικόνα 9-7: Εύρεση φακέλου αποθήκευσης αρχείων

Στο Table ‘Events’ ανακαλύπτουμε τα αρχεία που «ανεβάσαμε» καθώς και την ώρα και ημερομηνία που έλαβε χώρα αυτή η ενέργεια.



Εικόνα 9-8: Ανακάλυψη των αρχείων που διακινήσαμε

Εξετάζοντας το table sync_items βρίσκουμε τις τιμές κατακερματισμού values των αρχείων.



Εικόνα 9-9: Ανακάλυψη των τιμών κατακερματισμού

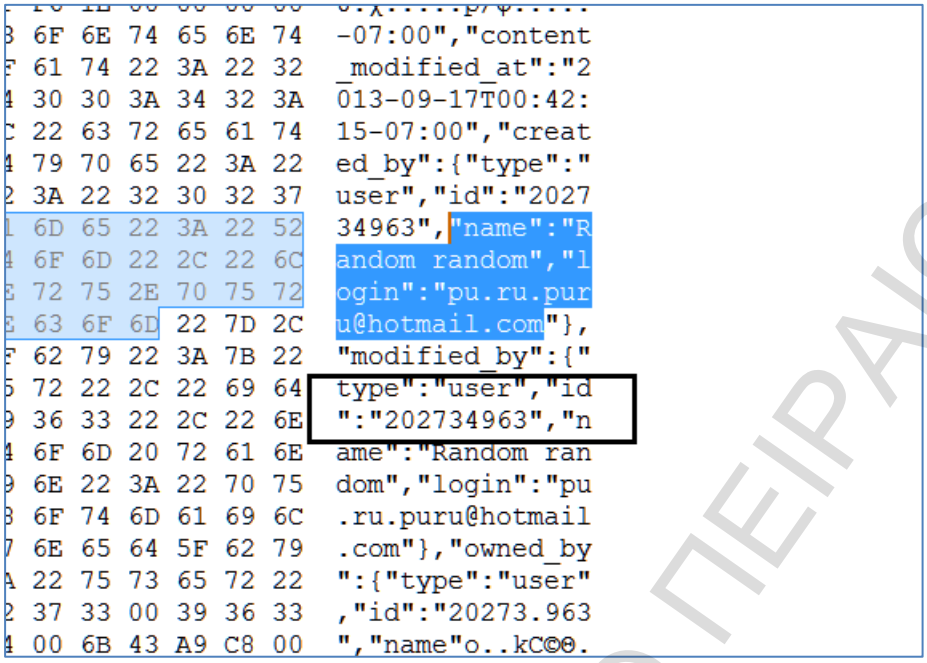
Συνοψίζοντας στον πίνακα που ακολουθεί παρουσιάζονται συνοπτικά τα ευρήματα μας στο σενάριο αυτό.

Πίνακας 9-9: Χρήση του λογισμικού του Box

Όνομα αρχείου	Ευρήματα
Logs	Πληροφορίες για: • την ενημέρωση της υπηρεσίας • το όνομα των αρχείων, το μέγεθος και τις τιμές κατακερματισμού τους
Databases • Syncdb.sqlite3	Πληροφορίες για: • τα αρχεία που «ανεβάσαμε» • (μέγεθος ,τιμή κατακερματισμού, ημερομηνία), • όνομα του χρήστη αλλά και την τελευταία φορά που κάναμε logout. • την διεύθυνση του φακέλου όπου αποθηκεύονται τα αρχεία που «κατεβάζουμε»
Roaming\Box Desktop • ChecksumHashFile.txt	Πληροφορίες για: για τα αρχεία που ανεβάσαμε (όνομα, τιμή κατακερματισμού, μέγεθος).

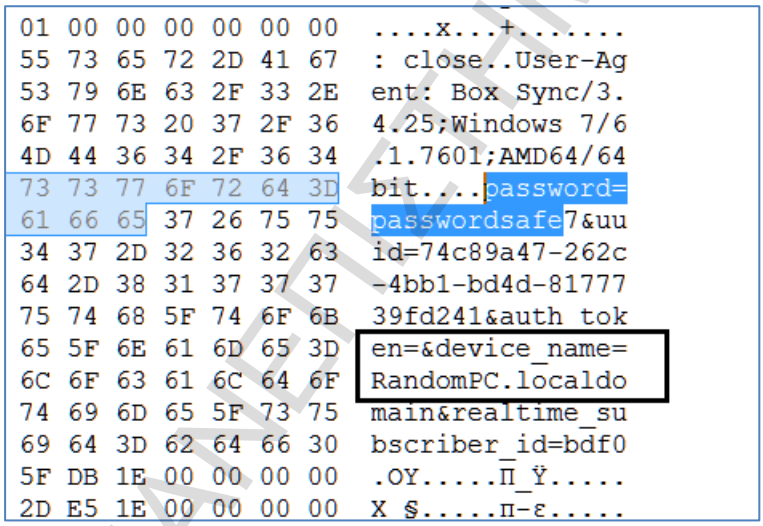
9.4.2 Εξέταση της μνήμης Ram

Στο στάδιο αυτό της έρευνας μας θα εξετάσουμε την μνήμη RAM.Καταφέραμε με επιτυχία να ανακαλύψουμε το όνομα του χρήστη, το ID του καθώς και την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό αυτόν.



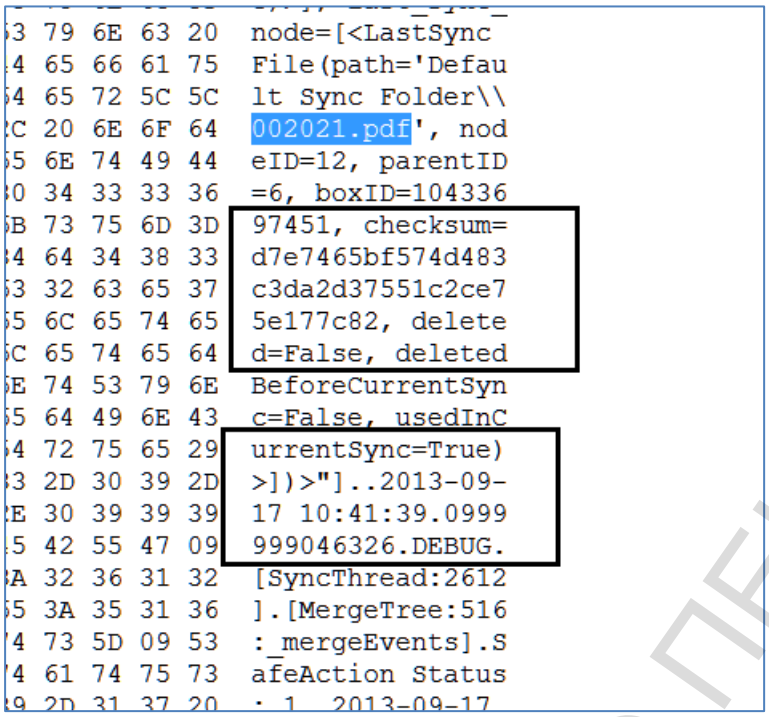
Εικόνα 9-10: Εύρεση ονόματος χρήστη,ID και e-mail στην μνήμη RAM

Αξίζει να επισημάνουμε ότι καταφέραμε να ανακαλύψουμε και τον κωδικό που εισάγαμε για να αποκτήσουμε πρόσβαση στην εφαρμογή Box.



Εικόνα 9-11: Ανακάλυψη συνθηματικού

Έπειτα επικεντρωθήκαμε στην ανακάλυψη των αρχείων που ανεβάσαμε. Με επιτυχία ανακτήσαμε τα ονόματα, τις τιμές κατακερματισμού και τις ώρες των αρχείων που «ανεβάσαμε» και ημερομηνίες που σχετίζονται με τις ενέργειες που πραγματοποιήσαμε.



Εικόνα 9-12: Εύρεση αρχείων που διακινήσαμε

Συνοψίζοντας με την εξέταση της μνήμης RAM ανακαλύψαμε πληροφορίες για:

- το όνομα χρήστη,
- το ID του χρήστη
- την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό αυτόν.
- τον κωδικό που εισάγαμε για να αποκτήσουμε πρόσβαση στην εφαρμογή Box.
- τα ονόματα και τις τιμές κατακερματισμού των αρχείων που «ανεβάσαμε»
- τις ώρες και ημερομηνίες που σχετίζονται με τις ενέργειες που πραγματοποιήσαμε.

Πίνακας 9-10: Μνήμη RAM (χρήση λογισμικού του Box)

Αρχείο	Ευρήματα
Αρχεία Log	Πληροφορίες για : • την ενημέρωση της υπηρεσίας • το όνομα των αρχείων, το μέγεθος και τις τιμή κατακερματισμού τους
Databases • Syncdb.sqlite3	Πληροφορίες για: • τα αρχεία που «ανεβάσαμε» • (μέγεθος, τιμή κατακερματισμού, ημερομηνία), • όνομα του χρήστη αλλά και την τελευταία φορά που κάναμε logout. • την διεύθυνση του φακέλου όπου αποθηκεύονται τα αρχεία που «κατεβάζουμε»
Roaming\Box Desktop\UserData • ChecksumHashFile	Πληροφορίες για: • για τα αρχεία που ανεβάσαμε (όνομα, τιμή κατακερματισμού, μέγεθος).
RAM	Πληροφορίες για: • το όνομα των αρχείων • το μέγεθος τους, • την ημερομηνία που τα «ανεβάσαμε» • πληροφορίες που σχετίζονται με τον λογαριασμό που χρησιμοποιήσαμε (όνομα χρήστη,ID χρήστη, διεύθυνση email που χρησιμοποίησε ο χρήστης).

9.5. Χρήση του λογισμικού της Εφαρμογής για την ανάκτηση αρχείων

Στο σενάριο αυτό «κατεβάσαμε» τα αρχεία που είχαμε αποθηκεύσει στον διακομιστή της εφαρμογής, τοπικά στον υπολογιστή μας .Όταν συνδεθούμε στον διακομιστή της εφαρμογής τότε αυτόματα συγχρονίζονται τα δεδομένα του φακέλου μας, που βρίσκονται τοπικά στον υπολογιστή, με αυτά του διακομιστή.

9.5.1 Εξέταση των αρχείων καταγραφής συμβάντων

Με την εξέταση των αρχείων Log ανακαλύπτουμε τα αρχεία που «κατεβάσαμε», τους κώδικες κατακερματισμού τους, το μέγεθος τους καθώς και την ημερομηνία και ώρα που τα «κατεβάσαμε».

Πίνακας 9-11: Εξέταση αρχείων Log(1)

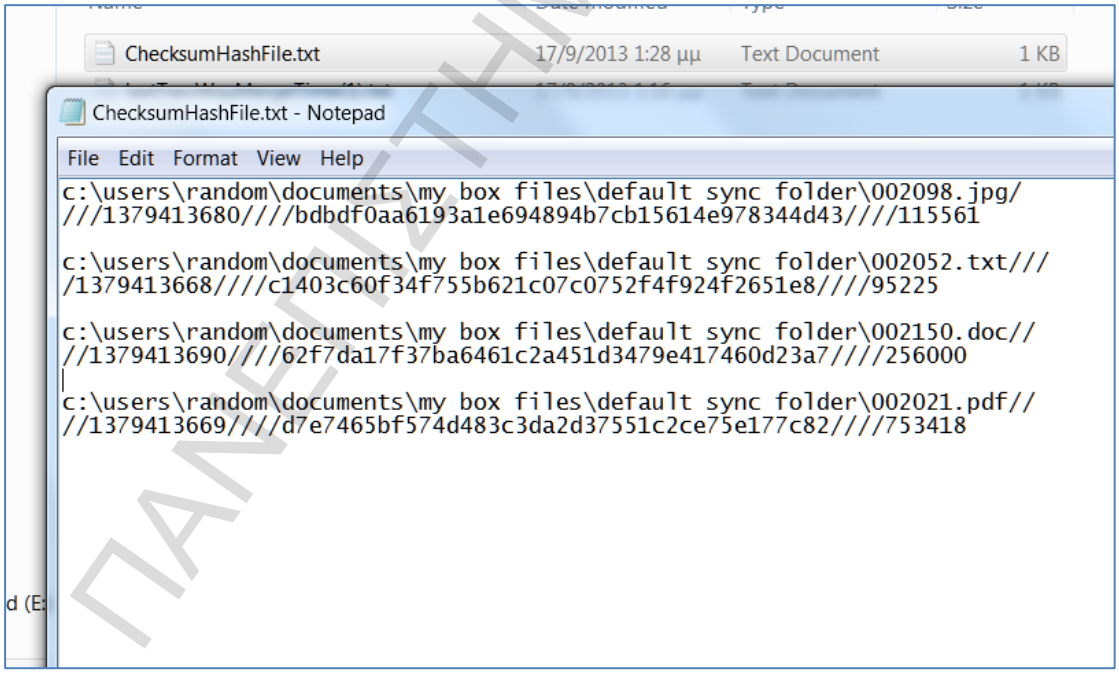
2013-09-17 13:27:56.887000083923 DEBUG [SyncThread:2748] [MergeTree:630:_processEvents] sync_progress: "pre-merge, find nodes": local_node=[**002021.pdf** 10436199249 d7e7465bf574d483c3da2d37551c2ce75e177c82 file]: box_node=[002021.pdf 10436199249 **d7e7465bf574d483c3da2d37551c2ce75e177c82** file]: last_sync_node=[002021.pdf 10436199249 d7e7465bf574d483c3da2d37551c2ce75e177c82 file]: extra_info=[u"<Local Event('File', event_item_type=Created src_path='Default Sync Folder\\002021.pdf', dst_path='', state=Applied)>"]

Τέλος ανακτήσαμε το όνομα του υπολογιστή που τα «κατεβάσαμε» καθώς και την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό αυτόν.

Πίνακας 9-12: Εξέταση αρχείων Log(2)

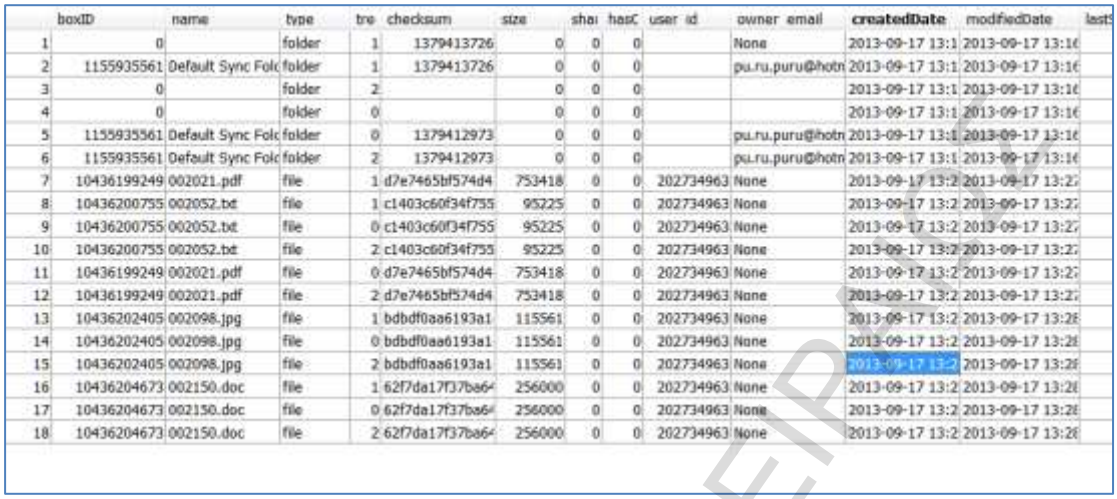
[Network:401:ConstructURLAndPostData] HTTP Post data as query string = api_key=dxn2555gstqdx8lkt48q0havqnp41oax&uuid=c32bc59d-274b-4e00-9443-34860be9ffaa&auth_token=AUTH_TOKEN&device_name=**RandomPC**.localdomain& realtime _subscriber_id=ae1ac412-8c26-4732-af52-97d6952b5eef&action=authorization&login=**pu.ru.puru%40hotmail.com**&password= PASSWORD&method=&device_id=0FABFBFF000306A9 [DEBUG]:9/17/2013;1:15:49.338 PM;{1} GetWebProxySettings2(): No auto detect setting or auto config script used. 2013-09-17 13:15:52.582999944687 DEBUG [MainThread:888]

Στην συνέχεια κατευθυνόμαστε στον φάκελο Roaming\Box Desktop\UserData. Εκεί ανακαλύπτουμε το όνομα των αρχείων, το μέγεθος καθώς και τους κώδικες κατακερματισμού τους.



Εικόνα 9-13: Εύρεση αρχείων που διακινήσαμε

Εξετάζοντας την βάση δεδομένων της εφαρμογής βρίσκουμε τα αρχεία που «κατεβάσαμε», την τιμή κατακερματισμού, το μέγεθος καθώς και την ημερομηνία που τα «κατεβάσαμε».



	boxID	name	type	tre	checksum	size	sha	hasC	user id	owner email	createdDate	modifiedDate	last
1	0		folder	1	1379413726	0	0	0		None	2013-09-17 13:1	2013-09-17 13:1	
2	1155935561	Default Sync Folc	folder	1	1379413726	0	0	0		pu.ru.puru@hotn	2013-09-17 13:1	2013-09-17 13:1	
3	0		folder	2		0	0	0			2013-09-17 13:1	2013-09-17 13:1	
4	0		folder	0		0	0	0			2013-09-17 13:1	2013-09-17 13:1	
5	1155935561	Default Sync Folc	folder	0	1379412973	0	0	0		pu.ru.puru@hotn	2013-09-17 13:1	2013-09-17 13:1	
6	1155935561	Default Sync Folc	folder	2	1379412973	0	0	0		pu.ru.puru@hotn	2013-09-17 13:1	2013-09-17 13:1	
7	10436199249	002021.pdf	file	1	d7e7465bf574d4	753418	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
8	10436200755	002052.txt	file	1	c1403c60f34f755	95225	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
9	10436200755	002052.txt	file	0	c1403c60f34f755	95225	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
10	10436200755	002052.txt	file	2	c1403c60f34f755	95225	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
11	10436199249	002021.pdf	file	0	d7e7465bf574d4	753418	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
12	10436199249	002021.pdf	file	2	d7e7465bf574d4	753418	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
13	10436202405	002098.jpg	file	1	bdbdf0aa6193a1	115561	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
14	10436202405	002098.jpg	file	0	bdbdf0aa6193a1	115561	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
15	10436202405	002098.jpg	file	2	bdbdf0aa6193a1	115561	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
16	10436204673	002150.doc	file	1	62f7da17f37ba6	256000	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
17	10436204673	002150.doc	file	0	62f7da17f37ba6	256000	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	
18	10436204673	002150.doc	file	2	62f7da17f37ba6	256000	0	0	202734963	None	2013-09-17 13:2	2013-09-17 13:2	

Εικόνα 9-14: Εξέταση της SQL βάσης δεδομένων

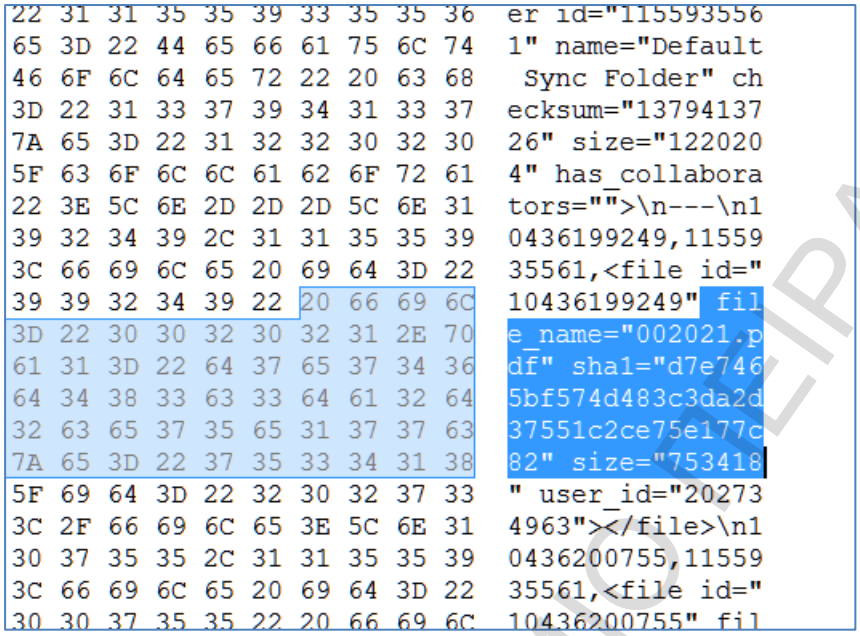
Συνοψίζοντας

Πίνακας 9-13: Χρήση του λογισμικού του Box

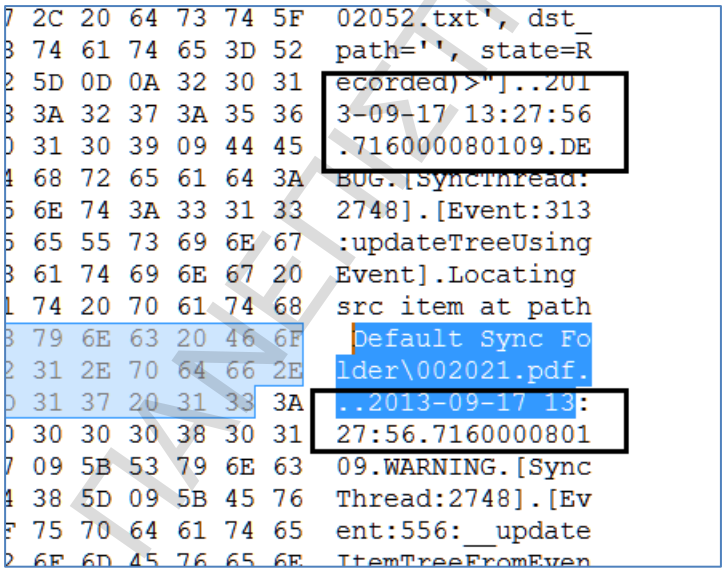
Όνομα αρχείου	Ευρήματα
Logs	Πληροφορίες για: • την ενημέρωση της υπηρεσίας • τον χρήστη του λογαριασμού • τα αρχεία που «κατέβηκαν» (ώρα, όνομα αρχείου, μέγεθος)
Roaming\Box Desktop\UserData • ChecksumashFile	Πληροφορίες για: • όνομα των αρχείων, • το μέγεθος • την τιμή κατακερματισμού τους • την ημερομηνία και ώρα που τα «κατεβάσαμε»
Databases • Syncdb.sqlite3	Πληροφορίες για: • τα αρχεία που «κατεβάσαμε» (μέγεθος, τιμή κατακερματισμού ,ημερομηνία), • Το όνομα του χρήστη αλλά και την τελευταία φορά που κάναμε logout. • την διεύθυνση του φακέλου όπου αποθηκεύονται τα αρχεία που «κατεβάζουμε»

9.5.2 Εξέταση της μνήμης RAM

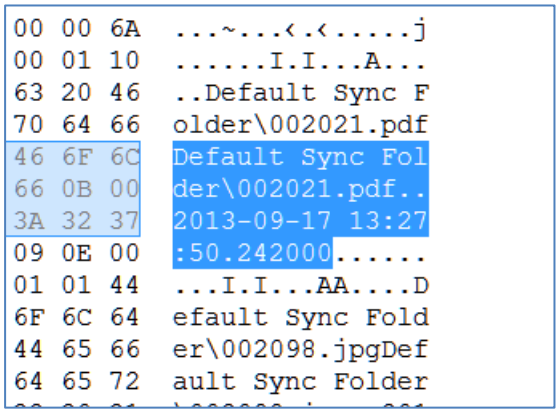
Εξετάζοντας την μνήμη RAM ανακαλύψαμε το όνομα των αρχείων ,το μέγεθος τους, την ημερομηνία που τα κατεβάσαμε καθώς τον φάκελο που αποθηκεύτηκαν.



Εικόνα 9-15: Εξέταση της μνήμης RAM(1)

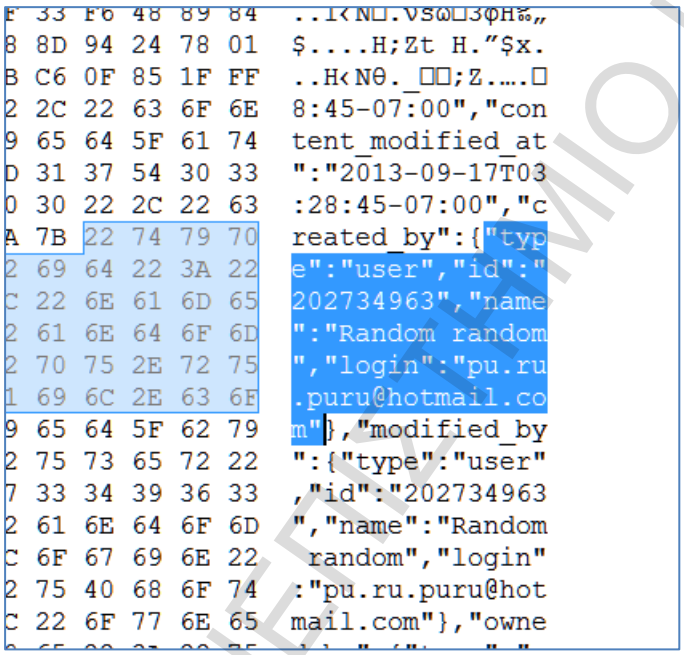


Εικόνα 9-16: Εξέταση της μνήμης RAM(2)



Εικόνα 9-17: Εξέταση της μνήμης RAM(3)

Τέλος, όπως φαίνεται από την εικόνα που ακολουθεί ανακαλύψαμε πληροφορίες που σχετίζονται με τον λογαριασμό που χρησιμοποιήσαμε.



Εικόνα 9-18: Εύρεση ID, ονόματος χρήστη και e-mail

Συνοψίζοντας

Οι πληροφορίες που ανακτήσαμε μέσω της εξέτασης της μνήμης είναι οι εξής:

- το όνομα των αρχείων ,
- το μέγεθος τους,
- ην ημερομηνία που τα κατεβάσαμε καθώς τον φάκελο που αποθηκεύτηκαν
- πληροφορίες που σχετίζονται με τον λογαριασμό που χρησιμοποιήσαμε (όνομα χρήστη,ID χρήστη, διεύθυνση email που χρησιμοποίησε ο χρήστης).

9.6. Αποτελέσματα ανάλυσης του λογισμικού της εφαρμογής Box

Στον πίνακα που ακολουθεί παρουσιάζουμε συνοπτικά τα ευρήματα μας από το σενάριο της διακίνησης αρχείων μέσω του λογισμικού της εφαρμογής

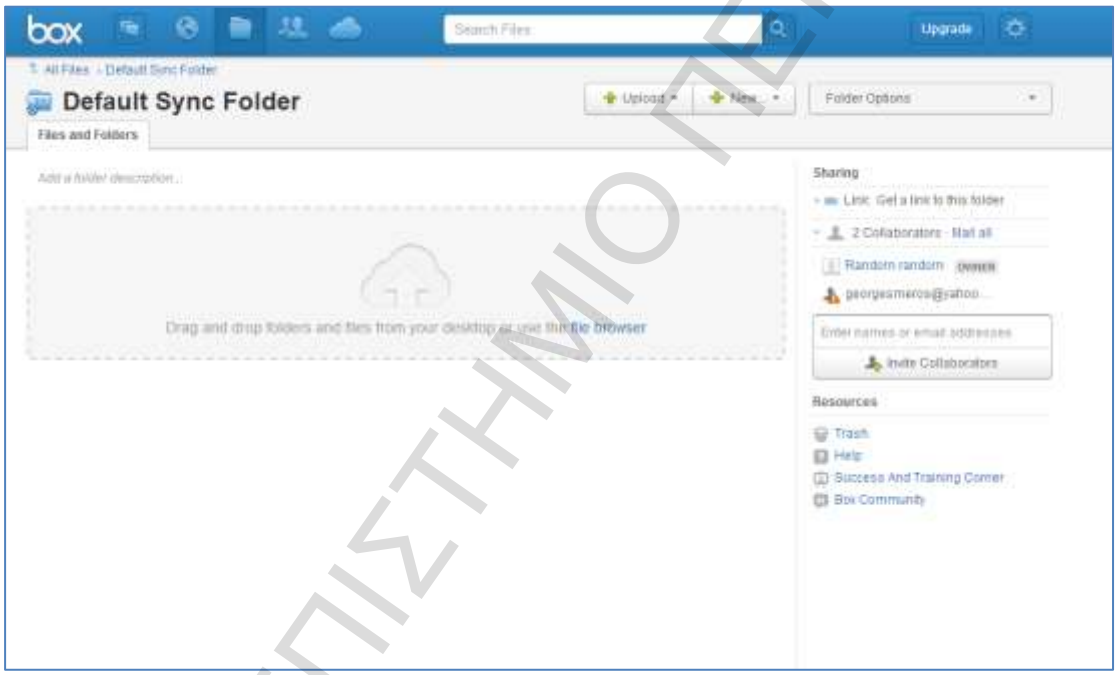
Πίνακας 9-14: Χρήση του λογισμικού της εφαρμογής

Αρχείο	Ευρήματα
Αρχεία Log	Πληροφορίες για : • τις συσκευές με τις οποίες σχετίζεται ο λογαριασμός μας • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος) • την ώρα και ημερομηνία που ανακτήσαμε τα αρχεία
Databases • Syncdb.sqlite3	Πληροφορίες για: • τα αρχεία που «κατεβάσαμε» (μέγεθος τιμή κατακερματισμού, ημερομηνία), • Το όνομα του χρήστη αλλά και την τελευταία φορά που κάναμε logout. • την διεύθυνση του φακέλου όπου αποθηκεύονται αρχεία που «κατεβάζουμε»
Roaming\Box Desktop\UserData • ChecksumHashFile	Πληροφορίες για: • όνομα των αρχείων, • το μέγεθος • την τιμή κατακερματισμού τους • την ημερομηνία και ώρα που τα «κατεβάσαμε»

RAM	Πληροφορίες για: • το όνομα των αρχείων , • το μέγεθος τους, • την ημερομηνία που τα κατεβάσαμε καθώς τον φάκελο που αποθηκεύτηκαν • πληροφορίες που σχετίζονται με τον λογαριασμό που χρησιμοποιήσαμε (όνομα χρήστη,ID χρήστη, διεύθυνση email που χρησιμοποίησε ο χρήστης).

9.7. Πρόσβαση μέσω Περιηγητή

Στο κεφάλαιο αυτό θα χρησιμοποιήσουμε το Box μέσω κάποιου περιηγητή .Στην εικόνα που ακολουθεί φαίνεται το περιβάλλον της εφαρμογής.

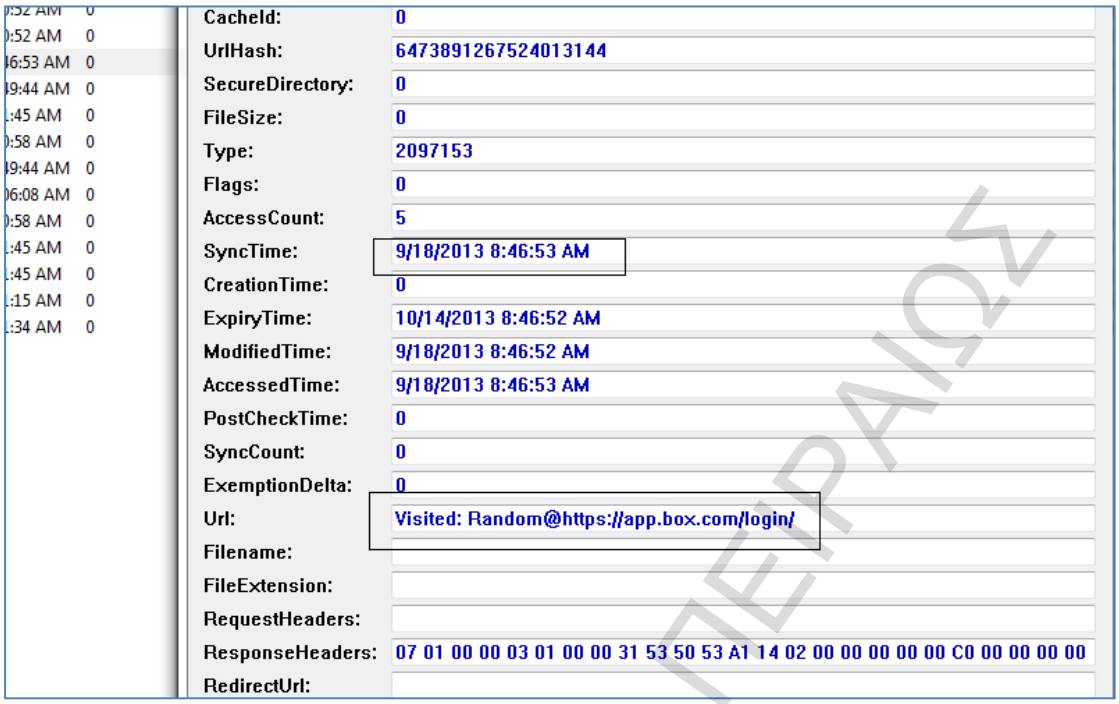


Εικόνα 9-19: Περιβάλλον εφαρμογής με την χρήση του περιηγητή

9.7.1 Χρήση του Internet Explorer

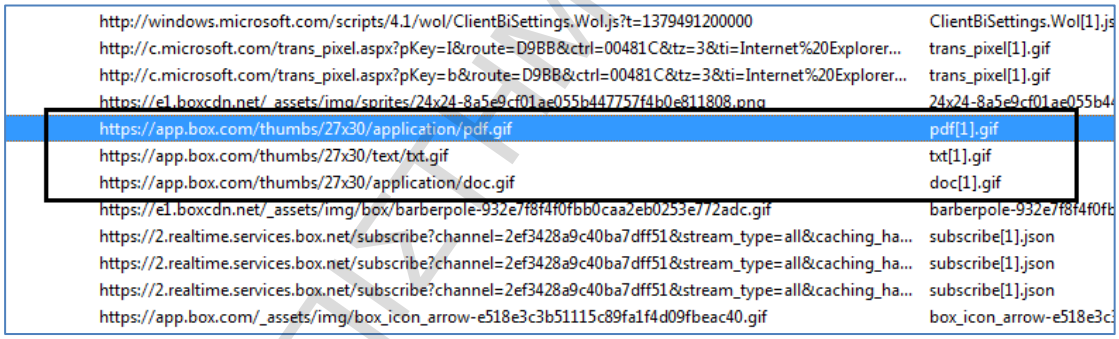
Στο σενάριο αυτό θα χρησιμοποιήσουμε τον Internet Explorer μέσω του οποίου θα «ανεβάσουμε» τα αρχεία μας στον διακομιστή της εφαρμογής. Ακολουθώντας την μεθοδολογία που έχουμε προσδιορίσει καταφέραμε να προσδιορίσουμε πολλές αναφορές που αποδεικνύουν την πρόσβαση μας στην εν λόγω υπηρεσία.

Η εξέταση του Ιστορικού του περιηγητή μας ότι όντως αποκτήσαμε πρόσβαση στην σελίδα της εφαρμογής.



Εικόνα 9-20: Εξέταση του ιστορικού του IE

Στην συνέχεια εξετάζοντας το table contents ανακαλύψαμε το είδος των αρχείων που «ανεβάσαμε».



Εικόνα 9-21: Εύρεση του είδους των αρχείων που διακινήσαμε

Τέλος η εξέταση των Cookies επιβεβαίωσε την πρόσβαση στον ιστότοπο την εφαρμογής Box.

Flags:	4
AccessCount:	26
SyncTime:	9/18/2013 8:48:22 AM
CreationTime:	9/18/2013 8:48:22 AM
ExpiryTime:	6/2/2019 4:46:49 PM
ModifiedTime:	9/18/2013 8:48:22 AM
AccessedTime:	9/18/2013 8:48:22 AM
PostCheckTime:	0
SyncCount:	0
ExemptionDelta:	0
Url:	Cookie:random@app.box.com/
Filename:	D4MX29TJ.txt
FileExtension:	

Εικόνα 9-22: Εξέταση των Cookies του IE

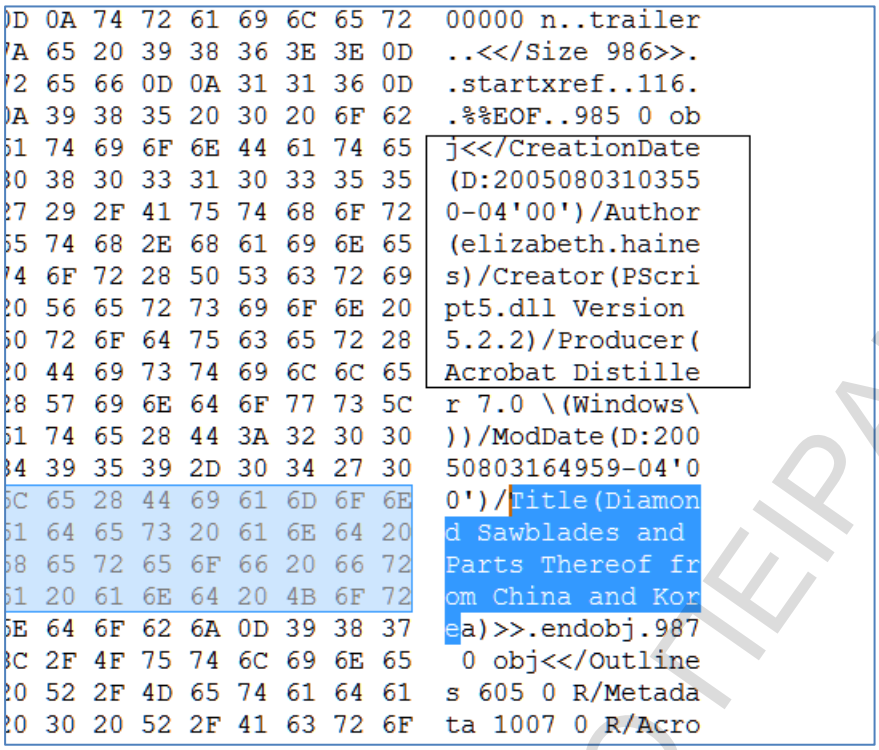
Ram

Η εξέταση της μνήμης RAM μας οδήγησε στην εύρεση ενδείξεων που επιβεβαιώνουν την χρήση της υπηρεσίας Box.

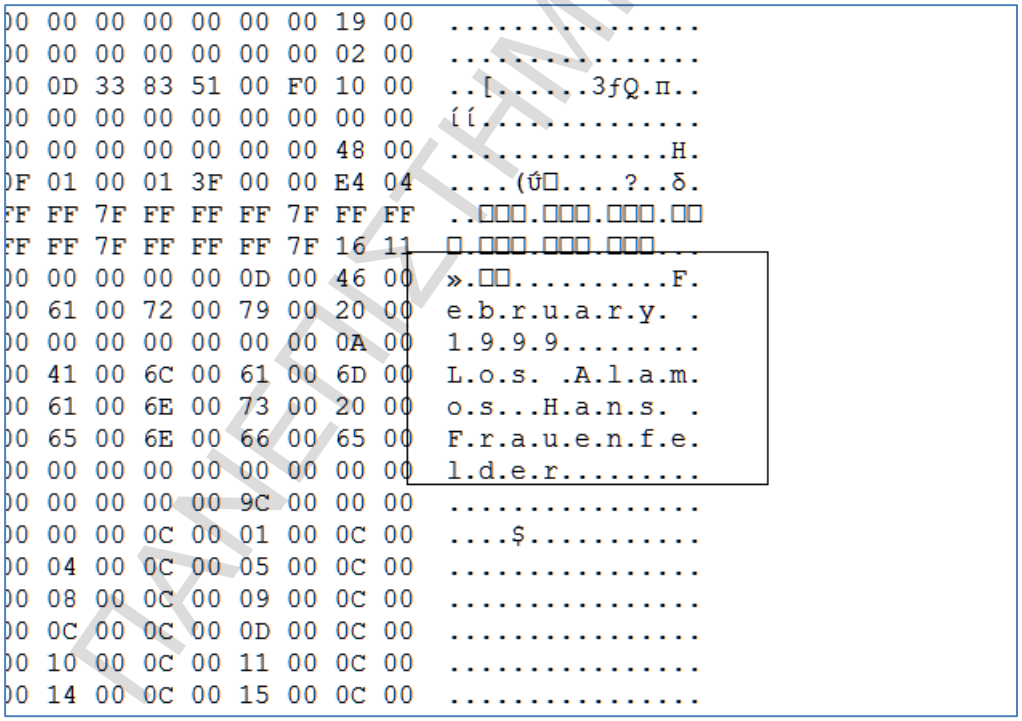
```
73 28 7B 70 6F  r=null}).css({po
6F 6C 75 74 65  sition:"absolute
30 30 70 78 22  ",left:"-1000px"
22 33 30 30 30  ,"z-index":"3000
54 6F 28 22 62  "}).prependTo("b
3D 24 6A 28 22  ody");var c=$j("
70 70 65 6E 64  <span/>").append
74 61 69 6E 65  To(this.containe
70 6C 69 63 61  r),d=Box.Applica
76 69 63 65 28  tion.getService(
6F 78 2E 41 70  "url"),.e=Box.Ap
65 74 53 65 72  plication.getSer
2D 63 61 63 68  vice("asset-cach
68 41 73 73 65  e").getFlashAsse
2E 73 77 66 5F  tURL();this.swf_
53 57 46 55 70  upload=new SWFUp
64 5F 75 72 6C  load({upload_url
69 6F 6E 61 6C  :d.addAdditional
73 2E 66 6C 61  Context(this.fla
72 6C 29 2C 66  sh_upload_url),f
```

Εικόνα 9-23: Εξέταση της μνήμς RAM(1)

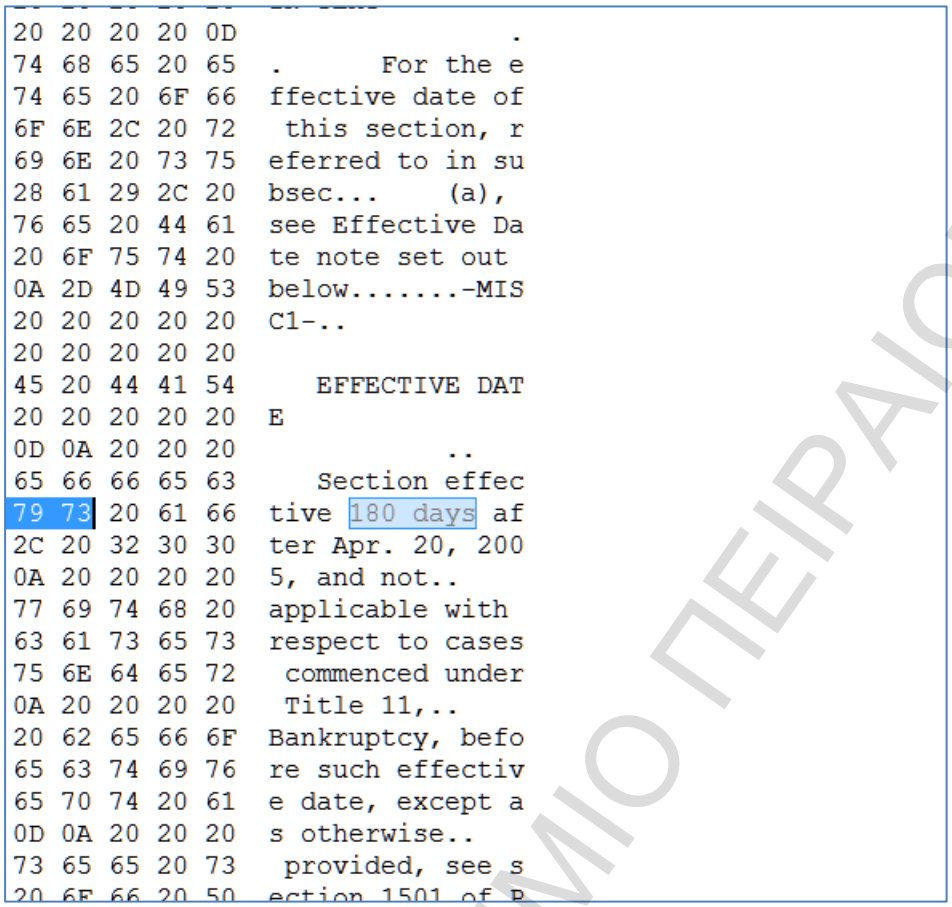
Ακόμα καταφέραμε επιτυχώς να ανακαλύψουμε τα περιεχόμενα των αρχείων που ανεβάσαμε καθώς και τα σχετικά με αυτά μεταδεδομένα.



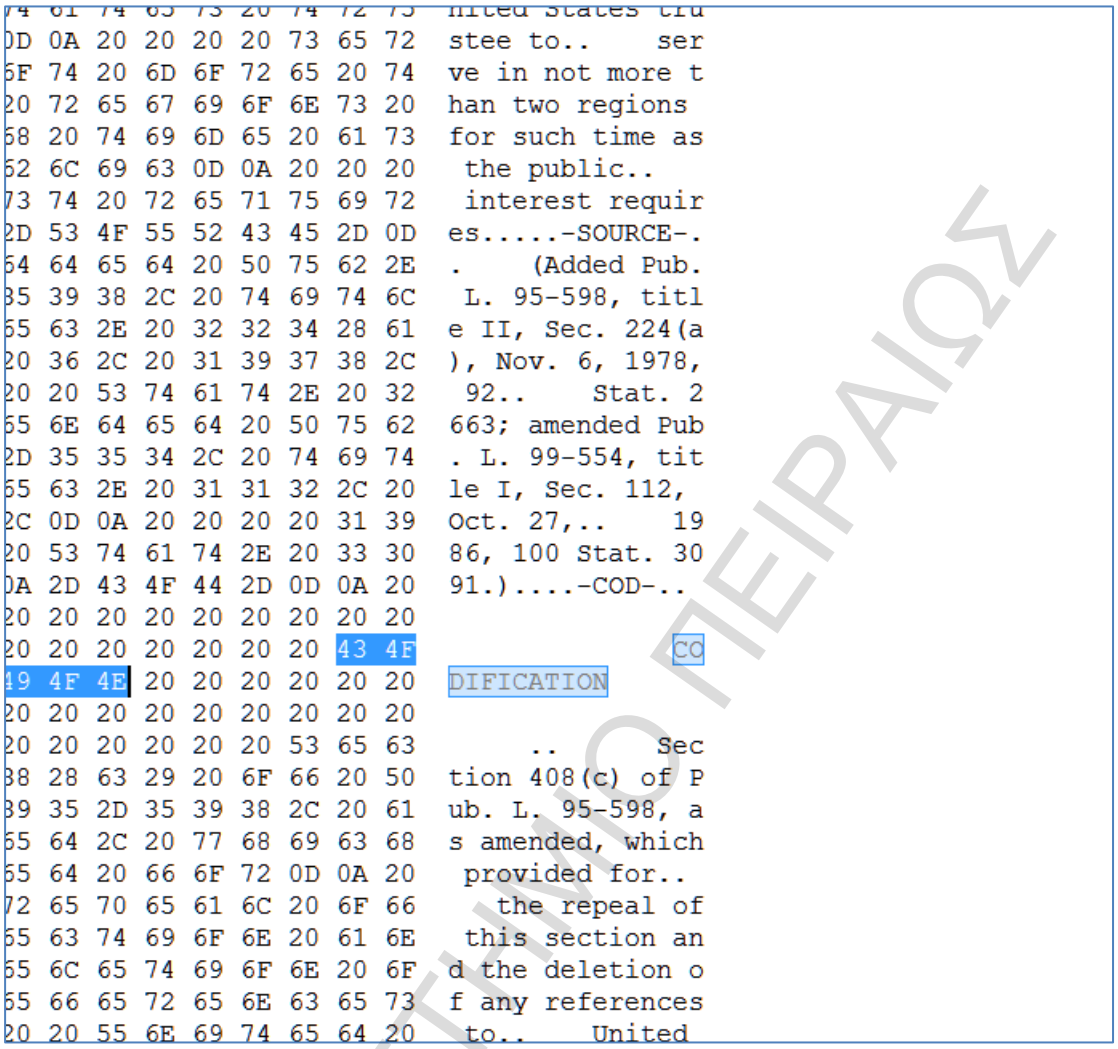
Εικόνα 9-24: Εύρεση μεταδεδομένων των αρχείων(1)



Εικόνα 9-25: Εύρεση μεταδεδομέων των αρχείων(2)



Εικόνα 9-26: Εύρεση περιεχομένων των αρχείων (1)



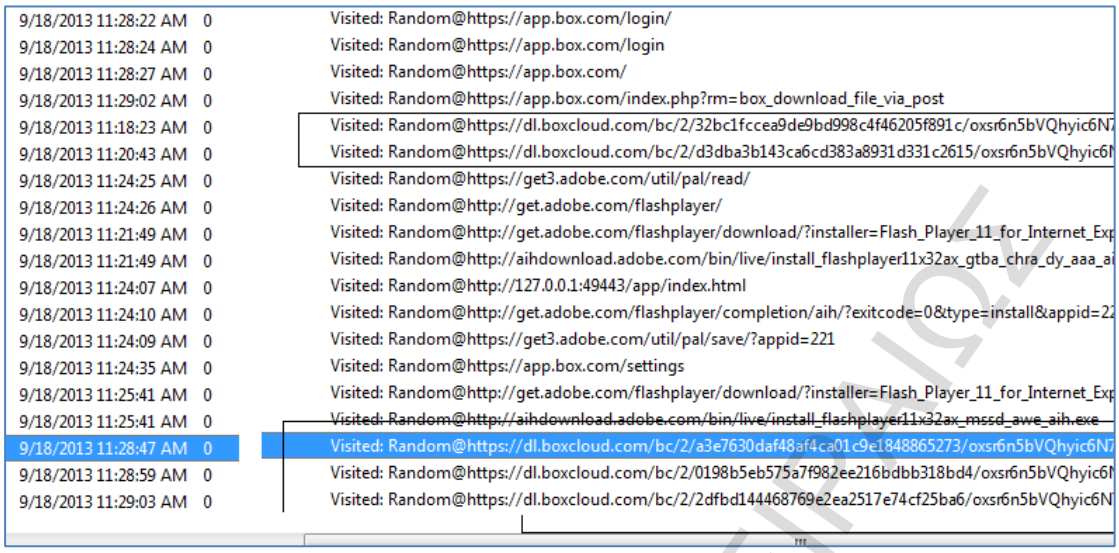
Εικόνα 9-27: Εύρεση περιεχομένων των αρχείων(2)

Τέλος δεν καταφέραμε να ανακαλύψουμε καμία πληροφορία σχετικά με το όνομα των αρχείων που διακινήσαμε, το μέγεθος ή την ημερομηνία που τα «ανεβάσαμε».

Download

Στο σενάριο αυτό, όπως και στο προηγούμενο, βρήκαμε πληροφορίες που υποδηλώνουν την πρόσβαση στον ιστότοπο της εφαρμογής. Δεν βρήκαμε καμία πληροφορία για τα αρχεία που διακινήσαμε πέρα από την ώρα που έγιναν οι ενέργειες αυτές.

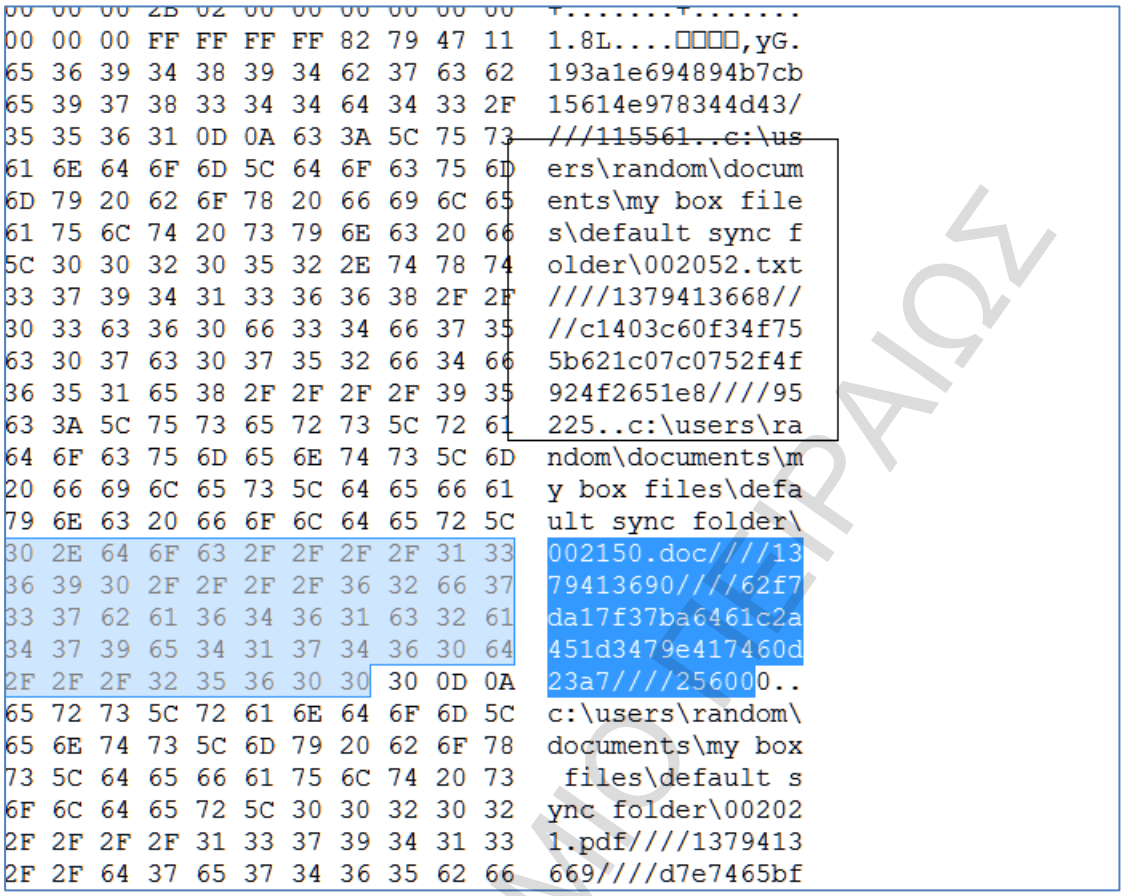
Εξετάζοντας το ιστορικό του περιηγητή ανακαλύπτουμε τις καταχωρήσεις *dl.boxcloud*,οι οποίες δημιουργούνται από το «κατέβασμα» των αρχείων που κάναμε.



Εικόνα 9-28: Ανακάλυψη των ενεργειών

Ram

Στο στάδιο αυτό, ερευνώντας την μνήμη RAM ανακαλύπτουμε τα αρχεία που κατεβάσαμε καθώς και τον κώδικα κατακερματισμού τους.

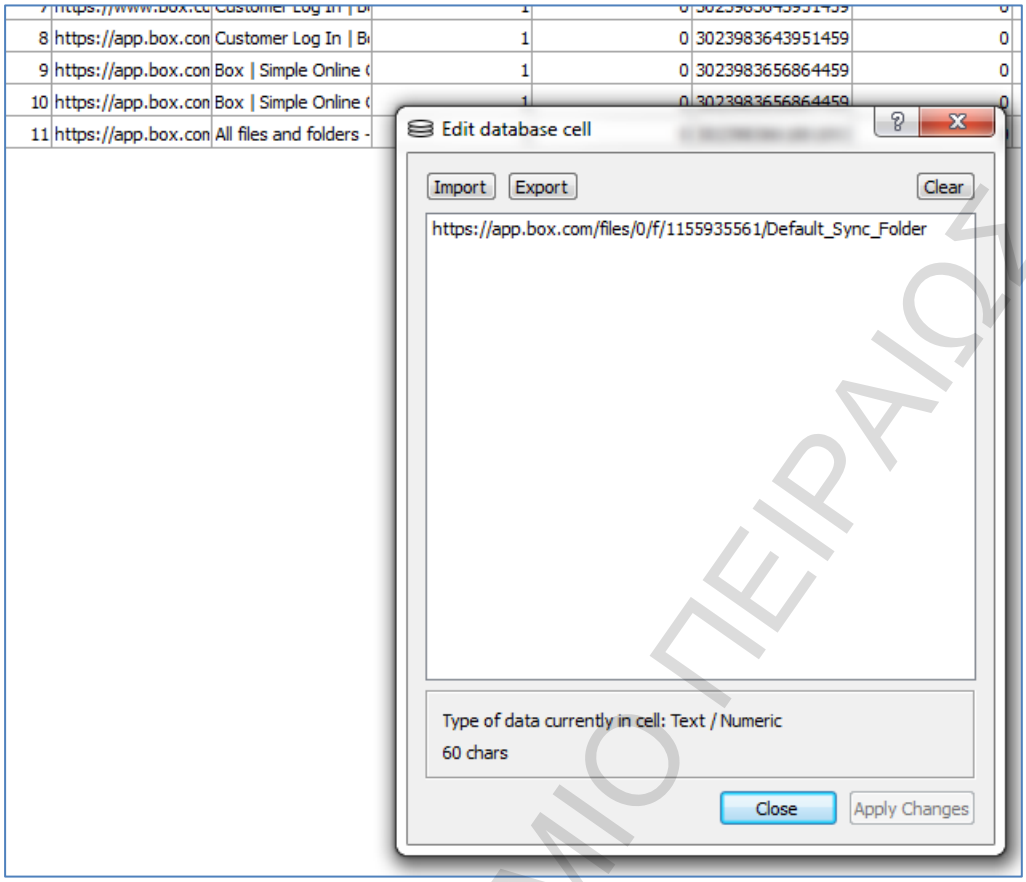


Εικόνα 9-29: Εξέταση μνήμης RAM

9.7.2 Χρήση του Google Chrome

Στο σενάριο αυτό θα χρησιμοποιήσουμε τον περιηγητή Google Chrome.Πλοηγούμαστε στον φάκελο *'C:\Users\Random\AppData\Local\Google\Chrome\Default'*.

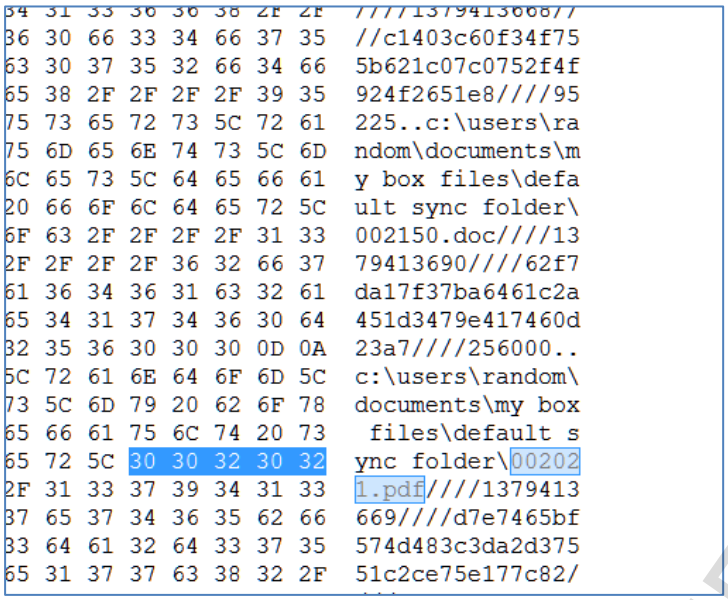
Μελετώντας τα αρχεία του περιηγητή ανακαλύπτουμε καταχωρήσεις που επιβεβαιώνουν την επίσκεψη μας στον ιστότοπο της εφαρμογής Box(Cookies,ιστορικό). Ωστόσο δεν καταφέραμε να ανακαλύψουμε κάποια άλλη πληροφορία.



Εικόνα 9-30: Εξέταση ιστορικού του GC

RAM

Με την εξέταση της μνήμης RAM βρήκαμε μόνο το όνομα των αρχείων που «ανεβάσαμε» και την τιμή κατακερματισμού τους.



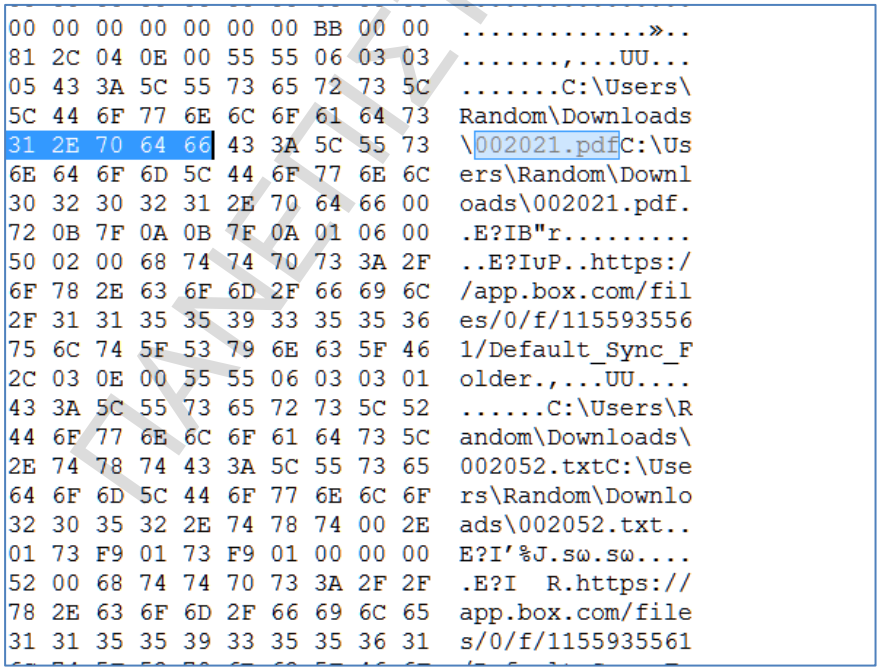
Εικόνα 9-31: Εξέταση μνήμης RAM

Download

Στο σενάριο αυτό καταφέραμε να ανακαλύψουμε τα αρχεία που «κατεβάσαμε » καθώς και το μέγεθος τους. Τέλος, μελετώντας τα αρχεία του περιηγητή ανακαλύπτουμε καταχωρήσεις που επιβεβαιώνουν την επίσκεψη μας στον ιστότοπο της εφαρμογής Box(Cookies,ιστορικό).

Ram

Στην μνήμη RAM ανακαλύψαμε το όνομα των αρχείων που «κατεβάσαμε» καθώς και τον φάκελο στον οποίο τα αποθηκεύσαμε.



Εικόνα 9-32: Εξέταση μνήμης RAM

9.7.3 Συμπεράσματα

Στον πίνακα που ακολουθεί παρουσιάζουμε συνοπτικά τα ευρήματα από την πρόσβαση στην υπηρεσία Box μέσω των δυο περιηγητών.

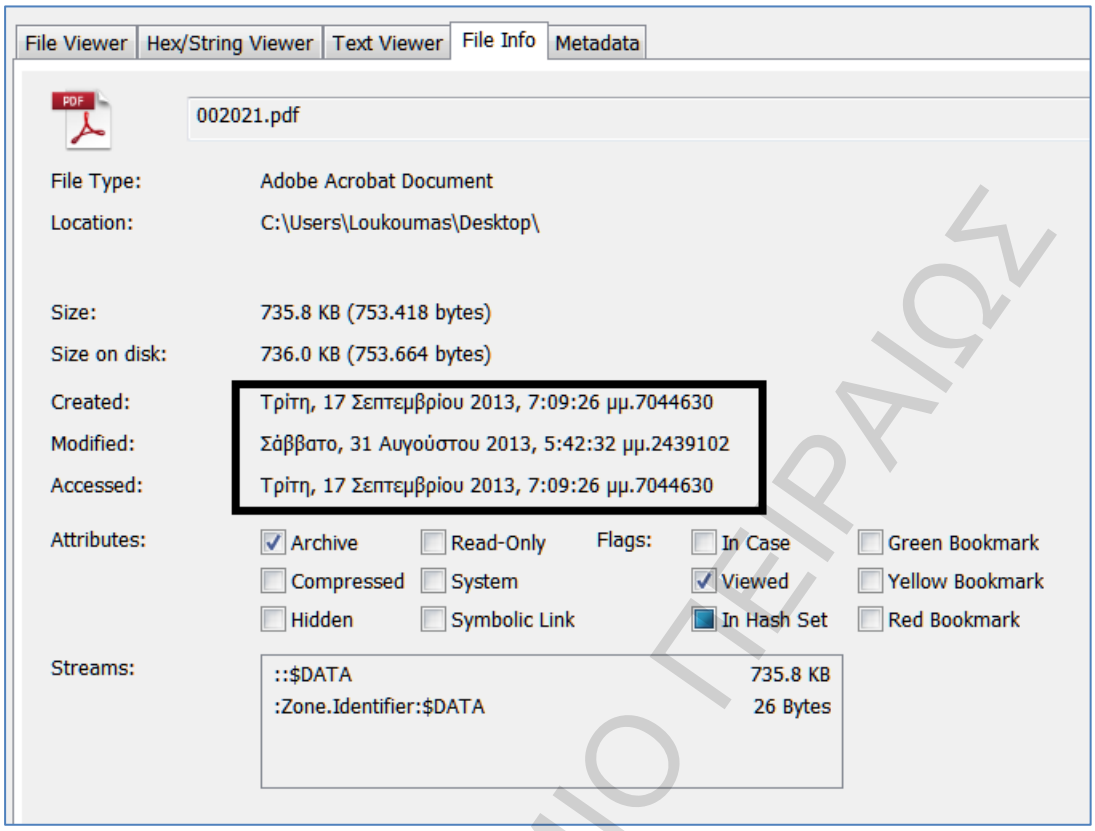
Πίνακας 9-15: Πρόσβαση στο Box μέσω περιηγητή

Περιηγητής	Ευρήματα
Internet Explorer • Cookies • History • RAM	**Upload** • ανακαλύψαμε το είδος των αρχείων που ανεβάσαμε. • περιεχόμενα των αρχείων που ανεβάσαμε καθώς και τα σχετικά με αυτά μεταδεδομένα **Download** • τα αρχεία που κατεβάσαμε καθώς και την τιμή κατακερματισμού τους
Google Chrome • Cookies • History • RAM	**Upload** • επιβεβαιώνουν την επίσκεψη μας στον ιστότοπο της εφαρμογής Box • το όνομα των αρχείων που «ανεβάσαμε» και τον κώδικα κατακερματισμού τους. **Download** • τα αρχεία που «κατεβάσαμε» καθώς και το μέγεθος τους. • το όνομα των αρχείων που «κατεβάσαμε» καθώς και τον φάκελο στον οποίο τα αποθηκεύσαμε

9.8. Μεταδεδομένα

9.8.1 Χρήση του λογισμικού

Στο σενάριο αυτό, μέσω του λογισμικού της εφαρμογής, «κατεβάσαμε» τα προς εξέταση αρχεία στην εικονική μηχανή μας. Όπως βλέπουμε στην εικόνα που ακολουθεί οι μεταβλητές Date created, Date accessed πήραν την τιμή της ημερομηνίας που ολοκληρώθηκε το «κατέβασμα». Αντίθετα η μεταβλητή Date Modified δεν επηρεάστηκε.



Εικόνα 9-33: Μεταδεδομένα αρχείων μέσω του λογισμικού

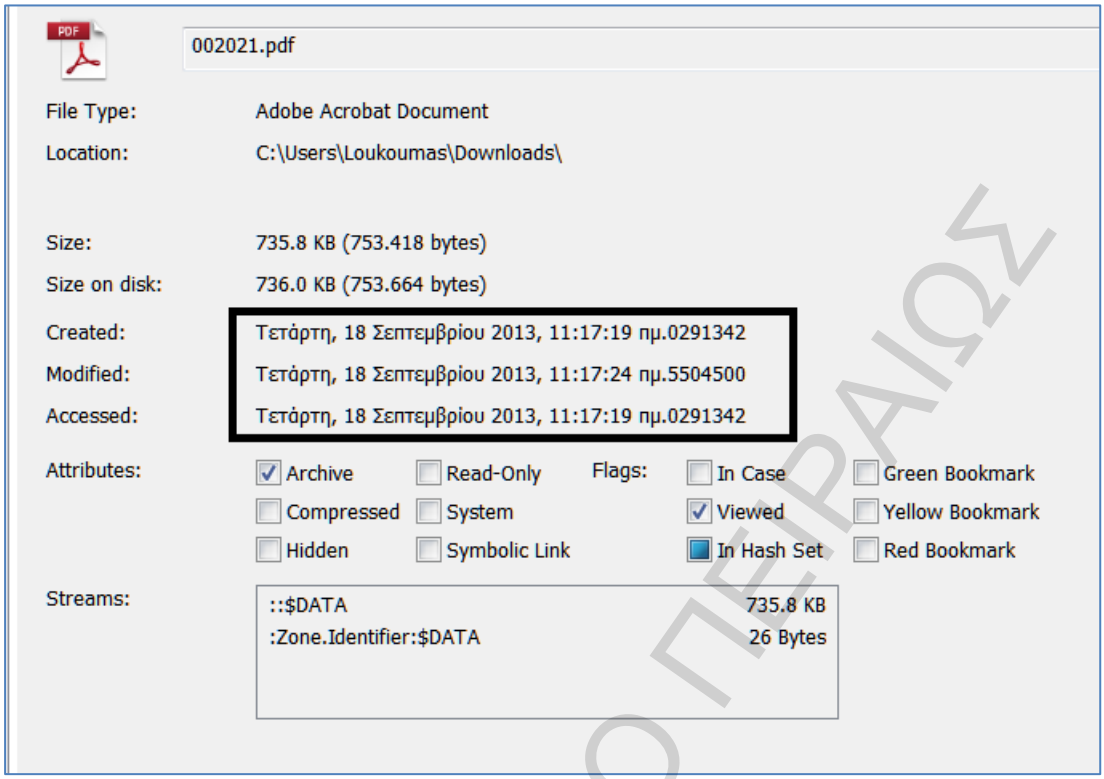
9.8.2 Χρήση Περιηγητή

Στο υποκεφάλαιο αυτό εξετάσαμε τις αλλαγές που επιφέρει στα μεταδεδομένα των αρχείων η χρήση του Box μέσω ενός περιηγητή(Internet Explorer, Google Chrome)

Οι μεταβλητές

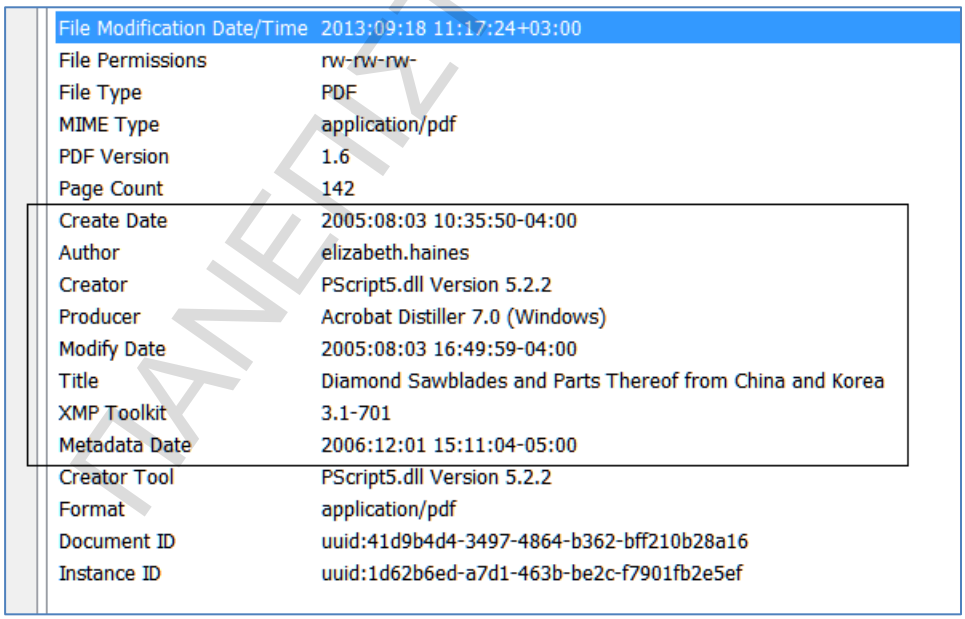
- Date Created
- Date Accessed
- Date modified

των αρχείων παίρνουν την τιμή της ημερομηνίας που ολοκληρώθηκε το «κατέβασμα» τους.



Εικόνα 9-34: Μεταδεδομένα αρχείων μέσω ενός περιηγητή

Αξίζει να επισημάνουμε ότι και στα δυο σενάρια τα υπόλοιπα μεταδεδομένα των αρχείων παρέμειναν ανεπηρέαστα.



Εικόνα 9-35: Μεταδεδομένα αρχείων

9.9. Διαγραφή

Στο υποκεφάλαιο αυτό εξετάζουμε την συμπεριφορά της εφαρμογής κατά την διαγραφή των αρχείων.

9.9.1 Πρώτο σενάριο διαγραφής αρχείων

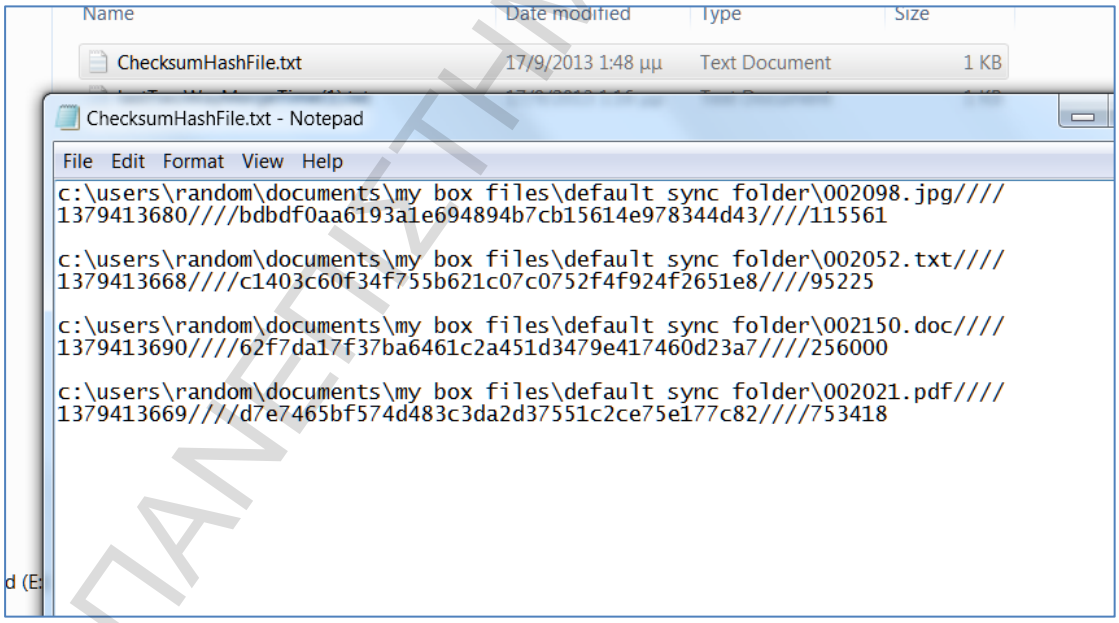
Στο πρώτο σενάριο μέσω του λογισμικού της εφαρμογής σβήσαμε τα αρχεία που είχαμε αποθηκεύσει τοπικά στην εικονική μηχανή μας. Τα αρχεία που σβήσαμε μεταφέρθηκαν στον τοπικό κάδο ανακύκλωσης ενώ μέσω του λογισμικού της εφαρμογής συγχρονίστηκε και ο λογαριασμός μας στον διακομιστή του Box

Εξετάζοντας τα αρχεία Log ανακαλύπτουμε τα αρχεία που σβήσαμε, το checksum τους καθώς και την ημερομηνία που έλαβε χώρα η ενέργεια αυτή.

Πίνακας 9-16: Εξέταση αρχείων Log

last_sync_node=[<LastSync File(path='Default Sync Folder\\002021.pdf', nodeID=13, parentID=9, boxID=10463246119, checksum=d7e7465bf574d483c3da2d37551c2ce75e177c82, deleted=True, deletedBeforeCurrentSync=False, usedInCurrentSync=True)>])>"]
2013-09-20 12:15:31.0780000686646 DEBUG [SyncThread:2196]

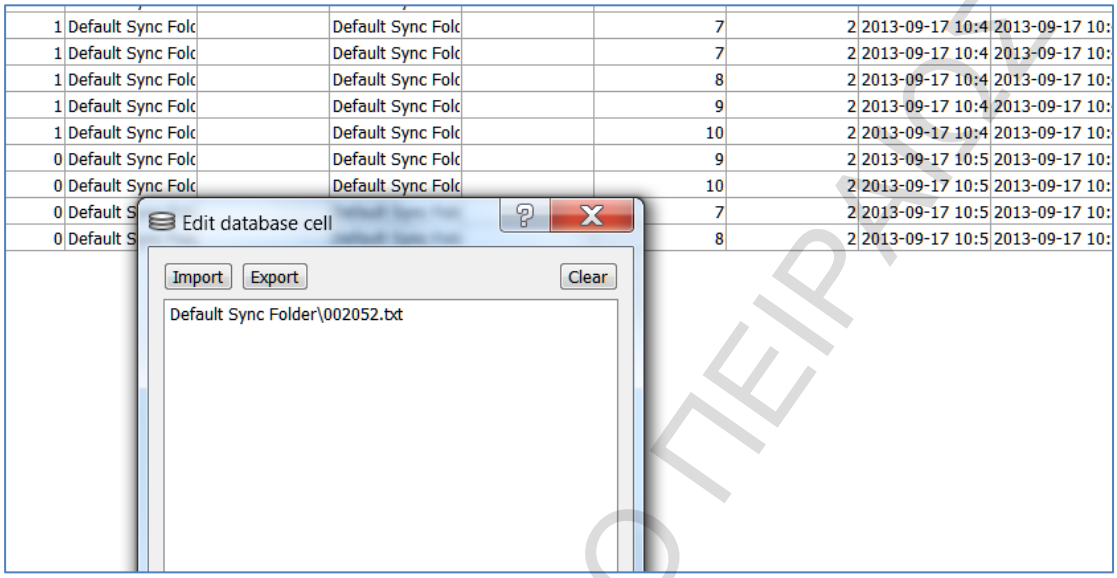
Επίσης αναφορές στα αρχεία που σβήσαμε ανακαλύπτουμε και στον φάκελο Roaming\Box Desktop\UserData όπως φαίνεται και στην εικόνα που ακολουθεί.



Εικόνα 9-36: Εύρεση διεγραμμένων αρχείων

Εξέταση της βάσης δεδομένων

Στο επόμενο βήμα θα εξετάσουμε την SQL βάση δεδομένων του λογισμικού της εφαρμογής. Στο table Sync_items δεν βρίσκουμε κάποια αναφορά στις ενέργειες που κάναμε .Ωστόσο η εξέταση του table Events μας αποκαλύπτει τα αρχεία που σβήσαμε.



Εικόνα 9-37: Εύρεση διαγραμμένων αρχείων στην βάση δεδομένων

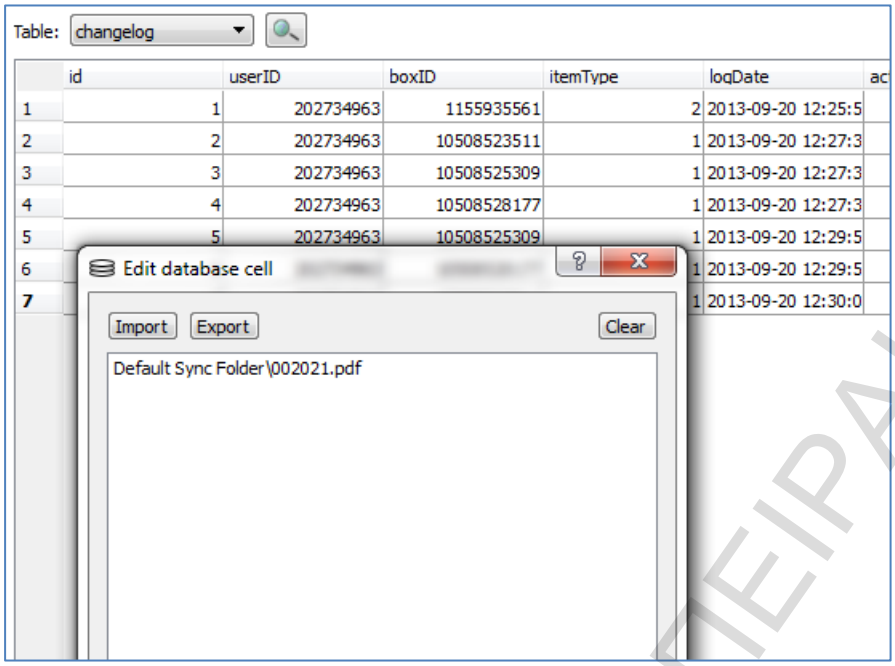
9.9.2 Δεύτερο σενάριο διαγραφής

Στο δεύτερο σενάριο χρησιμοποιώντας την εικονική μηχανή που έχουμε δημιουργήσει συνδεόμαστε στον λογαριασμό μας μέσω του λογισμικού της εφαρμογής. Στην συνέχεια χρησιμοποιώντας μια άλλη εικονική μηχανή, συνδεόμαστε στον λογαριασμό μας-είτε μέσω ενός περιηγητή είτε μέσω του λογισμικού - στο Box και διαγράφουμε τα αρχεία της επιλογής μας. Αυτό θα έχει σαν αποτέλεσμα τον συγχρονισμό του λογαριασμού μας και την διαγραφή των αρχείων και από την αρχική εικονική μηχανή.

Οι πληροφορίες που βρίσκουμε είναι παρόμοιες με το προηγούμενο σενάριο, όπως φαίνεται από την εξέταση των αρχείων Log και της βάσης δεδομένων του λογισμικού.

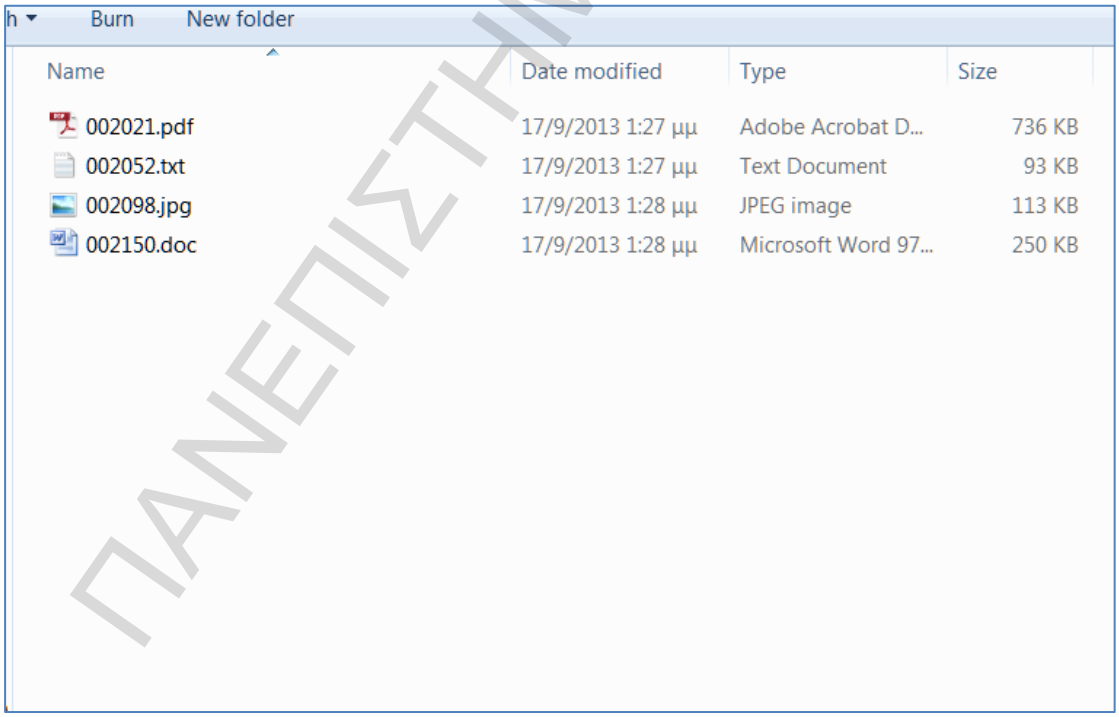
Πίνακας 9-17: Εξέταση αρχείων Log

2013-09-20 12:29:54.216000080109 DEBUG [SyncThread:3264] [SyncPoint:1382:__createDeleteEventsFromTree] sync_progress: "prepare box tree": node=[002150.doc 10508528177 62f7da17f37ba6461c2a451d3479e417460d23a7 file]: extra_info=[u"<Box Event('File', event_item_type=Deleted src_path='Default Sync Folder\\002150.doc', dst_path='None', state=Applied)>"]



Εικόνα 9-38: Εύρεση διαγραμμένων αρχείων στην βάση δεδομένων

Η μοναδική-και αξιοσημείωτη- αναφορά με το προηγούμενο σενάριο είναι το γεγονός ότι τα αρχεία που διαγράψαμε τώρα βρίσκονται αποθηκευμένα στην φάκελο Roaming\Box Sync\Trash\ pu.ru.puru@hotmail.com της εικονικής μας μηχανής.



Εικόνα 9-39: Εύρεση διαγραμμένων αρχείων στον φάκελο Trash

9.9.3 Διαγραφή αρχείων μέσω περιηγητή

Ανεξάρτητα από τον περιηγητή που θα χρησιμοποιήσουμε τα αρχεία που διαγράφουμε αποθηκεύονται στον φάκελο 'Trash'.Θα πρέπει χειροκίνητα να μεριμνήσουμε για την εκ νέου διαγραφή τους από τον φάκελο αυτόν. Όμως όπως φαίνεται και από την εικόνα που ακολουθεί έχουμε την δυνατότητα να ανακτήσουμε τα αρχεία αυτά εντός 14 ημερών.

Εικόνα 9-40: Ο φάκελος Trash του περιηγητή

9.10. Απεγκατάσταση του προγράμματος

Τέλος αναλύσαμε την συμπεριφορά του Box κατά την διαδικασία της απεγκατάστασης του με την σύγκριση των υπογραφών του συστήματος.

Στο πρώτο σενάριο απεγκαταστήσαμε το πρόγραμμα μέσω του Πίνακα Ελέγχου του λειτουργικού συστήματος .Με τον τρόπο αυτό βρήκαμε πληθώρα αναφορών του προγράμματος Box στην Registry των Windows ενώ και ο φάκελος " My Box Files " παρέμεινε ανέπαφος.

Στο δεύτερο σενάριο για την απεγκατάσταση του Box χρησιμοποιήσαμε το πρόγραμμα CC Cleaner .Αφού απεγκαταστήσαμε το Box χρησιμοποιήσαμε την επιλογή του Registry Scan για να αφαιρέσουμε τυχόν εναπομείναντες αναφορές στο Box από την Registry των Windows. Σε αυτό το σενάριο βρήκαμε και πάλι αναφορές στην Registry ενώ και ο φάκελος " My Box Files " παρέμεινε ανέπαφος.

Τέλος στο τρίτο σενάριο συνδυάσαμε το CC Cleaner με το Eraser. Καταφέραμε και σβήσαμε εντελώς τον φάκελο 'My Box Files' ωστόσο συνέχισαν να υπάρχουν εναπομείναντες αναφορές στο 'Box ' στην Registry των Windows.

Συνοψίζοντας μετά την απεγκατάσταση του Box μπορούμε με ασφάλεια να υποστηρίξουμε ότι ο ερευνητής μπορεί να ανακαλύψει δεδομένα που αποδεικνύουν την χρήση του-στην χειρότερη περίπτωση- και στην καλύτερη να ανακαλύψει και τα ίδια τα αρχεία που διακινήσαμε μέσω της εφαρμογής Box.

Πίνακας 9-18: Συμπεράσματα από την απεγκατάσταση του Box

Σενάριο	Ευρήματα
Σενάριο 1: Απλή απεγκατάσταση	Αναφορές στην Registry Άθικτος ο φάκελος 'My Box Files'
Σενάριο 2:Χρήση CC Cleaner	Αναφορές στην Registry (λιγότερες από το σενάριο 1) Άθικτος ο φάκελος 'My Box Files'
Σενάριο 3:Χρήση CC cleaner και Eraser	Αναφορές στην Registry (ίδιες με το σενάριο 2)

9.11. Παρουσίαση

Στον επόμενο πίνακα συνοψίζουμε τα ευρήματα μας από την δικανική εξέταση της υπηρεσίας Box.

Πίνακας 9-19: Ευρήματα δικανικής εξέτασης του Box

Υλισμικό	Ευρήματα
Διεύθυνση εγκατάστασης Διεύθυνση δεδομένων εφαρμογής	Program Files (x86)\Box\ C:\Users\ Username \AppData\Local\Box Sync C:\Users\ Username \AppData\Roaming\Box Desktop C:\Users\Username\Documents\MyBoxFiles\.boxsyn
Απεγκατάσταση	Αναφορές στην Registry Άθικτα τα δεδομένα της εφαρμογής. (χρήση ειδικού προγράμματος για την διαγραφή τους)
Αρχεία προς εξέταση	Ευρήματα
Logs	Πληροφορίες για : • τα αρχεία που διακινήσαμε καθώς και πληροφορίες για αυτά (μέγεθος) • την ώρα και ημερομηνία που ανακτήσαμε τα αρχεία
Databases • Syncdb.sqlite3	Πληροφορίες για: • τα αρχεία που «κατεβάσαμε/ανεβάσαμε» • (μέγεθος, τιμή κατακερματισμού, ημερομηνία), • Το όνομα του χρήστη αλλά και την τελευταία φορά που κάναμε logout • την διεύθυνση του φακέλου όπου αποθηκεύονται τα αρχεία που «κατεβάζουμε»
Roaming\Box Desktop\UserData • ChecksumHashFile	Πληροφορίες για: το όνομα των αρχείων, το μέγεθος, τον κώδικα κατακερματισμού τους

RAM	Πληροφορίες για: • το όνομα χρήστη, • το ID του χρήστη • την διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με τον λογαριασμό αυτόν. • τον κωδικό που εισάγαμε για να αποκτήσουμε πρόσβαση στην εφαρμογή Box. • τα ονόματα και τις τιμές κατακερματισμού των αρχείων που «ανεβάσαμε»/»κατεβάσαμε» • τις ώρες και ημερομηνίες που σχετίζονται με τις ενέργειες που πραγματοποιήσαμε.
Πρόσβαση μέσω Browser	Ευρήματα
Εξέταση των αρχείων του περιηγητή	**Upload** το είδος των αρχείων που «ανεβάσαμε». **Download** καταχωρήσεις που επιβεβαιώνουν την επίσκεψη μας στον ιστότοπο της εφαρμογής Box
RAM	**Upload** περιεχόμενα των αρχείων που «ανεβάσαμε» καθώς και τα σχετικά με αυτά μεταδεδομένα το όνομα των αρχείων που «διακινήσαμε» και τις τιμές κατακερματισμού τους. **Download** τα αρχεία που κατεβάσαμε καθώς και τις τιμές κατακερματισμού τους
Μεταδεδομένα	Ευρήματα
• Date Created • Date Accessed • Date modified	παίρνουν την τιμή της ημερομηνίας που ολοκληρώθηκε το «κατέβασμα» τους.
Διαγραφή Αρχείων	Ευρήματα
Log files	τα αρχεία που σβήσαμε, τις τιμές κατακερματισμού καθώς και την ημερομηνία που έλαβε χώρα η ενέργεια αυτή.

Databases • Syncdb.sqlite3	αποκαλύπτει τα αρχεία που διαγράψαμε
Διαγραφή αρχείων μέσω περιηγητή	Προσωρινή αποθήκευση στον φάκελο 'Trash' Δυνατότητα ανάκτησης των αρχείων αυτών εντός 14 ημερών

Κεφάλαιο 10: Συμπεράσματα Έρευνας

Σε αυτό το κεφάλαιο θα εξετάσουμε αν καταφέραμε να απαντήσουμε στα ερωτήματα που είχαμε θέση στην αρχή της έρευνας μας.

10.1. Στόχοι έρευνας

Όπως προείπαμε το επίκεντρο αυτής της έρευνας είναι να διαπιστωθεί εάν υπάρχουν τυχόν υπολείμματα δεδομένων από την χρήση των Cloud υπηρεσιών αποθήκευσης σε ένα υπολογιστικό σύστημα με λειτουργικό σύστημα Windows 7.Στο πρώτο κεφάλαιο καθορίσαμε τους στόχους της έρευνας:

Στόχος 1*:Να προσδιοριστεί το θεωρητικό υπόβαθρο όσον αφορά την ψηφιακή εγκληματολογία και την τεχνολογία Cloud Storage.*

Στο κεφάλαιο 2 αναλύσαμε την ψηφιακή εγκληματολογία, τις αρχές και τους κανόνες που την διέπουν. Στο κεφάλαιο 3 προσδιορίσαμε την τεχνολογία cloud και το πώς επηρεάζει την ψηφιακή εγκληματολογία. Στο κεφάλαιο 4 αναλύσαμε και εξετάσαμε την συμπεριφορά της μνήμης Ram καθώς και τα δεδομένα που μπορούμε να ανακαλύψουμε σε αυτήν.

Στόχος 2*: Να αναπτύξουμε ένα πλαίσιο ψηφιακής εγκληματολογικής ανάλυσης που θα βοηθήσει τους ερευνητές να ακολουθούν μια τυποποιημένη διαδικασία, όταν αναλαμβάνουν την εγκληματολογική ανάλυση των Cloud υπηρεσιών αποθήκευσης.*

Στο κεφάλαιο 5 προσδιορίσαμε την μεθοδολογία που προτείνουμε.

Στόχος 3*: Να εξετάσουμε δημοφιλείς Cloud υπηρεσίες αποθήκευσης:Evernote, SpiderOak, Box και να διαπιστώσουμε να υπάρχουν τυχόν υπολείμματα δεδομένων που να συμβάλουν στην εγκληματολογική έρευνα και ανάλυση.*

Στα κεφάλαια 7,8,9 εξετάσαμε τις Cloud αυτές υπηρεσίες .Με βάση τα ευρήματα μας καταλήξαμε στο συμπέρασμα ότι υπάρχει πληθώρα δεδομένων που δημιουργούνται από την χρήση των υπηρεσιών αυτών-είτε μέσω λογισμικού είτε μέσω κάποιου περιηγητή.

Στόχος 4*:Να εξετάσουμε τις επιπτώσεις, από εγκληματολογική σκοπιά(metadata,ημερομηνία πρόσβασης, αλλαγή της τιμής κατακερματισμού), που έχει η διακίνηση δεδομένων μέσω των εφαρμογών αυτών.*

Παρομοίως στα κεφάλαια 7,8,9 εξετάσαμε τις Cloud αυτές υπηρεσίες και ανακαλύψαμε τις αλλαγές που επιφέρει η διακίνηση αρχείων μέσω των Cloud αυτών υπηρεσιών.

10.2. Ευρήματα Έρευνας

Ο ρόλος του κεφαλαίου 6 είναι να συμβάλει στην μετάβαση μας από την θεωρητική σκοπιά της έρευνας μας στο πρακτικό κομμάτι της εξέτασης των Cloud υπηρεσιών. Για να το πετύχουμε αυτό θέσαμε μια σειρά από ερωτήματα.

10.2.1 Ερευνητική ερώτηση 1

Η πρώτη ερευνητική ερώτηση είναι η εξής:

E_1-Ποιά είναι τα αποδεικτικά στοιχεία/ απομεινάρια δεδομένων (data remnants) που δημιουργούνται από την χρήση των cloud υπηρεσιών;

Στα κεφάλαια 7,8 και 9 αναλύσαμε εις βάθος τις Cloud υπηρεσίες αποθήκευσης. Ανακαλύψαμε την ύπαρξη αποδεικτικών στοιχείων σε ένα υπολογιστικό σύστημα με Windows 7, είτε με την χρήση του λογισμικού της εφαρμογής είτε με την χρήση ενός περιηγητή. Επίσης ανακαλύψαμε απομεινάρια δεδομένων(data remnants) ακόμα και όταν χρησιμοποιήσαμε αντιδικανικές διαδικασίες. Η ερώτηση E1 μας είχε οδηγήσει στις ακόλουθες υποερωτήσεις:

Υπόθεση 1*: Δεν υπάρχουν data remnants από την χρήση των cloud υπηρεσιών που να επιτρέπουν τον προσδιορισμό του φορέα παροχής υπηρεσιών(service provider), του ονόματος του χρήστη, ή των αρχεία που μεταφέρθηκαν.*

Υπόθεση 2*: Υπάρχουν υπολείμματα από την χρήση των cloud υπηρεσιών που επιτρέπουν την αναγνώριση της υπηρεσίας, του ονόματος του χρήστη, ή των λεπτομερειών των αρχείων.*

Όπως προσδιορίσαμε προηγουμένως στα πλαίσια της έρευνας μας ανακαλύψαμε απομεινάρια δεδομένων στο υπολογιστικό μας σύστημα. Έτσι η δεύτερη υπόθεση αποδεικνύεται σωστή και μας οδηγεί στις ερωτήσεις που ακολουθούν.

1. *Ποιά είναι τα δεδομένα που παραμένουν στον υπολογιστή μετά την εγκατάσταση του λογισμικού της εφαρμογής και την χρήση του για «ανέβασμα» και αποθήκευση δεδομένων;*

Τα αποτελέσματα της ανάλυσης των επιλεγμένων Cloud υπηρεσιών παρουσιάζονται στα κεφάλαια 7,8 και 9.Αρχικά επικεντρωθήκαμε στην χρήση του λογισμικού των εφαρμογών Evernote, SpiderOak και Box και στα απομεινάρια δεδομένων που δημιουργούνται από την χρήση τους. Προσδιορίσαμε τις τοποθεσίες εγκατάστασης του λογισμικού,είτε στον φάκελο 'AppData', στον 'Roaming' ή στον 'Local'. Ανακαλύψαμε το όνομα του χρήστη για κάθε λογαριασμό είτε στην βάση δεδομένων τις εφαρμογής, είτε στα αρχεία του περιηγητή ή τέλος στην μνήμη RAM. Πρέπει να επισημάνουμε ότι ανακαλύψαμε και το συνθηματικό του λογαριασμού είτε στην μνήμη RAM είτε στα αρχεία του σκληρού δίσκου. Στον πίνακα που ακολουθεί παρουσιάζουμε τα αρχεία στα οποία κάθε ερευνητής πρέπει να επικεντρώνει την έρευνα του.

Πίνακας 10-1: Συνοπτική παρουσίαση των προς εξέτασιν αρχείων

Evernote	Αρχεία Log και georgesmeros.exb
SpiderOak	Αρχεία Log και object_cache και pandora_sqliite_database
Box	Αρχεία Log και Syncdb.sqlite3

2. *Ποιά είναι τα δεδομένα που παραμένουν στον υπολογιστή μετά την πρόσβαση στην υπηρεσία cloud μέσω ενός προγράμματος πλοήγησης;*

Δεδομένου της πρόσβασης στις υπηρεσίες Cloud μέσω των δυο περιηγητών ανακαλύψαμε επιτυχώς το όνομα του χρήστη του λογαριασμού. Ανακαλύψαμε, ακόμα, πολλαπλά URL που επιβεβαίωσαν την χρήση των συγκεκριμένων υπηρεσιών έλος με την εξέταση των αρχείων των περιηγητών ανακαλύψαμε τα αρχεία που διακινήσαμε καθώς και σχετικές με αυτά πληροφορίες (τιμές κατακερματισμού και ημερομηνίες).

3. *Ποια δεδομένα παραμένουν στην πτητική μνήμη, όταν χρησιμοποιείται το λογισμικό της εφαρμογής και ποιά όταν χρησιμοποιείται ένα πρόγραμμα πλοήγησης;*

Η ανάλυση της μνήμης μας αποκάλυψε ένα μεγάλο πλήθος πληροφοριών. Καταρχήν καταφέραμε να ανακαλύψουμε σε *plaintext* τα ονόματα των χρηστών και τα συνθηματικά που χρησιμοποιήσαμε

για την πρόσβαση μας στις τρεις αυτές υπηρεσίες. Τέλος καταφέραμε να ανακαλύψουμε το όνομα των αρχείων που διακινήσαμε, το μέγεθος τους, τις τιμές κατακερματισμού και το περιεχόμενο τους.

10.2.2 Ερευνητική ερώτηση 2

Η δεύτερη ερώτηση είναι η εξής:

E_2-Πως επηρεάζει η διακίνησης αρχείων από μια υπηρεσία cloud τα εσωτερικά δεδομένα και τα μεταδεδομένα (metadata) των αρχείων;

Η διαδικασία της διακίνησης αρχείων δεν μεταβάλει τα περιεχόμενα των φακέλων ούτε τα σχετικά με αυτά μεταδεδομένα όπως είναι η ημερομηνία δημιουργίας, ο συγγραφέας και η τιμή κατακερματισμού. Αντίθετα αυτό που μεταβάλλεται είναι οι μεταβλητές Date created, Date accessed και Date modified του αρχείου. Οι τιμές που παίρνουν οι μεταβλητές αυτές εξαρτάται από τον τρόπο που έγινε το «κατέβασμα» των αρχείων.

10.3. Επεκτάσεις

Ιδιαίτερη μνεία πρέπει να κάνουμε στο γεγονός ότι σε πολλά σενάρια που εξετάσαμε καταφέραμε να ανακαλύψουμε όχι μόνο το όνομα χρήστη αλλά και το συνθηματικό του. Επιπροσθέτως πρέπει να αναφέρουμε ότι με την δημιουργία μιας εικονικής μηχανής, με βάση τον σκληρό δίσκο που ανακτήσαμε ,μπορέσαμε να αποκτήσουμε αυτόματα πρόσβαση στις υπηρεσίες αυτές. Αυτό οφείλεται στο γεγονός ότι το λογισμικό των εφαρμογών αυτών με την εκκίνηση του συστήματος, συνδέονται αυτόματα στον λογαριασμό του χρήστη(auto-login).Τέλος τα πεδία στα οποία μπορεί να επικεντρωθεί μια μελλοντική έρευνα των υπηρεσιών αυτών είναι η εξέταση των δικτυακών πακέτων κατά την χρήση των συγκεκριμένων υπηρεσιών καθώς και η πρόσβαση στις συγκεκριμένες υπηρεσίες μέσω smartphones.

Αναφορές

Βιβλιογραφία

- Anon., 2012. *Digital investigations in the Cloud*
- Bert-Jaap Koops, Ronald Leenes, Paul De Hert & Sandra Olislaegers, 2012. Crime and Criminal Investigation in the Clouds.
- Carvey, H., 2012. *Windows Forensics Analysis Toolkit.*
- Cory Altheide & Harlan Carvey, 2011. *Digital Forensics with open source Tools.*
- Deloitte, 2009. *Cloud computing Forecasting change.*
- Iqbal, H., 2009. *Forensic Analysis of Physical Memory and Page File.*
- Kam-Pui Chow & Sujeet Shenoi, 2010. *Advances in Digital Forensics.*

Πηγές στο Διαδίκτυο

- ACPO, 2007.
  Διαθέσιμο :
  http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
  [Πρόσβαση Σεπτεμβριος 2013].
- Amari, K., 2009. *Techniques and Tools for Recovering and Analyzing Data from.*
  Διαθέσιμο: http://www.sans.org/
  [Πρόσβαση Σεπτέμβριος 2013].
- Bonnie Malmström & Philip Teveldal, 2013. *Forensic analysis of the ESE database in Internet Explorer 10.*
  Διαθέσιμο: http://www.diva-portal.org/smash/get/diva2:635743/FULLTEXT02
  [Πρόσβαση Σεπτεμβριος 2013].
- Box, 2013. *Box Overview.*
  Διαθέσιμο: https://app.box.com/personal/
  [Πρόσβαση Σεπτέμβριος 2013].
- Deloitte, 2012. *Impact of Cloud Computing.*
  Διαθέσιμο: http://www.deloitte.com/assets/Dcom-Netherlands/Local%20Assets/Documents/NL/Diensten/Risicomanagement/nl_nl_risk_Cloud-Compliance_en_Forensics_in_de_cloud_03-11-2012.pdf
  [Πρόσβαση Σεπτέμβριος 2013].

- Department of Finance and Deregulation,Australia, 2011. *Cloud Computing Strategic Direction Paper.*
  Διαθέσιμο:
  http://agimo.gov.au/files/2012/04/final_cloud_computing_strategy_version_1.pdf
  [Πρόσβαση Σεπτέμβριος 2013].

- Digital Corpora, n.d. *Govdocs1.*
  Διαθέσιμο: http://digitalcorpora.org/corpora/files
  [Πρόσβαση Σεπτέμβριος 2013].

- Dykstra, J., 2013. *Seizing Electronic Evidence from Cloud Computing Enviroments.*
  Διαθέσιμο: http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf
  [Πρόσβαση Σεπτέμβριος 2013].

- Dykstra, J., 2013. *Seizing Electronic Evidence from Cloud Computing Enviroments.*
  Διαθέσιμο: http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf
  [Πρόσβαση Σεπτέμβριος 2013].

- Lawton, G., 2011. *http://searchcloudcomputing.techtarget.com/.*
  Διαθέσιμο: http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges
  [Πρόσβαση Σεπτέμβριος 2013].

- McKemmish, R., 1999. *What is Forensic Computing?.*
  Διαθέσιμο: http://www.aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf
  [Πρόσβαση Σεπτεμβριος 2013].

- OSForensics, n.d. *Disk Drive Signatures.* Διαθέσιμο:
  http://www.osforensics.com/compare-drive-signatures.html
  [Πρόσβαση Σεπτέμβριος 2013].

- National Institute of Standars and Technology, n.d. *The NIST Definition of Cloud Computing.*
  Διαθέσιμο: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
  [Πρόσβαση Σεπτέμβριος 2013].

- Pavel Alpeyev, Joseph Galante & Mariko Yasu, 2011. *Amazon.com Server Said to Have Been Used in Sony Attack.* [Ηλεκτρονικό]
  Διαθέσιμο: http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html
  [Πρόσβαση Σεπτέμβριος 2013].

- Sammons, J., 2012. *The Basics of Digital Forensics.* s.l.:s.n.
  Scientific Working Group on Digital Evidence, 2008. *Scientific Working Group on Digital Evidence.* Available at:
  https://www.swgde.org/documents/Current%20Documents/2008-01-

28%20SWGDE%20Capture%20of%20Live%20Systems%20v1.0
[Πρόσβαση Σεπτέμβριος 2013].

- Scientific Working Group on, 2008. *SWGDE Capture of Live Systems.*
  Available at: https://www.swgde.org/documents/Current%20Documents/2008-01-28%20SWGDE%20Capture%20of%20Live%20Systems%20v1.0
  [Πρόσβαση Σεπτέμβριος 2013].

- SpiderOak, 2013. *Encryption Specifications.*
  Available at: https://spideroak.com/engineering_matters
  [Πρόσβαση Σεπτέμβριος 2013].

- SpiderOak, n.d. *SpiderOak Hive.*
  Available at: https://spideroak.com/hive/
  [Πρόσβαση Σεπτέμβριος 2013].

- Tal Garfinkel, Ben Pfaff, Jim Chow & Mendel Rosenblum, 2004. *Data Lifetime is a Systems Problem.*
  Available at: http://www-cs.stanford.edu/people/jchow/papers/lifetime-sigops04.pdf
  [Πρόσβαση Σεπτέμβριος 2013].

- U.S Department of Justice, 2004. *Forensic Examination of Digital Evidence.*
  [Ηλεκτρονικό]
  Available at: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
  [Πρόσβαση Σεπτεμβριος 2013].

- VMware, n.d. *Using the Snapshot.*
  Available at: http://www.vmware.com/support/ws4/doc/preserve_snapshot_ws.html
  [Πρόσβαση Σεπτέμβριος 2013].

- Why the Future is in the Cloud, 2012. *Why the Future is in the Cloud.*
  Available at: http://hub.uberflip.com/h/i/472971-infographic-why-the-future-for-marketers-is-in-the-cloud
  [Πρόσβαση Σεπτέμβριος 2013].

Ιστότοπος Εργαλείων

- Access Data, n.d. *FTK IMAGER.*
  Available at: http://www.accessdata.com/support/product-downloads
  [Πρόσβαση Σεπτέμβριος 2013].

- ESEDatabaseView, n.d. [Ηλεκτρονικό]
  Available at: http://www.nirsoft.net/utils/ese_database_view.html

- Esentutl.exe, n.d. [Ηλεκτρονικό]
  Available at: http://support.microsoft.com/kb/930832

- Evernote, 2013. *Evernote.* [Ηλεκτρονικό]
  Διαθέσιμο: http://evernote.com/evernote/
  [Πρόσβαση Σεπτέμβριος 2013].

- HexEdit, n.d. *HexEdit.*
  Διαθέσιμο: http://www.hexedit.com/
  [Πρόσβαση Σεπτέμβριος 2013].

- OSForensics, n.d. *OSForensics.*
  Διαθέσιμο: http://www.osforensics.com/

- Prodiscover Basic, n.d. *Prodiscover Basic.*
  Διαθέσιμο: http://www.techpathways.com/desktopdefault.aspx?tabindex=8&tabid=14

- MoonSols, n.d. *MoonSols DumpIt.*
  Διαθέσιμο: http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/

- VMware, n.d. *VMware Workstation.* [Ηλεκτρονικό]
  Διαθέσιμο:
  https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0