ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

M.Sc. in Digital Systems Security

Διπλωματική Εργασία

Τίτλος Εργασίας	«Ψηφιακή Εγκληματολογία στο Νέφος: Εντοπισμός ευρημάτων στο μοντέλο λογισμικό ως υπηρεσία» "Cloud Forensics: Locating artifacts in SaaS cloud model"
Ονοματεπώνυμο Φοιτητή	Δραγώνας Ευάγγελος
Πατρώνυμο	Γεώργιος
Αριθμός Μητρώου	MTE1712
Επιβλέπων	Ξενάκης Χρήστος

Ημερομηνία Παράδοσης: **Ιούνιος 2019**

Τριμελής Εξεταστική Επιτροπή

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

Στον αγαπημένο μου παππού Μιχάλη,
ο οποίος φέτος έφυγε από κοντά μας
για τη γειτονιά των αγγέλων

Ευχαριστίες

Θα ήθελα να ευχαριστήσω από τα βάθη της καρδιάς μου, τους καθηγητές μου κα. Μήτρου και κ. Λαμπρινουδάκη, για την άριστη συνεργασία που είχαμε στα πλαίσια της παρούσας διπλωματικής εργασίας. Χωρίς τις πολύτιμες συμβουλές της κα. Μήτρου και τη στήριξη του κ. Λαμπρινουδάκη, η ολοκλήρωση της θα ήταν αδύνατη. Εύχομαι να έχω τη τιμή να επαναλάβουμε τη συνεργασία μας στο μέλλον.

Τέλος, να ευχαριστήσω τη σύντροφο μου Στεφανία και την οικογένεια μου, για την πίστη που μου δείχνουν σε κάθε μου εγχείρημα.

Περίληψη

Η τεχνολογία του υπολογιστικού νέφους χρησιμοποιείται καθημερινά από χιλιάδες ανθρώπους και εταιρείες. Από μεγάλους επιχειρηματικούς κολοσσούς, οι οποίοι την έχουν ενσωματώσει στην υποδομή τους, μέχρι τον απλό χρήστη των υπηρεσιών που στηρίζονται σε αυτή, η εν λόγω τεχνολογική καινοτομία αγαπήθηκε όσο καμία άλλη τα τελευταία χρόνια. Η ποικιλομορφία της αγοράς, οδήγησε το υπολογιστικό νέφος να διατίθεται σε διαφορετικά μοντέλα υπηρεσίας στο αγοραστικό κοινό. Το πιο δημοφιλές εξ αυτών, είναι το μοντέλο «Λογισμικό ως Υπηρεσία». Ο συνδυασμός των οφελών που προσφέρει η τεχνολογία αυτή και της ευρείας αποδοχής που γνωρίζει, κάνει ολοένα και συχνότερο το φαινόμενο να χρησιμοποιείται ως το μέσο τέλεσης ή ο στόχος αξιόποινων πράξεων. Η διερεύνηση των εγκλημάτων που τελούνται στο νέφος, αποτελεί αντικείμενο μελέτης της Ψηφιακής Εγκληματολογίας. Η επιστήμη αυτή, αποτελεί την τελευταία προσθήκη στον επιστημονικό κλάδο της Εγκληματολογίας. Ωστόσο, μία εγκληματολογική εξέταση στο νέφος παρουσιάζει αρκετές ιδιομορφίες σε σχέση με τα υπόλοιπα είδη αξιόποινων ενεργειών που εξετάζει η επιστήμη αυτή. Η έλλειψη νομοθετικού πλαισίου γύρω από τη δικανική εξέταση στο νέφος και η ακεραιότητα των δεδομένων που συλλέγονται από αυτό, συνιστούν μόνο δύο από τα ζητήματα που καλείται να αντιμετωπίσει ένας ερευνητής Ψηφιακής Εγκληματολογίας. Στην παρούσα διπλωματική εργασία, πραγματοποιείται εγκληματολογική εξέταση στο νέφος. Αναλυτικότερα, εξετάζονται δικανικά δημοφιλείς υπηρεσίες νέφους (Dropbox, Google Drive) που ανήκουν στο μοντέλο «Λογισμικό ως Υπηρεσία», με έμφαση στον εντοπισμό ευρημάτων που απορρέουν από τη χρήση τους, στο λειτουργικό σύστημα Windows 10.

Abstract

Cloud computing technology is being used by thousands of people and companies on a daily basis. From business leaders, who have incorporated this technology in their infrastructure to the simple user of the services that rely on it, this technological innovation has been celebrated as no other in recent years. Market heterogeneity, has led cloud computing to be distributed to different service models in the buying audience. The most popular among them, is the "Software as Service" model. The combination of both the benefits offered by this technology and its widespread acceptance, makes it increasingly common for it to be used as the means of execution or the target of crime. The investigation of crimes committed in the cloud is a subject of Digital Forensics. This science field is the latest addition to the branch of Forensic Science. However, a cloud forensics investigation has several peculiarities in relation to the other types of crime that this science deals with. The lack of a legal framework around cloud forensics and the integrity of data collected from it, constitute only two of the issues that a forensicator has to cope with. In this master thesis, a complete cloud forensics investigation is

performed. In more detail, well known cloud services (Dropbox, Google Drive) belonging to the "Software as a Service" model are being examined, with emphasis on detecting findings resulting from their use in the Windows 10 operating system.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1ο: Εισαγωγή

1.1. Γενικά

Στην εποχή της πληροφορίας στην οποία ζούμε τις τελευταίες δεκαετίες, η τεχνολογία εξελίσσεται με ανεξέλεγκτους ρυθμούς. Μετά τον ερχομό του προσωπικού υπολογιστή, του Διαδικτύου και των έξυπνων κινητών τηλεφώνων, η τεχνολογική ανακάλυψη που κυριαρχεί σταδιακά σε παγκόσμιο επίπεδο στο τομέα της Πληροφορικής, είναι αυτή του υπολογιστικού νέφους (cloud computing). Η τεχνολογία αυτή συνδυάζει τα οφέλη του Διαδικτύου με αυτά των κινητών συσκευών, παρέχοντας υπηρεσίες σε οποιοδήποτε σημείο του πλανήτη, οποιαδήποτε στιγμή. Ολοένα και περισσότερες εταιρείες χρησιμοποιούν υπηρεσίες υπολογιστικού νέφους είτε ως βασικό εταιρικό δίκτυο είτε πιο απλά εξάγοντας τα δεδομένα τους σε αυτό. Ολοένα και περισσότεροί είναι οι χρήστες που προτιμούν το νέφος για την αποθήκευση των δεδομένων τους, έναντι άλλων μεθόδων, όπως η αποθήκευση τους σε ένα εξωτερικό σκληρό δίσκο. Οι προαναφερθείσες υπηρεσίες του νέφους διατίθενται σε διάφορα μοντέλα, ανάλογα με το είδος υπηρεσίας που προσφέρουν.

Η χρήση των τεχνολογικών επιτευγμάτων που προκύπτουν στον τομέα της Πληροφορικής, αν και εν γένει ωφελεί την ανθρώπινη κοινωνία, δεν παύει να ενέχει κινδύνους και να χρησιμοποιείται με τρόπο διαφορετικό, από αυτόν που οραματίζονταν οι δημιουργοί τους. Ειδικότερα, είναι πλέον σύνηθες ένας κακόβουλος χρήστης εκμεταλλευόμενος την πληροφορική τεχνολογία, να διαπράττει κάποια αξιόποινη πράξη.

Η αξιοποίηση της τεχνολογίας της Πληροφορίας σε παράνομες ενέργειες, έχει οδηγήσει στη δημιουργία νέων μορφών εγκλήματος, όπως αυτή του ηλεκτρονικού εγκλήματος και του κυβερνοεγκλήματος. Το κυβερνοέγκλημα τα τελευταία χρόνια έχει εξελιχθεί σε ένα από τα πιο δημοφιλή είδη εγκλήματος, κυρίως λόγω του κέρδους που προσφέρει, σε συνδυασμό με το χαμηλό κόστος που απαιτεί. Σύμφωνα με έκθεση του CSIS και της εταιρείας McAfee (Lewis 2018), το κόστος που προκάλεσε το κυβερνοέγκλημα για το έτος 2017 στην παγκόσμια οικονομία ανέρχεται στα 600$ δισεκατομμύρια δολάρια, ενώ το αντίστοιχο ποσό για το έτος 2014, ήταν 445$ δισεκατομμύρια δολάρια. Η διερεύνηση τόσο του ηλεκτρονικού εγκλήματος, όσο και του κυβερνοεγκλήματος, αποτελούν το αντικείμενο μελέτης μίας νέας επιστήμης, της ψηφιακής εγκληματολογίας ή αλλιώς δικανικής πληροφορικής.

Αν και η πρώτη νομοθεσία που προέβλεπε ποινή για ηλεκτρονικό έγκλημα εμφανίστηκε το 1978 (Norman n.d.), δεν ήταν πριν τη δύση του 20ου αιώνα όταν σχημα-

τίστηκαν και καθιερώθηκαν οι πρώτες διεθνείς μεθοδολογίες και πρότυπες διαδικασίες για την επιστήμη της ψηφιακής εγκληματολογίας. Η εν λόγω επιστήμη έκτοτε αναγνωρίστηκε ως νέα κατηγορία της εγκληματολογίας. Οι διαδικασίες αυτές αποσκοπούν μεταξύ άλλων, στην εξασφάλιση της εγκυρότητας των αποτελεσμάτων μίας εγκληματολογικής εξέτασης, καθώς και στη διασφάλιση της ποιότητας της. Αυτές οι εγγυήσεις θεωρούνται αναγκαίες τόσο για τη δικανική πληροφορική όσο και για την εγκληματολογική επιστήμη συνολικά. Ο βασικός λόγος που τις καθιστά απαραίτητες είναι το γεγονός ότι, αμφότερες χρησιμοποιούνται σημαντικά στην ποινική διαδικασία, χωρίς να αποκλείεται βέβαια η αξιοποίηση τους και σε άλλου είδους υποθέσεις (αστικές, κ.ά.).

Η ψηφιακή εγκληματολογία (Reith et al. 2002) ειδικεύεται στη συλλογή, στην εξέταση και στην ερμηνεία δεδομένων που αποθηκεύονται ή διαβιβάζονται σε ψηφιακή μορφή. Αρχικά ο όρος αυτός, χρησιμοποιούταν ως συνώνυμο της εγκληματολογίας των υπολογιστών (computer forensics) (Carrier 2003). Με την πάροδο του χρόνου και την εμφάνιση νεών συσκευών που αποθηκεύουν, διαβιβάζουν και επεξεργάζονται δεδομένα σε ψηφιακή μορφή, η έννοια του όρου διευρύνθηκε, προκειμένου να περιλαμβάνει όλες αυτές τις τεχνολογικές καινοτομίες (digital forensics). Η ραγδαία τεχνολογική πρόοδος όμως, θέτει πολλές φορές εμπόδια και προκλήσεις στις πρότυπες διαδικασίες της εν λόγω επιστήμης, οι οποίες αγωνίζονται να συμβαδίσουν μαζί της. Μία από τις τελευταίες τεχνολογικές ανακαλύψεις που αποτελούν πρόκληση για τις υπάρχουσες διαδικασίες ψηφιακής εγκληματολογικής εξέτασης, είναι αυτή του υπολογιστικού νέφους.

Ένα από τα διαθέσιμα μοντέλα υπηρεσιών υπολογιστικού νέφους είναι το «Λογισμικό ως Υπηρεσία (SaaS Cloud)». Στο μοντέλο αυτό (Mell and Grance 2011), οι χρήστες αφού αποκτήσουν πρόσβαση στο νέφος, μπορούν να αποθηκεύουν τα δεδομένα τους σε αυτό. Αυτή η δυνατότητα που έχουν χρήστες δημιουργεί ένα εντελώς νέο περιβάλλον αποθήκευσης δεδομένων. Ένα περιβάλλον το οποίο ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί για τη διάπραξη παράνομων ενεργειών. Η χρήση ενός διαδικτυακού χώρου αποθήκευσης δεδομένων, στον οποίο μάλιστα η πρόσβαση καθορίζεται από τον ίδιο τον κακόβουλο χρήστη, παρουσιάζει ποικίλα πλεονεκτήματα έναντι της χρήσης συμβατικών μεθόδων αποθήκευσης. Για παράδειγμα, σε εγκλήματα όπως η κατοχή και ο διαμοιρασμός αρχείων που εμπίπτουν στις διατάξεις περί προστασίας της πνευματικής ιδιοκτησίας, ο ύποπτος μπορεί να διαθέτει το παράνομο υλικό διαδικτυακά, στο νέφος (cloud) του, χωρίς να αποθηκεύει τοπικά τίποτε στις συσκευές του (κινητό τηλέφωνο, υπολογιστής, κ.ά.). Ο ερευνητής δικανικής πληροφορικής στην προκειμένη περίπτωση, εκτός από τα νομικά ζητήματα (Kaur and

Singh 2016) που έχει να αντιμετωπίσει ακολουθώντας μόνο τις παραδοσιακές διαδικασίες δικανικής πληροφορικής, δύναται να χάσει μέρος της απαραίτητης αποδεικτικής πληροφορίας που στοιχειοθετεί το ανωτέρω αδίκημα. Η απουσία εξειδικευμένης γνώσης, όσον αφορά την τεχνολογία του υπολογιστικού νέφους και κατ' επέκταση, η αδυναμία εντοπισμού των επίμαχων ευρημάτων, θέτουν εμπόδια στον ερευνητή που βρίσκεται σε δύσκολη θέση (Arafat et al. 2017). Το πρόβλημα επιδεινώνεται στην περίπτωση που η εξέταση γίνεται σε μεταγενέστερο χρόνο (post mortem-dead) από τη συλλογή των συσκευών και όχι «ζωντανά» (live) επί τόπου. Άλλα παραδείγματα χρήσης των υπηρεσιών υπολογιστικού νέφους για εγκληματικές ενέργειες αφορούν τη διαρροή απόρρητων αρχείων, DDoS επιθέσεις, hacking, εγκατάσταση malware, σεξουαλική κακοποίηση ανηλίκων, κ.ά. Το κάθε ένα από αυτά απαιτεί ειδική μεταχείριση.

Είναι απαραίτητο για τα στελέχη των τριών εξουσιών (νομοθετική, εκτελεστική και δικαστική) που λειτουργούν σε ένα σύγχρονο κράτος δικαίου (Μανιτάκης 2011), να μελετήσουν την τεχνολογία πάνω στην οποία στηρίζεται το υπολογιστικό νέφος και να αντιληφθούν το πώς αυτή δουλεύει. Είναι ο μόνος τρόπος για να θεσπιστεί το απαραίτητο νομικό πλαίσιο, το οποίο θα επιλύει τα νομικά ζητήματα μίας εγκληματολογικής εξέτασης στο νέφος, τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Το εν λόγω νομικό πλαίσιο θα πρέπει ιδανικά να μεριμνά για τη συνεργασία όλων των εμπλεκόμενων οντοτήτων (αστυνομικές αρχές, πάροχοι υπηρεσιών, δικαστές, ερευνητές, κ.τ.λ.) σε περίπτωση διάπραξης ενός εγκλήματος με χρήση της τεχνολογίας αυτής.

Αντίστοιχα απαραίτητο είναι και για τον ερευνητή δικανικής πληροφορικής να κατανοήσει την εν λόγω τεχνολογία. Μόνο έτσι θα μπορέσει να αντιληφθεί το τι είδους ευρήματα δύναται να προκύψουν κατά την εγκληματολογική εξέταση του και κατά συνέπεια να ενεργήσει καταλλήλως για τον εντοπισμό και την εξασφάλιση τους. Αν περισσότεροι ερευνητές γνωρίζουν τι να περιμένουν και τι ψάχνουν σε μία εγκληματολογική εξέταση στο νέφος, θα είναι σε θέση να προτείνουν ποιες τροποποιήσεις χρειάζονται να γίνουν στις υπάρχουσες διαδικασίες ή τι είναι απαραίτητο να συμπεριληφθεί στις νέες που δημιουργούνται.

Η αρχή για την ανωτέρω μελέτη από τη μεριά ενός ερευνητή, όσον αφορά τα ευρήματα που εμφανίζονται σε μία εγκληματολογική εξέταση στο νέφος, επελέγη να γίνει με βάση το μοντέλο υπηρεσιών με τη μεγαλύτερη απήχηση στο κοινό. Αφού μελετηθεί ενδελεχώς μία εγκληματολογική εξέταση σε αυτό το μοντέλο, ο ερευνητής θα έχει τα εφόδια για να ανταπεξέλθει σε περισσότερες υποθέσεις. Το μοντέλο υπηρεσιών υπολογιστικού νέφους με το μεγαλύτερο μερίδιο αγοράς, είναι το μοντέλο «Λογισμικό ως Υπηρεσία». Για την ακρίβεια, σύμφωνα με έρευνα της Gartner (Gartner

2018), τα έσοδα από το μοντέλο αυτό για το έτος 2018 (μέχρι τον Απρίλιο μήνα) ανήλθαν περίπου στα 74$ δισεκατομμύρια δολάρια και είναι περισσότερα από το άθροισμα των εσόδων των υπόλοιπων κύριων μοντέλων υπηρεσιών νέφους (περίπου 56$ δισεκατομμύρια δολάρια). Στο μοντέλο αυτό, ο χρήστης χρειάζεται μία συσκευή (π.χ. υπολογιστή), εφοδιασμένη με λειτουργικό σύστημα και σύνδεση στο Ίντερνετ προκειμένου να έχει πρόσβαση στα δεδομένα του. Αντίστοιχα με τα ανωτέρω, το λειτουργικό σύστημα με το μεγαλύτερο μερίδιο αγοράς για τους υπολογιστές είναι το Windows (StatCounter n.d.). Επομένως συμπεραίνεται ότι, ο εντοπισμός ευρημάτων σε μία εγκληματολογική εξέταση στο νέφος που συνδυάζει τη χρήση του μοντέλου SaaS, με συσκευές που έχουν λειτουργικό σύστημα Windows, είναι πολύ χρήσιμη για τους ερευνητές ψηφιακής εγκληματολογίας.

1.2. Σκοπός της Διπλωματικής Εργασίας

Απώτερος σκοπός της παρούσας διπλωματικής εργασίας είναι η ερευνητική συνεισφορά στην επιστήμη της ψηφιακής εγκληματολογίας. Αναλυτικότερα, επίκεντρο της έρευνας της διπλωματικής εργασίας αποτελεί η διεξαγωγή εγκληματολογικής εξέτασης σε συσκευές που χρησιμοποιούν λειτουργικό σύστημα Windows 10 και δημοφιλείς υπηρεσίες (Dropbox και Google Drive) υπολογιστικού νέφους (μοντέλο SaaS), προς αναζήτηση ευρημάτων που σχετίζονται με τη χρήση των εν λόγω υπηρεσιών. Για την εκπλήρωση του σκοπού της διπλωματικής εργασίας, χρειάζεται να επιτευχθούν συγκεκριμένοι θεωρητικοί και ερευνητικοί στόχοι. Οι εν λόγω στόχοι παρουσιάζονται κάτωθι:

Θεωρητικοί Στόχοι:

- **Θ.1. :** Ανάλυση των εννοιών της ψηφιακής εγκληματολογίας, του υπολογιστικού νέφους καθώς και της ψηφιακής εγκληματολογίας στο νέφος,

- **Θ.2. :** Επισκόπηση βασικών τεχνικών προκλήσεων και νομικών ζητημάτων που εμφανίζονται κατά την εγκληματολογική εξέταση στο νέφος και

- **Θ.3. :** Παρουσίαση των σημαντικότερων ευρημάτων που μπορούν να προκύψουν κατά τη δικανική εξέταση ψηφιακών δεδομένων, με έμφαση στα ευρήματα που σχετίζονται με τις υπηρεσίες νέφους.

Ερευνητικοί Στόχοι:

- **Ε.1. :** Αναζήτηση δεδομένων που σχετίζονται με χρήση υπηρεσιών νέφους (μοντέλο SaaS), σε συσκευές που χρησιμοποιούν λειτουργικό σύστημα Windows 10 και δημοφιλείς εφαρμογές του μοντέλου αυτού (Dropbox και Google Drive),

- **Ε.2. :** Μελέτη των αλλαγών που επιφέρει η διακίνηση αρχείων μέσω των εφαρμογών αυτών, στα τεχνικά χαρακτηριστικά ενός αρχείου (metadata, hash, κ.τ.λ.).

Με την ολοκλήρωση της έρευνας αυτής και την ικανοποίηση των ανωτέρω στόχων, ένας ερευνητής δικανικής πληροφορικής, μελετώντας το σύνολο των ευρημάτων που περιγράφονται στην εργασία, μπορεί να αναμένει τα κάτωθι αποτελέσματα:

Αποτελέσματα:

- **Α.1. :** Καλύτερη κατανόηση των εννοιών της ψηφιακής εγκληματολογίας, του υπολογιστικού νέφους καθώς και της ψηφιακής εγκληματολογίας στο νέφος,

- **Α.2. :** Ενημέρωση ως προς τις κυριότερες τεχνικές προκλήσεις και νομικά ζητήματα που εμφανίζονται κατά την εγκληματολογική εξέταση στο νέφος,

- **Α.3. :** Δυνατότητα αναγνώρισης των ευρημάτων που αναμένεται να προκύψουν κατά την εγκληματολογική εξέταση των υπηρεσιών νέφους,

- **Α. 4. :** Δυνατότητα εντοπισμού δεδομένων που σχετίζονται με τη χρήση των εφαρμογών Dropbox και Google Drive σε περιβάλλον Windows 10,

- **Α. 5.:** Καλύτερη αντίληψη του πώς μεταχειρίζονται τα τεχνικά χαρακτηριστικά ενός αρχείου, οι εφαρμογές Dropbox και Google Drive.

1.3. Δομή της Διπλωματικής Εργασίας

Η δομή της υπόλοιπης εργασίας παρουσιάζεται εδώ. Τα κεφάλαια 2, 3, 4 και 5 συνιστούν το θεωρητικό υπόβαθρο της εργασίας, όπου επιτυγχάνεται η ολοκλήρωση των θεωρητικών στόχων της. Ειδικότερα, στο κεφάλαιο 2 αναλύεται η έννοια της ψηφιακής εγκληματολογίας, του ψηφιακού πειστηρίου, του εγκληματολογικού αντιγράφου, οι κατηγορίες της ψηφιακής εγκληματολογίας καθώς και οι υπάρχουσες διεθνείς διεργασίες και μεθοδολογίες. Στο κεφάλαιο 3 εξετάζεται η έννοια του υπολογιστικού νέφους, τα βασικά του χαρακτηριστικά και τα μοντέλα υπηρεσιών και ανάπτυξης

του. Στο κεφάλαιο 4 περιγράφονται συνοπτικά ορισμένες βασικές τεχνικές προκλήσεις και νομικά ζητήματα που συχνά πρέπει να αντιμετωπιστούν σε μία δικανική εξέταση των υπηρεσιών νέφους. Στο κεφάλαιο 5 αναλύονται τα είδη των ευρημάτων που αναμένεται να προκύψουν κατά την εγκληματολογική εξέταση στο νέφος. Στο κεφάλαιο 6 παρουσιάζεται η μεθοδολογία της έρευνας που εφαρμόζεται στην εξέταση των υπηρεσιών νέφους. Στα κεφάλαια 7 και 8 εξετάζονται αντίστοιχα οι υπηρεσίες νέφους Dropbox και Google Drive. Τέλος στο κεφάλαιο 9 γίνεται επισκόπηση όλων των ευρημάτων της έρευνας και εξάγονται τα συμπεράσματα της εργασίας.

Κεφάλαιο 2ο: Ψηφιακή Εγκληματολογία

2.1. Γενικά

Η Ψηφιακή Εγκληματολογία είναι ο κλάδος της εγκληματολογικής επιστήμης που ειδικεύεται στην ανάκτηση, ανάλυση και ερμηνεία δεδομένων που αποθηκεύονται ή διαβιβάζονται σε ψηφιακή μορφή. Η εφαρμογή της εν λόγω επιστήμης διέπεται από κανόνες και πρότυπες διαδικασίες, οι οποίες εμπλουτίζονται και επανεξετάζονται τακτικά, προκειμένου να συμβαδίζουν με τις συνεχείς τεχνολογικές εξελίξεις στον τομέα της Πληροφορικής.

Αρκετοί είναι οι Οργανισμοί που έχουν ερμηνεύσει την έννοια της δικανικής πληροφορικής (NIST, ACPO, SWGDE, κ.ά.), προκειμένου να υπάρξει ένα κοινό σημείο αναφοράς ως προς τι είναι αλλά και τι δεν είναι ψηφιακή εγκληματολογία. Σύμφωνα λοιπόν με τον NIST (Grance et al. 2006), Ψηφιακή Εγκληματολογία θεωρείται (παρατίθεται σε μετάφραση): «*… η εφαρμογή της επιστήμης στην αναγνώριση, συλλογή, εξέταση και ανάλυση των δεδομένων, διασφαλίζοντας παράλληλα την ακεραιότητα τους και διατηρώντας αυστηρά καταγεγραμμένες τις ενέργειες που λαμβάνουν χώρα επί αυτών*». Σχεδόν κάθε μία από τις ανωτέρω λέξεις στα εισαγωγικά, καλύπτει μία ξεχωριστή πτυχή της επιστήμης αυτής. Για αυτό το λόγο, στη συνέχεια επεξηγούνται οι σημαντικότερες εξ αυτών.

2.2. Έννοια του ψηφιακού πειστηρίου

Μία από τις θεμελιώδης έννοιες της εγκληματολογικής επιστήμης είναι αυτή του «πειστηρίου». Δεν μπορεί να διενεργηθεί εγκληματολογική εξέταση, χωρίς την ύπαρξη πειστηρίων. Οι δύο αυτές έννοιες είναι στενά συνυφασμένες. Στην ελληνική γλώσσα με τον όρο «πειστήριο» νοείται: (Μπαμπινιώτης 2012): «*Οποιοδήποτε αντικείμενο συντελεί στη βεβαίωση της τελέσεως ενός εγκλήματος ή στην απόδειξη της ενοχής ή της αθωότητας του κατηγορουμένου*». Με αυτήν την ερμηνεία χρησιμοποιείται ο όρος και στην ελληνική νομοθεσία. Δύο παραδείγματα πειστήριων σε ένα έγκλημα όπως η κλοπή, είναι η κουκούλα του δράστη και ένας χρησιμοποιημένος λοστός που εντοπίστηκαν στη σκηνή του εγκλήματος. Στο συγκεκριμένο παράδειγμα, η άντληση της αποδεικτικής πληροφορίας από τα πειστήρια και συνολικά η εγκληματολογική εξέταση αυτών, είναι σχετικά απλή υπόθεση. Δεν θα ίσχυε το ίδιο βέβαια, αν στα ανωτέρω πειστήρια προστίθονταν το κινητό τηλέφωνο του δράστη.

Επεκτείνοντας την έννοια του πειστηρίου στον ψηφιακό κόσμο και ειδικότερα στην ψηφιακή εγκληματολογία, εμφανίζεται η έννοια του «ψηφιακού πειστηρίου». Η

διαφορά τους έγκειται στο ότι το ψηφιακό πειστήριο φέρει τα δεδομένα του αποθηκευμένα ή διαβιβαζόμενα σε ψηφιακή μορφή. Κατ' αναλογία με τη συμβατική εγκληματολογική εξέταση, η ψηφιακή εγκληματολογική εξέταση ειδικεύεται στην εξέταση ψηφιακών πειστηρίων. Εφεξής λοιπόν, όταν γίνεται λόγος για εξέταση ψηφιακού πειστηρίου, νοείται η εξέταση οποιουδήποτε αντικειμένου που φέρει τα δεδομένα του αποθηκευμένα ή διαβιβαζόμενα σε ψηφιακή μορφή και συντελεί στη βεβαίωση της τελέσεως ενός εγκλήματος ή στην απόδειξη της ενοχής ή της αθωότητας του κατηγορουμένου.

Εξαιτίας της τεράστιας πληροφορίας που αποθηκεύουν, τα ψηφιακά πειστήρια παίζουν πολλές φορές καθοριστικό ρόλο για την εκδίκαση μίας υπόθεσης. Εκτός από τις περιπτώσεις εγκλημάτων των οποίων η εξιχνίαση στηρίζεται εξ ολοκλήρου στην εξέταση τους (ηλεκτρονικό έγκλημα, κυβερνοέγκλημα), τα ψηφιακά πειστήρια «μαρτυρούν» πολλές φορές πληροφορίες για την τέλεση άλλων εγκλημάτων, όπως μία ανθρωποκτονία ή μία ληστεία (TheTOC 2018). Το γεγονός αυτό, αφενός τα καθιστά εξαιρετικά χρήσιμα για την Δικαστική Αρχή και αφετέρου τα μετατρέπει σε στόχο των διασταυρωμένων πυρών, μεταξύ των διαδίκων.

Γίνεται κατανοητό από τα ανωτέρω ότι ένα ψηφιακό πειστήριο, όπως και πάσης φύσης πειστήριο, χρήζει ειδικής μεταχείρισης, προκειμένου να εξασφαλίζεται η ακεραιότητα του καθ' όλη τη διάρκεια που αυτό χρησιμοποιείται (Tenhunen 1997). Η διασφάλιση της ακεραιότητας ενός πειστηρίου, είναι ένας από τους ύψιστους στόχους όχι μόνο της δικανικής πληροφορικής, αλλά και της εγκληματολογικής επιστήμης εν γένει. Δεν είναι λίγες οι περιπτώσεις που ένα πολύ σημαντικό πειστήριο για την καταδίκη του κατηγορούμενου, εξαιρείται από την εκδίκαση της υπόθεσης, εξαιτίας αμφιβολιών ως προς την ακεραιότητα των δεδομένων του και υπό το φόβο μη τήρησης των αυστηρών διαδικασιών μεταχείρισης του.

Με αφορμή τη σημασία που έχει ένα ψηφιακό πειστήριο στην ποινική διαδικασία, κάτωθι παρατίθενται συνοπτικά τα σημαντικότερα χαρακτηριστικά γνωρίσματα που πρέπει να έχει, προκειμένου να γίνει αποδεκτό (admissible) σε μία δίκη (Antwi-Boasiako and Venter 2017):

- **Νομική Εξουσιοδότηση/ Πρόβλεψη στο νόμο** (Legal Authorization): Για να συλλεχθεί ένα πειστήριο, θα πρέπει πρωτίστως να υπάρχει σχετική πρόβλεψη στο νόμο που να το επιτρέπει. Αυτό όμως δεν είναι αρκετό από μόνο του. Θα πρέπει η συλλογή του να πραγματοποιείται, κατόπιν εξασφάλισης της απαραίτητης νομικής εξουσιοδότησης (στην ελληνική νομοθεσία για παράδειγμα, όσον αφορά τις ποινικές υποθέσεις, η εξουσιοδότηση ως επί το πλείστον παρέχεται με τη φυσική παρουσία εισαγγελέα κατά τη διαδικασία της έρευνας και

κατάσχεσης των πειστηρίων και όχι μέσω εντάλματος έρευνας όπως συμβαίνει στο εξωτερικό). Η προστασία των δικαιωμάτων του κατηγορούμενου προσώπου (ανθρώπινα δικαιώματα, προστασία προσωπικών δεδομένων, κ.ά.) που προβλέπονται από το Σύνταγμα και τους νόμους, είναι απαραίτητη. Η τήρηση της νομιμότητας (πρόβλεψη στο νόμο σε συνδυασμό με νομική εξουσιοδότηση) κατά τα συλλογή ενός πειστηρίου, αποτελεί το πιο σημαντικό βήμα για την αποδοχή των πειστηρίων στην κύρια διαδικασία. Εάν αυτή δεν τηρηθεί, τότε τα προσκομισθέντα πειστήρια στο δικαστήριο χαρακτηρίζονται ως «παράνομα αποδεικτικά μέσα» και εξαιρούνται από την εκδίκαση της υπόθεσης.

- **Συνάφεια ψηφιακού πειστηρίου** (Digital Evidence Relevance): Η συνάφεια είναι ακόμη ένας καθοριστικός παράγοντας για την αποδοχή των ψηφιακών πειστηρίων. Όπως γίνεται αντιληπτό, η συλλογή οποιουδήποτε αντικειμένου σχετίζεται με το κατηγορούμενο άτομο, ακόμα και αν δεν προκύπτουν αποχρώσες ενδείξεις συσχετισμού του με το υπό εξέταση αδίκημα, κρίνεται απαράδεκτη (εκτός ελαχίστων εξαιρέσεων). Αντίθετα, τα ψηφιακά πειστήρια που πρέπει να συλλέγονται είναι αυτά που φέρονται να σχετίζονται με την άδικη πράξη. Σύμφωνα με το άρθρο 280 του Κώδικα Ποινικής Δικονομίας (Κ.Π.Δ.), τα πειστήρια που πρέπει να κατάσχονται, είναι όσα βρέθηκαν σε αυτόν που έχει συλληφθεί και έχουν σχέση με το έγκλημα.

- **Ακεραιότητα ψηφιακού πειστηρίου** (Digital Evidence Integrity): Από τα πιο σημαντικά χαρακτηριστικά ενός ψηφιακού πειστηρίου είναι αυτό της ακεραιότητας. Η ακεραιότητα ενός ψηφιακού πειστηρίου, συνεπάγεται ότι το σύνολο των δεδομένων που αυτό περιέχει έχουν παραμείνει πλήρη και αμετάβλητα, καθ' όλη τη διάρκεια που το πειστήριο χρησιμοποιείται. Κατά την αξιολόγηση της ακεραιότητας των ψηφιακών πειστηρίων, τα δικαστήρια εξετάζουν επιπλέον και διάφορους παράγοντες και συνθήκες (κυρίως τεχνικές δυσκολίες όπως συλλογή πτητικών δεδομένων κ.τ.λ.) που μπορούν να οδηγήσουν στην αλλοίωση τους και κατόπιν αποφαίνονται για την αποδοχή ή την απόρριψη τους.

- **Αξιοπιστία ψηφιακού πειστηρίου** (Digital Evidence Reliability): Ένα ψηφιακό πειστήριο προκειμένου να γίνει αποδεκτό στην ποινική διαδικασία πρέπει να θεωρείται αξιόπιστο. Ειδικότερα, δεν πρέπει να υπάρχουν αμφιβολίες ως προς τις μεθόδους συλλογής και της μετέπειτα εξέτασης του.

Επισημαίνεται ότι, τα ανωτέρω χαρακτηριστικά δύναται να διαφέρουν από χώρα σε χώρα και ανάλογα με το δίκαιο που εφαρμόζεται στην κάθε περίπτωση.

2.3. Δημιουργία και επαλήθευση εγκληματολογικού αντιγράφου

Γίνεται σαφές από τα ανωτέρω ότι προκειμένου να διασφαλιστεί η ακεραιότητα ενός ψηφιακού πειστηρίου, ο ερευνητής οφείλει να ενεργήσει με συγκεκριμένο τρόπο κατά την έναρξη της εγκληματολογικής εξέτασης του. Αυτός ο τρόπος αποτελεί έναν από τους σημαντικότερους κανόνες της Ψηφιακής Εγκληματολογίας. Σύμφωνα με τον κανόνα αυτό, ο ερευνητής δεν θα πρέπει ποτέ να προβαίνει στην εγκληματολογική εξέταση αυτής καθαυτής της συσκευής που αποτελεί ψηφιακό πειστήριο. Αντίθετα, θα πρέπει πάντοτε να δημιουργεί αρχικά ένα αντίγραφο των δεδομένων που αυτή περιέχει και στη συνέχεια να εξετάζει το αντίγραφο αυτό. Το αντίγραφο αυτό στη δικανική πληροφορική, ονομάζεται εγκληματολογικό αντίγραφο. Με αυτόν τον τρόπο και το ψηφιακό πειστήριο παραμένει ακέραιο και συλλέγονται όλα τα δεδομένα που περιέχονται σε αυτό. Η δημιουργία του εγκληματολογικού αντιγράφου ενός ψηφιακού πειστηρίου, αποτελεί ένα από τα πρώτα βήματα σε μία εγκληματολογική εξέταση (Wilson 2014). Υπάρχουν διαφορετικά είδη εγκληματολογικών αντιγράφων ανάλογα με την ποσότητα των δεδομένων που συλλέγονται από το ψηφιακό πειστήριο. Τα δύο βασικά είδη εγκληματολογικών αντιγράφων παρατίθενται κάτωθι:

- **Εγκληματολογικό αντίγραφο σε λογικό επίπεδο** (logical image): Το εγκληματολογικό αντίγραφο γίνεται σε επίπεδο συστήματος αρχείων (file system)(CRU-INC). Αυτή η επιλογή χρησιμεύει όταν δεν είναι εφικτή η δημιουργία εγκληματολογικού αντιγράφου σε φυσικό επίπεδο ή όταν είναι επιθυμητή η εγκληματολογική εξέταση συγκεκριμένων αρχείων, φακέλων ή κατατμήσεων (partitions). Το μειονέκτημα αυτής της μεθόδου είναι ότι δεν συλλέγονται τα δεδομένα του ψηφιακού πειστηρίου που βρίσκονται στον μη κατανεμημένο χώρο (unallocated space). Στον μη κατανεμημένο χώρο βρίσκονται τα δεδομένα εκείνα που δεν χρησιμοποιούνται από το λειτουργικό σύστημα, συμπεριλαμβανομένων και των διαγεγραμμένων αρχείων από τον χρήστη. Είναι εύκολα κατανοητό ότι εφόσον ο ύποπτος διαγράψει αρχεία πριν την κατάσχεση των ψηφιακών πειστηρίων, αυτά συνήθως δεν θα ανακτηθούν από ένα τέτοιο εγκληματολογικό αντίγραφο.

- **Εγκληματολογικό αντίγραφο σε φυσικό επίπεδο** (physical image): Το εγκληματολογικό αντίγραφο που δημιουργείται, αποτελεί ένα αντίγραφο όλων των δεδομένων που βρίσκονται αποθηκευμένα στο ψηφιακό πειστήριο. Σε αυ-

τήν την κατηγορία η μέθοδο αντιγραφής των δεδομένων που ακολουθείται είναι η bit-προς-bit (ή αλλιώς bitstream copy), δηλ. αντιγράφονται ένα-προς-ένα όλα τα bits του αποθηκευτικού μέσου. Το κυριότερο πλεονέκτημα της μεθόδου αυτής είναι ότι μπορεί να γίνει ανάκτηση διαγεγραμμένων αρχείων από τον μη κατανεμημένο χώρο.

Η δημιουργία ενός εγκληματολογικού αντιγράφου θα πρέπει να γίνεται πάντα με τον κατάλληλο εξοπλισμό (Write Blockers, κ.ά.) και σε κατάλληλο περιβάλλον (περιβάλλον εργαστηρίου, κ.τ.λ.), ώστε να αποφευχθούν τυχόν λάθη που ενδέχεται να προκαλέσουν αλλοίωση στο ψηφιακό πειστήριο (Santos 2015). Κατόπιν της δημιουργίας του εγκληματολογικού αντιγράφου, ακολουθεί η διαδικασία επαλήθευσης του. Είναι εξίσου απαραίτητο να διασφαλιστεί ότι το εγκληματολογικό αντίγραφο που δημιουργήθηκε είναι ένα πιστό και πλήρες αντίγραφο του ψηφιακού πειστηρίου και επομένως μπορεί να εξεταστεί αντί του. Επομένως, σε αυτή τη διαδικασία υπολογίζονται με χρήση συναρτήσεων κατακερματισμού, οι αλφαριθμητικές ταυτότητες μοναδικότητας τόσο του ψηφιακού πειστηρίου όσου και του εγκληματολογικού αντιγράφου (imageforensicexpert n.d.). Εάν αυτές οι δύο ταυτότητες ταυτίζονται, τότε αυτό σημαίνει ότι η αντιγραφή ήταν επιτυχής και το εγκληματολογικό αντίγραφο αποτελεί ένα πιστό αντίγραφο του ψηφιακού πειστηρίου. Οι συναρτήσεις κατακερματισμού που συνήθως χρησιμοποιούνται από τους ερευνητές είναι δύο, η συνάρτηση MD5 (Message Digest 5) και η SHA1 (Secure Hashing Algorithm SHA-1).

Στον προαναφερθέν κανόνα περί εξέτασης των συσκευών που συνιστούν ψηφιακά πειστήρια, υπάρχουν αναπόφευκτα εξαιρέσεις. Παραδείγματος χάρη, όταν απουσιάζει ο απαραίτητος τεχνολογικός εξοπλισμός (υλισμικό και λογισμικό) για τη δημιουργία του εγκληματολογικού αντιγράφου, ο ερευνητής ίσως χρειαστεί να ενεργήσει επί του αρχικού ψηφιακού πειστηρίου. Ακόμα και για αυτές τις περιπτώσεις όμως, ο ερευνητής δεσμεύεται να ακολουθήσει συγκεκριμένες διαδικασίες ώστε η παρεμβολή του στα αρχικά δεδομένα να είναι η ελάχιστη δυνατή.

2.4. Η διεργασία της εγκληματολογικής εξέτασης

Σε αυτό το σημείο έχει υπογραμμιστεί τόσο η σημασία της δημιουργίας ενός εγκληματολογικού αντιγράφου όσο και η ευαισθησία που παρουσιάζει ένα ψηφιακό πειστήριο στη μεταχείριση του. Επίσης, όπως αναφέρθηκε και ανωτέρω, προκειμένου ένας ερευνητής να μπορεί να ανταπεξέλθει στο δυναμικό περιβάλλον μίας εγκληματολογικής έρευνας και εξέτασης, ακολουθεί πιστά σαφώς ορισμένες διαδικασίες. Το σύνολο των εν λόγω διαδικασιών απαρτίζουν ένα μοντέλο διεργασίας (process model) της ψηφιακής εγκληματολογίας.

Τα μοντέλα αυτά εξυπηρετούν στην ορθή εφαρμογή της ψηφιακής εγκληματολογίας στην πράξη. Στη διεθνή κοινότητα υπάρχει μεγάλη ποικιλία αναγνωρισμένων μοντέλων διεργασίας. Η ύπαρξη διαφορετικών μοντέλων διεργασίας οφείλεται στο γεγονός ότι, τα περισσότερα μοντέλα προορίζονται είτε για συγκεκριμένους χρήστες (αρχές επιβολής του νόμου, εταιρικό περιβάλλον, κ.ά.) ή για συγκεκριμένο είδος ψηφιακών συσκευών (π.χ. έρευνα σε «έξυπνο» κινητό), καθιστώντας αδύνατη την καθολική χρήση ενός εξ αυτών. Επιπρόσθετα, υπάρχουν επιπλέον παράμετροι που ένας ερευνητής συνυπολογίζει, προκειμένου να επιλέξει το μοντέλο διεργασίας που τον εξυπηρετεί καλύτερα. Ενδεικτικά αναφέρονται παράμετροι όπως η προθεσμία για την εξέταση της υπόθεσης, το πλήθος των ψηφιακών πειστηρίων και το είδος της υπόθεσης που διερευνάται. Υπάρχουν λοιπόν μοντέλα διεργασίας αποτελούμενα από τέσσερις διαδικασίες (Συλλογή, Διατήρηση, Ανάλυση και Παρουσίαση) αλλά υπάρχουν και μοντέλα διεργασίας με αρκετές παραπάνω διαδικασίες.

Ο σημαντικότερος λόγος για τον οποίο χρησιμοποιούνται τα διάφορα μοντέλα διεργασίας είναι η εξασφάλιση μιας πιο πλήρους, ακριβούς και αποτελεσματικής εγκληματολογικής εξέτασης. Επισημαίνεται ότι, απλά και μόνο η χρήση ενός τέτοιου μοντέλου δεν συνεπάγεται αυτόματα και την αποδοχή των πειστηρίων και των ευρημάτων στο δικαστήριο, πλην όμως τα μοντέλα αυτά αποτελούν μία αξιόπιστη και πρακτική βάση για τον ερευνητή. Ένας ερευνητής που πραγματοποιεί την εξέταση του ακολουθώντας καθιερωμένα μοντέλα και διαδικασίες, έχει περισσότερες πιθανότητες για μία σύννομη και πιο ολοκληρωμένη έρευνα από εκείνον που στηρίζεται ως επί το πλείστον στο ένστικτό του.

Για μόρφωση άποψης και για τους σκοπούς της παρούσας διπλωματικής εργασίας, παρουσιάζεται κάτωθι ένα από τα διαθέσιμα μοντέλα διεργασίας της ψηφιακής εγκληματολογίας. Το κριτήριο επιλογής του ήταν το περιβάλλον εξέτασης που πραγματεύεται (cloud forensics). Από την αξιοποίηση των ευρημάτων που προέκυψαν κατά την αξιολόγηση (Du et al. 2017, Milagre and Caiado 2013, Mitrou et al. 2012, Simou et al. 2015) των σχετικών μοντέλων, το μοντέλο που επιλέχθηκε να παρουσιαστεί, είναι αυτό των Martini και Choo (Martini and Choo 2012).

2.4.1. Ένα μοντέλο διεργασίας για εξέταση στο Νέφος

Ένα μοντέλο διεργασίας αποτελείται από επί μέρους διαδικασίες. Το πλήθος των διαδικασιών αλλά και οι ονομασίες αυτών, διαφοροποιούνται ανάλογα με το επιλεγμένο μοντέλο διεργασίας. Η κάθε διαδικασία με τη σειρά της απαρτίζεται από καθορισμένα στάδια-βήματα, τα οποία όταν ολοκληρωθούν σημάνουν και την ολοκλήρωση της

διαδικασίας. Για κάθε διαδικασία ενός μοντέλου, υπάρχουν ποικίλες περαιτέρω μεθοδολογίες και προτεινόμενες πρακτικές, δεδομένου ότι δεν επεξηγούνται επαρκώς στην περιγραφή του μοντέλου.

Το μοντέλο των Martini και Choo στηρίχθηκε στα μοντέλα των McKemmish (McKemmish 1999) και του NIST (Grance et al. 2006) και σκοπό είχε την αντιμετώπιση των προκλήσεων της ψηφιακής εγκληματολογίας σε περιβάλλον υπολογιστικού νέφους. Ειδικότερα η καινοτομία του βρισκόταν στην προσθήκη μίας επιπλέον διαδικασίας κατά την οποία, σε περίπτωση εντοπισμού ευρημάτων που σχετίζονταν με το νέφος, η διεργασία επαναλαμβανόταν εκ νέου χρησιμοποιώντας τα ευρήματα που προέκυψαν. Η δεύτερη επανάληψη της διεργασίας ενεργούνταν παράλληλα με την πρώτη και άρχιζε από τη διαδικασία της αναγνώρισης και διατήρησης των πηγών αποδεικτικής πληροφορίας στο νέφος. Εάν κατά την εξέταση και ανάλυση του νέφους, νέα ευρήματα προέκυπταν, μία τρίτη επανάληψη θα ξεκινούσε. Το εν λόγω μοντέλο παρουσιάζεται κάτωθι συνοπτικά (παρατίθεται σε μετάφραση):

- **Αναγνώριση και διατήρηση πηγών αποδεικτικής πληροφορίας** (Evidence source identification and preservation): Η διαδικασία αυτή αφορά την αναγνώριση των διαφόρων πηγών αποδεικτικής πληροφορίας. Κατά την πρώτη επανάληψη, πιθανές πηγές αποδεικτικών στοιχείων αποτελούν τα ψηφιακά πειστήρια (Η/Υ, κινητές συσκευές, κ.ά.). Κατά τη δεύτερη επανάληψη, η διαδικασία αυτή αφορά την αναγνώριση πιθανών αποδεικτικών στοιχείων που είναι αποθηκευμένα στο νέφος καθώς και τη διατήρηση αυτών.

- **Συλλογή** (Collection): Η διαδικασία αυτή αφορά τη συλλογή της αποδεικτικής πληροφορίας για τη μετέπειτα εξέταση της. Σε αυτή δημιουργούνται και τα απαραίτητα εγκληματολογικά αντίγραφα των ψηφιακών πειστηρίων που θα αξιοποιηθούν στην επακόλουθη εξέταση τους. Αναμφίβολα, ανάλογα με το μοντέλο της υπηρεσίας του νέφους (IaaS,PaaS,SaaS) που εντοπίστηκε, θα υπάρχει αντίστοιχη ποικιλία στο πλήθος των αποδεικτικών στοιχείων που μπορούν να συλλεχθούν.

- **Εξέταση και Ανάλυση** (Examination and Analysis): Η διαδικασία αυτή αφορά την εξέταση και την ανάλυση της αποδεικτικής πληροφορίας που συλλέχθηκε στην προηγούμενη διαδικασία. Σε αυτή τη διαδικασία αναμένεται να προκύψουν τυχόν ευρήματα που σχετίζονται με υπηρεσίες υπολογιστικού νέφους. Εάν προκύψουν τότε ικανοποιείται η συνθήκη εκτέλεσης της κατωτέρω διαδικασίας.

- **Επανάληψη Διεργασίας** (Iteration): Η διαδικασία αυτή ενεργοποιείται υπό την προϋπόθεση ότι στο στάδιο της ανάλυσης και εξέτασης προέκυψαν ευρήματα που να σχετίζονται με το νέφος. Κατά την εκτέλεση της διαδικασίας αυτής, επαναλαμβάνεται η διεργασία από την αρχή.

- **Αναφορά και Παρουσίαση** (Reporting and Presentation): Η διαδικασία αυτή αφορά τη νομική παρουσίαση των ευρημάτων που προέκυψαν στα προηγούμενα στάδια.

Όπως επισημάνθηκε και ανωτέρω, κάθε διαδικασία αποτελείται από επί μέρους στάδια-βήματα. Για την περαιτέρω κατανόηση των βημάτων αυτών, υπάρχει πλήθος μεθοδολογιών και προτεινόμενων πρακτικών. Το πλήθος των βημάτων που αντιστοιχούν σε μία διαδικασία δεν είναι σταθερό, αλλά εξαρτάται από τη μεθοδολογία που χρησιμοποιείται. Για παράδειγμα, η διαδικασία της «συλλογής» (collection) της αποδεικτικής πληροφορίας μπορεί να επιτευχθεί σε τρία, τέσσερα ή και παραπάνω βήματα, ανάλογα με το ποια μεθοδολογία ακολουθείται.

Γίνεται κατανοητό επομένως ότι, ακόμα και για την επεξήγηση των βημάτων μίας μόνο διαδικασίας, δεν υπάρχει μία καθολική προσέγγιση. Για την ακρίβεια, κάθε μεθοδολογία δύναται να εμβαθύνει σε διαφορετικές πτυχές της περιγραφόμενης διαδικασίας και ως εκ τούτου να διαφοροποιείται από μία άλλη. Στο παράδειγμα με τη διαδικασία της «Συλλογής», διαφορετική μεθοδολογία ακολουθείται όταν ένας υπολογιστής είναι κλειστός (post mortem) και διαφορετική όταν βρίσκεται σε λειτουργία (live). Παρακάτω παρουσιάζεται μία διεθνής μεθοδολογία που εμβαθύνει στις διαδικασίες της «Αναγνώρισης και διατήρησης πηγών αποδεικτικής πληροφορίας» και της «Συλλογής» (ISO/IEC 2016). Η εν λόγω μεθοδολογία αναλύεται όσον αφορά τη διαδικασία της «Συλλογής».

2.4.2. Μεθοδολογία για τη διαδικασία της «Συλλογής»

Με την εδραίωση της επιστήμης της ψηφιακής εγκληματολογίας, ολοένα και περισσότεροι Οργανισμοί που έκτοτε δραστηριοποιούνται στο αντικείμενο αυτό, έκαναν την εμφάνιση τους. Οι περισσότεροι από αυτούς έχουν κατά καιρούς εκδώσει τις δικές τους μεθοδολογίες και προτεινόμενες πρακτικές.

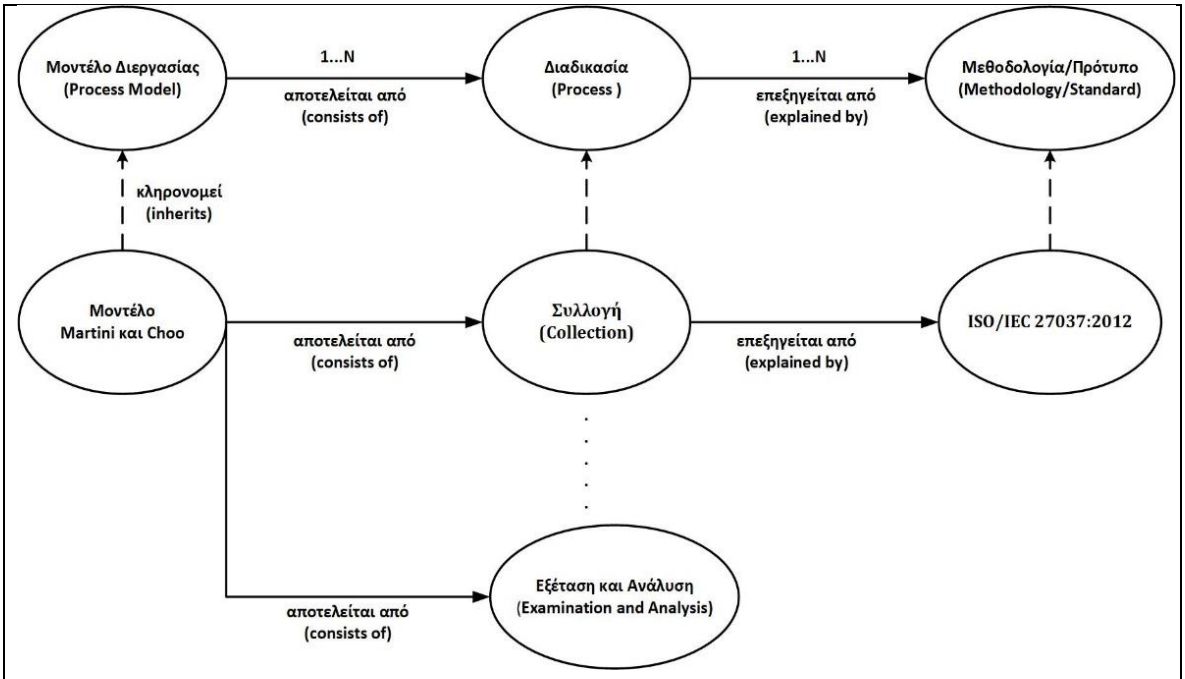
Το 2012, ο Οργανισμός ISO προχώρησε στην προτυποποίησή των διαδικασιών της ψηφιακής εγκληματολογίας (ISO/IEC 2016), με απώτερο σκοπό να συνδυάσει όλες τις υπάρχουσες μεθοδολογίες σε ένα ενιαίο πρότυπο. Ακολουθώντας το πρότυπο ISO/IEC 27037:2012, ένας ερευνητής θα βρει μία βελτιωμένη μεθοδολογία που εμβαθύνει μεταξύ άλλων, στη διαδικασία της «Συλλογής» της αποδεικτικής πληροφορίας.

Ειδικότερα, στο πρότυπο περιγράφονται οι ενέργειες στις οποίες πρέπει να προβεί ο ερευνητής κατά τη «Συλλογή» των ψηφιακών πειστηρίων. Οι συσκευές που αναγνωρίζονται στο ανωτέρω πρότυπο, χωρίζονται σε δύο βασικές κατηγορίες, οι οποίες και παρουσιάζονται κάτωθι συνοπτικά (παρατίθενται σε μετάφραση):

- **Ψηφιακές συσκευές σε κατάσταση λειτουργίας** (powered on digital devices): Για τις συσκευές που ανήκουν στην κατηγορία αυτή, στο πρότυπο προτείνονται κάποιες βασικές ενέργειες όσον αφορά τη συλλογή τους και τη δημιουργία των εν θέματι εγκληματολογικών αντιγράφων αυτών. Συμπληρωματικά προτείνονται και ορισμένες πρόσθετες ενέργειες που ενδέχεται να βοηθήσουν τον ερευνητή.

- **Ψηφιακές συσκευές σε κατάσταση εκτός λειτουργίας** (powered off digital devices): Αντίστοιχα και για όσες συσκευές ανήκουν σε αυτή την κατηγορία, προτείνονται κάποιες βασικές ενέργειες όσον αφορά τη συλλογή τους και τη δημιουργία των εν θέματι εγκληματολογικών αντιγράφων τους. Παράλληλα προτείνονται και ορισμένες πρόσθετες ενέργειες που ενδέχεται να βοηθήσουν τον ερευνητή.

Όπως συμβαίνει και με τα διάφορα μοντέλα διεργασίας, ο ερευνητής που στηρίζεται σε ένα τέτοιο πρότυπο κατά τη διεξαγωγή της έρευνας του, εξασφαλίζει μία πιο ολοκληρωμένη έρευνα υπό κάθε έννοια. Για την καλύτερη κατανόηση του πώς συνδέονται τα προαναφερόμενα μοντέλα διεργασίας, οι περιεχόμενες διαδικασίες αυτών καθώς και οι περαιτέρω επεξηγηματικές μεθοδολογίες των εν λόγω διαδικασιών, απεικονίζεται κάτωθι η εννοιολογική σχέση τους (Βλ. Εικόνα 1):



1...N: Δηλώνει τη σχέση «ένα προς πολλά»

Εικόνα 1

Εννοιολογική σχέση των οντοντήτων που απαρτίζουν τη διεργασία της Ψηφιακής Εγκληματολογίας

Συνοψίζοντας όλα τα ανωτέρω, εξάγεται το συμπέρασμα ότι η ψηφιακή εγκληματολογία χαρακτηρίζεται από ποικιλομορφία και μπορεί να γίνει μία αρκετά πολύπλοκη και επίπονη διεργασία για τον ερευνητή, αν εκείνος δεν ακολουθήσει τα σαφώς καθορισμένα βήματα που αναλύονται στις διαθέσιμες μεθοδολογίες.

2.5. Κατηγορίες Ψηφιακής Εγκληματολογίας

Η συνεχής διεύρυνση και διαφοροποίηση των αξιοποιήσιμων πηγών αποδεικτικής πληροφορίας στη δικανική πληροφορική, καθιστούσε αναγκαίο τον διαχωρισμό του κλάδου σε κατηγορίες. Ο σκοπός του διαχωρισμού αυτού ήταν η ενδελεχής μελέτη της κάθε κατηγορίας ξεχωριστά και η περαιτέρω εξέλιξη τόσο των διαθέσιμων μοντέλων διεργασίας που την αφορούν όσο και των πρότυπων διαδικασιών που τη διέπουν. Οι κυριότερες κατηγορίες που υπάρχουν καταγεγραμμένες στη διεθνή βιβλιογραφία όσον αφορά τη δικανική πληροφορική, παρουσιάζονται κάτωθι:

- **Ψηφιακή εγκληματολογία υπολογιστών** (Computer Forensics): Το αντικείμενο μελέτης της κατηγορίας αυτής είναι η εγκληματολογική εξέταση ψηφιακών συσκευών τύπου υπολογιστή (κεντρική μονάδα υπολογιστή, φορητό υπο-

λογιστή, διακομιστή server, κ.ά.). Επισημαίνεται ότι στην κατηγορία αυτή εννοιολογικά ανήκουν και υποκατηγορίες όπως η εγκληματολογική εξέταση βάσεων δεδομένων.

- **Ψηφιακή εγκληματολογία δικτύων** (Network Forensics): Το αντικείμενο μελέτης της κατηγορίας αυτής περιλαμβάνει την επίβλεψη, τη συλλογή και την ανάλυση της δραστηριότητας ενός δικτύου συνδεδεμένων ψηφιακών συσκευών. Ο σκοπός της εν λόγω εγκληματολογικής εξέτασης είναι η ανίχνευση επιθέσεων παραβίασης ασφαλείας, ο εντοπισμός τυχόν εισβολέων και η διασταύρωση της προέλευσης μίας ενδεχόμενης επίθεσης. Αξίζει να τονιστεί ότι το μεγαλύτερο μέρος των δεδομένων που εξετάζονται σε αυτή την κατηγορία είναι πτητικά (volatile data) και συνεπώς το περιβάλλον της εξέτασης θεωρείται αρκετά δυναμικό. Είναι από τις λίγες κατηγορίες της ψηφιακής εγκληματολογίας που χρησιμοποιείται και προληπτικά.

- **Ψηφιακή εγκληματολογία κινητών συσκευών** (Mobile Forensics): Το αντικείμενο μελέτης της κατηγορίας αυτής είναι η εγκληματολογική εξέταση κινητών συσκευών. Η διαφοροποίηση της κατηγορίας αυτής από την αντίστοιχη κατηγορία των υπολογιστών, έγκειται στο ότι οι εν λόγω κινητές συσκευές εκτός του λειτουργικού τους συστήματος, φέρουν επιπλέον ενσωματωμένο σύστημα επικοινωνίας (π.χ. 3G). Η εν λόγω ιδιαιτερότητα συνθέτει ένα εντελώς διαφορετικό περιβάλλον εξέτασης και επομένως κρίθηκε σκόπιμος ο διαχωρισμός τους.

- **Ψηφιακή εγκληματολογία σε «ζωντανό» περιβάλλον** (Live Forensics): Το αντικείμενο μελέτης της κατηγορίας αυτής είναι η εγκληματολογική εξέταση η οποία λαμβάνει χώρα σε συστήματα που βρίσκονται σε κατάσταση λειτουργίας. Ειδικότερα, η εγκληματολογική εξέταση σε «ζωντανό» περιβάλλον στοχεύει στην εξαγωγή πτητικών δεδομένων είτε από την κύρια μνήμη (μνήμη RAM) του συστήματος ή από δευτερεύουσες πηγές πτητικών δεδομένων (μνήμη cache, pagefile.sys, κ.ά.). Επισημαίνεται ότι η εν λόγω κατηγορία ξεκίνησε σαν υποκατηγορία της ψηφιακής εγκληματολογίας υπολογιστών αλλά με την πάροδο του χρόνου, την αύξηση της χωρητικότητας της μνήμης RAM και της διεύρυνσης των πτητικών δεδομένων που μπορούν να αποθηκευτούν σε αυτή (ευρήματα σχετικά με την κρυπτογράφηση αρχείων, ίχνη στεγανογραφίας, στοιχεία εισόδου των χρηστών, κ.ά.) διαχωρίστηκε από αυτή και σχημάτισε μία νέα κατηγορία. Συχνά αναφέρεται και ως ψηφιακή εγκληματολογία

μνήμης (memory forensics).

- **Ψηφιακή εγκληματολογία συσκευών IoT** (IoT Forensics): Το αντικείμενο μελέτης της κατηγορίας αυτής είναι η εγκληματολογική εξέταση ψηφιακών συσκευών που ανήκουν στην κατηγορία «Internet of Things-IoT». Η εν λόγω κατηγορία αποτελεί την τελευταία προσθήκη στις κατηγορίες ψηφιακής εγκληματολογίας.

- **Ψηφιακή εγκληματολογία στο Νέφος** (Cloud Forensics): Το αντικείμενο μελέτης της κατηγορίας αυτής είναι η εγκληματολογική εξέταση στο νέφος. Αρχικά η ψηφιακή εγκληματολογία στο νέφος είχε χαρακτηριστεί ως υποκατηγορία της ψηφιακής εγκληματολογίας δικτύων (Ruan et al. 2011b), καθώς η τεχνολογία στην οποία βασίζεται το υπολογιστικό νέφος απαιτεί εκτεταμένη χρήση δικτυακής κίνησης και η δικτυακή δραστηριότητα είναι αντικείμενο μελέτης της εν λόγω κατηγορίας. Παρόλα αυτά όμως, όπως επισημάνθηκε (Zawoad and Hasan 2013) η ψηφιακή εγκληματολογία στο νέφος περιλαμβάνει πρόσθετες πηγές δεδομένων, όπως οι τρέχουσες διεργασίες (processes) του συστήματος, τυχόν εγγραφές στο μητρώο καταγραφής (registry), κ.ά. που καθιστούν τον ανωτέρω χαρακτηρισμό ελλιπή για την κατηγορία αυτή. Η κατηγορία αυτή εξετάζεται στην παρούσα διπλωματική εργασία.

Έχοντας αποκτήσει μία σφαιρική άποψη για την έννοια της ψηφιακής εγκληματολογίας, του ψηφιακού πειστηρίου και γενικά για τα χαρακτηριστικά γνωρίσματα της επιστήμης αυτής, θα περιγραφεί στη συνέχεια η τεχνολογία του υπολογιστικού νέφους, τα διάφορα μοντέλα των υπηρεσιών της, καθώς και τα βασικά χαρακτηριστικά κάθε μοντέλου υπηρεσίας που προσφέρει.

Κεφάλαιο 3ο: Υπολογιστικό Νέφος

3.1. Γενικά

Η δημιουργία του υπολογιστικού νέφους άλλαξε για πάντα το ρου της ιστορίας της Πληροφορικής. Αν και η ιδέα πρωτοεμφανίστηκε τη δεκαετία του 1960 (Destefani Neto 2014), το υπολογιστικό νέφος υλοποιήθηκε με τη σημερινή μορφή και ονομασία του στις αρχές του 2000.

Ο ορισμός που δίνει ο NIST (Mell and Grance 2011) για το υπολογιστικό νέφος είναι ο εξής (παρατίθεται σε μετάφραση): «*Το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την πανταχού παρούσα, βολική, κατά παραγγελία δικτυακή πρόσβαση σε ένα κοινόχρηστο χώρο από ρυθμιζόμενες υπολογιστικές πηγές (π.χ. δίκτυα, διακομιστές server, αποθήκευση, εφαρμογές και υπηρεσίες), οι οποίες μπορούν να παρασχεθούν γρήγορα και να απελευθερωθούν με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης με τον πάροχο της υπηρεσίας. Αυτό το μοντέλο νέφους συντίθεται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης*».

Στο υπόλοιπο κεφάλαιο θα παρουσιαστούν διαδοχικά, τα βασικά χαρακτηριστικά του υπολογιστικού νέφους όπως αυτά προκύπτουν από τον ανωτέρω ορισμό, τα μοντέλα υπηρεσίας με τα οποία διατίθεται καθώς και τα μοντέλα ανάπτυξης του.

3.2. Χαρακτηριστικά του υπολογιστικού νέφους

Ως απόρροια του ανωτέρω δοθέντα ορισμού για το υπολογιστικό νέφος και σύμφωνα πάντα με την προσέγγιση του Οργανισμού NIST (Ruan et al. 2011a), προκύπτουν πέντε (5) βασικά χαρακτηριστικά που σχετίζονται με την εν λόγω τεχνολογία, τα οποία περιγράφονται κάτωθι συνοπτικά (παρατίθενται σε μετάφραση):

- **Κατά παραγγελία υπηρεσία** (on-demand self-service): Ένας καταναλωτής μπορεί να αποκτά αυτομάτως πρόσβαση σε υπολογιστικούς πόρους που επιθυμεί, όπως η δικτυακή αποθήκευση και η δέσμευση χρόνου στο διακομιστή server, χωρίς να απαιτείται ανθρώπινη παρέμβαση από πλευράς παρόχου της υπηρεσίας (Cloud Service Provider, εφεξής CSP).

- **Ευρεία δικτυακή πρόσβαση** (broad network access): Οι υπολογιστικές δυνατότητες είναι διαθέσιμες μέσω του δικτύου και είναι προσβάσιμες διαμέσου πρότυπων μηχανισμών οι οποίοι προωθούν τη χρήση από ετερογενείς πλατφόρμες εκ μέρους του πελάτη (π.χ. κινητά τηλέφωνα, συσκευές τύπου tablets, φορητοί Η/Υ αλλά και κεντρικές μονάδες Η/Υ).

- **Συγκέντρωση πόρων** (resource pooling): Οι υπολογιστικοί πόροι του παρόχου συγκεντρώνονται προκειμένου να εξυπηρετούν πολλαπλούς καταναλωτές ταυτόχρονα, χρησιμοποιώντας ένα μοντέλο «πολλαπλών-ενοικιαστών» (multi-tenant), όπου οι διάφοροι φυσικοί και εικονικοί πόροι ανατίθενται και επανατίθενται δυναμικά, σύμφωνα με τη ζήτηση του καταναλωτή. Υπάρχει μια αίσθηση ανεξαρτησίας ως προς την τοποθεσία, δεδομένου ότι ο πελάτης γενικά δεν έχει κανέναν έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά είναι σε θέση να προσδιορίσει την τοποθεσία σε υψηλότερο επίπεδο αφαίρεσης (π.χ. χώρα, πολιτεία ή κέντρο δεδομένων). Παραδείγματα πόρων αποτελούν η αποθήκευση, η επεξεργασία, η μνήμη και το εύρος ζώνης (bandwith).

- **Ταχεία ελαστικότητα** (rapid elasticity): Οι δυνατότητες μπορούν να δεσμευτούν αλλά και να απελευθερωθούν με ελαστικότητα και σε ορισμένες περιπτώσεις αυτόματα, έτσι ώστε να εμφανίζεται άμεσα η μη διαθεσιμότητα ή η απελευθέρωση τους, ανάλογα πάντα με τη ζήτηση. Από την πλευρά του καταναλωτή, οι υπολογιστικές δυνατότητες που εμφανίζονται διαθέσιμες για δέσμευση παρουσιάζονται συχνά ως απεριόριστες και μπορούν να διατεθούν σε οποιαδήποτε ποσότητα ανά πάσα χρονική στιγμή.

- **Μετρήσιμη παροχή υπηρεσίας** (measured service): Τα συστήματα νέφους ελέγχουν αυτόματα και βελτιστοποιούν τη χρήση των πόρων, αξιοποιώντας τη δυνατότητα μετρήσεων (σε αφαιρετικό επίπεδο), ανάλογα με τον τύπο υπηρεσίας (π.χ. αποθήκευση, επεξεργασία, εύρος ζώνης και ενεργοί λογαριασμοί χρηστών). Η χρήση των πόρων μπορεί να παρακολουθείται, να ελέγχεται και να περιλαμβάνεται σε αναφορές, παρέχοντας διαφάνεια τόσο για τον πάροχο όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας.

Από όλα τα παραπάνω γίνεται φανερό ότι το υπολογιστικό νέφος αποτελεί αμάλγαμα τεχνολογικών επιτευγμάτων, τα οποία συνδυάζονται και συνθέτουν την τελική του μορφή. Στη συνέχεια παρουσιάζονται τα βασικά μοντέλα υπηρεσίας με τα οποία διατίθεται το νέφος στην αγορά. Ο διαχωρισμός τους γίνεται ανάλογα με το είδος υπηρεσίας που προσφέρουν.

3.3. Μοντέλα υπηρεσίας του υπολογιστικού νέφους

Οι υπηρεσίες που έχει τη δυνατότητα να υποστηρίζει το υπολογιστικό νέφος είναι πολλές και ποικίλουν μεταξύ τους. Το γεγονός αυτό, οδήγησε στη συγκέντρωση των

υπηρεσιών αυτών σε διακριτά μοντέλα υπηρεσίας, καθένα εκ των οποίων υποστηρίζει ένα διαφορετικό πακέτο παρεχόμενων υπηρεσιών. Παρακάτω αναλύονται τα βασικά μοντέλα υπηρεσίας (υπάρχουν περισσότερα) με τα οποία διατίθενται οι υπηρεσίες υπολογιστικού νέφους στην αγορά, σύμφωνα με τον Οργανισμό NIST (Mell and Grance 2011) (παρατίθενται σε μετάφραση):

- **Υποδομή ως Υπηρεσία** (Infrastructure as a Service, IaaS): Στο μοντέλο αυτό, οι δυνατότητες που παρέχονται στον καταναλωτή είναι η επεξεργασία δεδομένων, η αποθήκευση δεδομένων, τα δίκτυα καθώς και άλλοι βασικοί υπολογιστικοί πόροι με τους οποίους ο καταναλωτής είναι σε θέση να αναπτύξει και να εκτελέσει αυθαίρετο (δηλ. που δεν προέρχεται από τον CSP) λογισμικό, στο οποίο συμπεριλαμβάνονται τυχόν λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει τη βασική υποδομή πάνω στην οποία λειτουργεί το νέφος, αλλά έχει τον πλήρη έλεγχο των λειτουργικών συστημάτων, της αποθήκευσης των δεδομένων και των εφαρμογών που αναπτύχθηκαν πάνω σε αυτή. Επιπλέον, ενδέχεται να ασκεί περιορισμένο έλεγχο σε επιλεγμένα στοιχεία του δικτύου (π.χ. firewalls υποδοχής).

- **Πλατφόρμα ως Υπηρεσία** (Platform as a Service, PaaS): Στο μοντέλο αυτό, η δυνατότητα που παρέχεται στον καταναλωτή είναι η ανάπτυξη εφαρμογών (που είτε δημιουργούνται από καταναλωτές ή αποκτώνται με άλλο τρόπο) πάνω στη βασική υποδομή του νέφους. Για τη δημιουργία των εν λόγω εφαρμογών χρησιμοποιούνται γλώσσες προγραμματισμού, βιβλιοθήκες, υπηρεσίες και εργαλεία που υποστηρίζονται από τον πάροχο της υπηρεσίας. Ο καταναλωτής και σε αυτό το μοντέλο δεν διαχειρίζεται ούτε ελέγχει την υποδομή πάνω στην οποία λειτουργεί το νέφος, συμπεριλαμβανομένου του δικτύου, των εξυπηρετητών (server), των λειτουργικών συστημάτων και του χώρου αποθήκευσης των δεδομένων, αλλά έχει τον έλεγχο των εφαρμογών που αναπτύχθηκαν και ενδεχομένως τον έλεγχο των ρυθμίσεων των παραμέτρων που αφορούν το περιβάλλον φιλοξενίας τους.

- **Λογισμικό ως Υπηρεσία** (Software as a Service, SaaS): Στο μοντέλο αυτό το οποίο αποτελεί και το μοντέλο που διερευνάται στην παρούσα διπλωματική εργασία, η δυνατότητα που παρέχεται στον καταναλωτή είναι η χρήση εφαρμογών που έχει αναπτύξει ο πάροχος και εκτελούνται σε υποδομή νέφους. Οι εν λόγω εφαρμογές είναι προσβάσιμες από διάφορες συσκευές (όπως «έξυπνα» κινητά, υπολογιστές, κ.τ.λ.), είτε μέσω της χρήσης ενός προγράμματος

περιήγησης Ιστού ή μέσω της χρήσης σχετικής διεπαφής που προσφέρει ο πάροχος της υπηρεσίας. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει την υποδομή πάνω στην οποία λειτουργεί το νέφος, συμπεριλαμβανομένου του δικτύου, των εξυπηρετητών (server), των λειτουργικών συστημάτων και του χώρου αποθήκευσης των δεδομένων. Επιπρόσθετα, ο καταναλωτής δεν διαχειρίζεται ή ελέγχει ούτε μεμονωμένες δυνατότητες της εφαρμογής, με εξαίρεση ενδεχομένως, τις περιορισμένες ρυθμίσεις εξατομίκευσης χρήσης της εν λόγω εφαρμογής.

Τα ανωτέρω μοντέλα δεν είναι τα μοναδικά που υπάρχουν πλέον στην αγορά, πλην όμως αποτελούν τον πυρήνα των κατηγοριών των διαθέσιμων υπηρεσιών υπολογιστικού νέφους, πάνω στον οποίο βασίστηκαν τα νεότερα μοντέλα. Στη συνέχεια παρουσιάζονται τα μοντέλα ανάπτυξης των υπηρεσιών υπολογιστικού νέφους. Τα διαφορετικά μοντέλα ανάπτυξης του υπολογιστικού νέφους, διαχωρίζουν τους διαθέσιμους τρόπους με τους οποίους δύναται να χρησιμοποιήσει τις παρεχόμενες υπηρεσίες του ο καταναλωτής.

3.4. Μοντέλα ανάπτυξης του υπολογιστικού νέφους

Οι υπηρεσίες υπολογιστικού νέφους ταξινομούνται σε διακριτά μοντέλα ανάπτυξης με βάσει το ποιος έχει πρόσβαση στις παρεχόμενες υπηρεσίες και το ποιος είναι ο ιδιοκτήτης των παρεχόμενων υπηρεσιών. Τα μοντέλα ανάπτυξης που αναγνωρίζει ο Οργανισμός NIST (Mell and Grance 2011) παρουσιάζονται κάτωθι (παρατίθενται σε μετάφραση):

- **Δημόσιο νέφος**(Public Cloud): Στο εν λόγω μοντέλο ανάπτυξης, η υποδομή πάνω στην οποία λειτουργεί το νέφος προορίζεται για χρήση ανοικτού τύπου, δηλ. για χρήση από το ευρύ κοινό. Μπορεί να ανήκει, να διαχειρίζεται και να λειτουργεί από έναν επιχειρηματικό, ακαδημαϊκό ή κυβερνητικό Οργανισμό ή από κάποιο συνδυασμό αυτών. Βρίσκεται όμως πάντα εντός των εγκαταστάσεων του παρόχου της υπηρεσίας.

- **Ιδιωτικό νέφος** (Private Cloud): Στο εν λόγω μοντέλο ανάπτυξης, η υποδομή πάνω στην οποία λειτουργεί το νέφος προορίζεται για αποκλειστική χρήση από ένα Οργανισμό (ή εταιρεία), ο οποίος περιλαμβάνει πολλούς χρήστες. Μπορεί να ανήκει, να διαχειρίζεται και να λειτουργεί από τον Οργανισμό, ή από μία τρίτη οντότητα (third-party) ή από ένα συνδυασμό αυτών, και μπορεί να βρίσκεται εντός των εγκαταστάσεων ή και εκτός.

- **Κοινοτικό νέφος** (Community Cloud): Στο εν λόγω μοντέλο ανάπτυξης, η υποδομή πάνω στην οποία λειτουργεί το νέφος προορίζεται για αποκλειστική χρήση από μία συγκεκριμένη κοινότητα καταναλωτών που προέρχονται από Οργανισμούς (ή εταιρείες), οι όποιοι μοιράζονται κοινές ανησυχίες (π.χ. αποστολή, απαιτήσεις ασφαλείας, πολιτικές, ανησυχίες σχετικά με συμμόρφωση). Μπορεί να ανήκει, να διαχειρίζεται και να λειτουργεί από έναν ή περισσότερους από τους Οργανισμούς που απαρτίζουν την κοινότητα, ή από μία τρίτη οντότητα (third-party) ή από ένα συνδυασμό αυτών, και μπορεί να βρίσκεται εντός των εγκαταστάσεων ή και εκτός.

- **Υβριδικό νέφος** (Hybrid Cloud): Στο εν λόγω μοντέλο ανάπτυξης, η υποδομή πάνω στην οποία λειτουργεί το νέφος αποτελεί μία σύνθεση δύο ή περισσοτέρων διακριτών μοντέλων ανάπτυξης (ιδιωτικό, κοινοτικό, ή δημόσιο), τα οποία καίτοι παραμένουν ξεχωριστές οντότητες, συνδυάζονται μεταξύ τους μέσω τυποποιημένης ή ιδιόκτητης (proprietary) τεχνολογίας, η οποία επιτρέπει τη φορητότητα δεδομένων και εφαρμογών (π.χ. εξισορρόπηση του φόρτου εργασίας μεταξύ των νεφών λόγω υπερβολικού φορτίου σε ένα από αυτά).

Με την ολοκλήρωση των κεφαλαίων 2 και 3, έχουν αποσαφηνιστεί οι έννοιες της ψηφιακής εγκληματολογίας, του υπολογιστικού νέφους αλλά και της ψηφιακής εγκληματολογίας στο νέφος και ως εκ τούτου ο θεωρητικός στόχος [**Θ.1**] έχει επιτευχθεί. Μετά από αυτό, γίνεται περαιτέρω εμβάθυνση στην έννοια της ψηφιακής εγκληματολογίας στο νέφος και ειδικότερα στις τεχνικές προκλήσεις και τα νομικά ζητήματα που κάνουν την εμφάνιση τους κατά τη διάρκεια μίας δικανικής εξέτασης σε αυτό.

Κεφάλαιο 4ο: Ζητήματα ως προς την εγκληματολογική εξέταση στο Νέφος

4.1. Γενικά

Η δημοτικότητα και η ευρεία αποδοχή της τεχνολογίας του υπολογιστικού νέφους έκανε αναπόφευκτη τη χρήση του και σε παράνομες ενέργειες. Ειδικότερα τα τελευταία χρόνια παρατηρείται αύξηση στα ηλεκτρονικά εγκλήματα και στα κυβερνοεγκλήματα που εκμεταλλεύονται το νέφος τόσο ως στόχο όσο και ως μέσο τέλεσης τέτοιων εγκλημάτων.

Η τεχνολογία του υπολογιστικού νέφους εγείρει ποικίλα ζητήματα στην επιστήμη της Ψηφιακής Εγκληματολογίας. Αυτά τα ζητήματα χωρίζονται σε νομικά και τεχνικά, ανάλογα με το είδος τους. Ένας ερευνητής δικανικής πληροφορικής οφείλει να γνωρίζει τις ενδεχόμενες προκλήσεις με τις οποίες μπορεί να έρθει αντιμέτωπος σε μία ενδεχόμενη εγκληματολογική εξέταση στο νέφος. Στη διεθνή βιβλιογραφία έχει γίνει αξιόλογη προσπάθεια αφενός για τη καταγραφή όλων των προκλήσεων που παρουσιάζει η τεχνολογία του νέφους στην ψηφιακή εγκληματολογία και αφετέρου στο να επιλυθούν αρκετές από αυτές. Ωστόσο, επισημαίνεται ότι για να εξαλειφθούν τα ζητήματα αυτά δεν επαρκεί η χρήση μόνο τεχνολογικών ή νομοθετικών ή οργανωτικών μέτρων αλλά απαιτείται ένας συνδυασμός όλων αυτών.

Στο παρών κεφάλαιο θα γίνει σύντομη παρουσίαση των σημαντικότερων νομικών ζητημάτων και τεχνικών προκλήσεων που σχετίζονται με τη δικανική εξέταση στο νέφος. Ο ερευνητής εφόσον είναι σε θέση να αναγνωρίζει τα εμπόδια που πιθανότατα θα κληθεί να αντιμετωπίσει σε μία τέτοια εξέταση, έχει τη δυνατότητα να οργανώσει τις ενέργειες του καλύτερα.

4.2. Νομικά Ζητήματα

Όπως έχει προαναφερθεί, η δικανική πληροφορική δεδομένης και της χρήσης της, πρέπει να ακολουθεί πιστά το γράμμα του νόμου. Αναμφίβολα η τεχνολογία του υπολογιστικού νέφους δεν αποτελεί αρωγό σε αυτό το εγχείρημα. Τα βασικότερα νομικά ζητήματα (Kaur and Singh 2016, Leroux 2004, Liles et al. 2009, Mitrou and Karyda 2007, Mitrou et al. 2012, Reilly et al. 2010) που παρουσιάζονται σε μία δικανική εξέταση στο νέφος, παρατίθενται κάτωθι περιληπτικά:

- **Πολλαπλή Δικαιοδοσία** (Multi-Jurisdiction): Η γεωγραφική ανεξαρτησία που εκφράζει την τεχνολογία του υπολογιστικού νέφους δημιουργεί νομικά εμπό-

δια στην περίπτωση διάπραξης κάποιου εγκλήματος μέσω αυτού. Στη διερεύνηση εγκλημάτων στο νέφος, κανείς (εκτός του παρόχου της υπηρεσίας) δεν γνωρίζει την ακριβή τοποθεσία των πόρων που χρησιμοποιήθηκαν και επομένως δεν μπορεί να ξεκαθαριστεί ποιανού αρμοδιότητά είναι άσκηση της ποινικής δίωξης και κατ' επέκταση της εγκληματολογικής εξέτασης. Η γεωγραφική διασπορά των πόρων αυτών, έχει ως αποτέλεσμα την συνύπαρξη διαφορετικών νομοθετικών πλαισίων, ανάλογα με τη χώρα στην οποία βρίσκεται ο συγκεκριμένος πόρος. Αυτή η περίπτωση πολλαπλής δικαιοδοσίας, καθιστά προβληματική την εγκληματολογική εξέταση στο νέφος, αφού μέχρι σήμερα δεν υπάρχουν αποτελεσματικοί μέθοδοι διεθνούς συνεργασίας μεταξύ των εμπλεκομένων χωρών που να βοηθούν στην αντιμετώπιση αυτής της πρόκλησης, εκτός ελαχίστων εξαιρέσεων (James and Szewczyk 2017).

- **Πολλαπλοί Ενοικιαστές** (Multi-Tenancy): Ακόμα και αν εντοπιστεί η ακριβής τοποθεσία των πόρων οι οποίοι εμπλέκονται σε κάποια εγκληματική ενέργεια, ακόμα και αν προσδιοριστούν τα συγκεκριμένα επίμαχα ψηφιακά πειστήρια, η κατάσχεση τους δεν είναι τόσο απλή υπόθεση. Αυτό οφείλεται στην αρχιτεκτονική του υπολογιστικού νέφους και στη δυνατότητα που έχει ένα αποθηκευτικό μέσο να εξυπηρετεί περισσότερους από έναν ενοικιαστές ταυτόχρονα. Στην προκείμενη περίπτωση, αυτό σημαίνει ότι το ψηφιακό πειστήριο που ενδεχομένως εμπλέκεται στην παράνομη ενέργεια, φέρει αποθηκευμένα δεδομένα πολλών χρηστών και όχι μόνο του υπόπτου. Το γεγονός αυτό εμποδίζει την άμεση κατάσχεση του αφού με αυτό τον τρόπο παραβιάζονται τα δικαιώματα αλλά και η ιδιωτικότητα των υπόλοιπων χρηστών.

- **Εξάρτηση από τον πάροχο της υπηρεσίας** (Reliance on Cloud Service Provider): Αναπόφευκτα για να γίνει μία πλήρης εγκληματολογική εξέταση στο νέφος, χρειάζεται η συνδρομή του παρόχου της υπηρεσίας. Ειδικότερα, στα μοντέλα υπηρεσίας «Πλατφόρμα ως Υπηρεσία» και «Λογισμικό ως Υπηρεσία», ο πάροχος της υπηρεσίας είναι ο μόνος που έχει πρόσβαση σε αρχεία καταγραφής (αρχεία καταγραφής ενεργειών του χρήστη, αρχεία καταγραφής ηλεκτρονικών διευθύνσεων IP του χρήστη, κ.ά.) τα οποία είναι απαραίτητα για μία ολοκληρωμένη δικανική εξέταση στο νέφος. Η εξέταση του συνόλου των προαναφερθέντων δεδομένων οδηγεί με τη σειρά της στην εξαγωγή ασφαλέστερων συμπερασμάτων σχετικά με την υπό διερεύνηση υπόθεση. Ωστόσο ο πάροχος της υπηρεσίας, τις περισσότερες φορές δεν συνεργάζεται πρόθυμα με τις διω-

κτικές αρχές και αυτό έχει ως αποτέλεσμα να καθυστερεί υπερβολικά η συγκέντρωση των εν λόγω δεδομένων ή ακόμα χειρότερα να μην πραγματοποιείται ποτέ.

- **Ακεραιότητα δεδομένων** (Data Integrity): Ένα άλλο νομικό ζήτημα που προκύπτει κατά την εγκληματολογική εξέταση στο νέφος, αφορά το κατά πόσο τα αποδεικτικά στοιχεία που έχουν συλλεχθεί, έχουν τα απαραίτητα χαρακτηριστικά για να γίνουν αποδεκτά στο δικαστήριο. Όπως υπογραμμίστηκε και στο κεφάλαιο 2, η ακεραιότητα των δεδομένων αποτελεί προτεραιότητα σε μία εγκληματολογική εξέταση. Η υποδομή πάνω στην οποία λειτουργεί το νέφος στηρίζεται σε ένα πολύ δυναμικό περιβάλλον, όπου τα δεδομένα συνεχώς μεταβάλλονται. Αυτό το δυναμικό περιβάλλον κάνει εξαιρετικά δύσκολη την εξασφάλιση της εκ νέου αναπαραγωγής (reproducibility) των δεδομένων που συλλέγονται. Αυτό πρακτικά σημαίνει ότι τα αποδεικτικά στοιχεία που έχουν συλλεχθεί σε μία δεδομένη χρονική στιγμή στο νέφος, δεν μπορούν να συλλεχθούν ξανά στο μέλλον όπως ακριβώς ήταν, αντίθετα από ότι συμβαίνει με τα δεδομένα που προκύπτουν από συμβατικά ψηφιακά πειστήρια (π.χ. τα δεδομένα ενός σκληρού δίσκου).

Τα ανωτέρω προβλήματα δεν είναι τα μοναδικά νομικά ζητήματα που έχει να αντιμετωπίσει ο ερευνητής ψηφιακής εγκληματολογίας κατά την εγκληματολογική εξέταση στο νέφος, πλην όμως αποτελούν τα κυριότερα εξ αυτών.

Παρόλο που η ολοκληρωτική επίλυση των ανωτέρω νομικών ζητημάτων δεν αναμένεται σύντομα, αρκετές χώρες έχουν θεσπίσει νόμους για την αντιμετώπιση ορισμένων εξ αυτών. Παραδείγματος χάρη, στο ελληνικό ποινικό δίκαιο έχει θεσπιστεί ο νόμος Ν. 4267/2014. Σύμφωνα με το άρθρο 2 του εν λόγω νόμου, η έννοια του τόπου τέλεσης (Άρθρο 5 Π. Κ.) μίας άδικης πράξης, βάσει της οποίας καθορίζεται και η αρμοδιότητα ασκήσεως της ποινικής δίωξης, διευρύνεται ως εξής ("Καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις."): «*Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφός της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους*». Με αυτόν τον τρόπο, επιτυγχάνεται και μερική επίλυση του προβλήματος πολλαπλής δικαιοδοσίας στο περιβάλλον του υπολογιστικού νέφους, όταν η πρόσβαση στα μέσα αυτά είναι διαθέσιμη στον ελλαδικό χώρο. Ο νόμος αυτός είναι εξαιρετικά χρήσιμος σε μία εγκληματολογική εξέταση στο μοντέλο «Λογισμικό ως Υπηρεσία», καθώς δεν απαιτείται επιπλέον νομική δικαιοδοσία για τη συλλογή και εξέταση των δεδομένων του κα-

τηγορούμενου που είναι αποθηκευμένα στο νέφος του, εφόσον υπάρχει νομική εξουσιοδότηση για τη συλλογή και εξέταση των ψηφιακών πειστηρίων που βρίσκονται στην κατοχή του. Ωστόσο, η συλλογή και η εξέταση τους θα πρέπει να γίνει με ιδιαίτερη προσοχή. Τέλος ο νόμος αυτός, αν και είναι όπως αναφέρθηκε πολύ χρήσιμος, δεν παύει να δημιουργεί νέα προβλήματα (Πριλή 2018).

Εκτός όμως από τα νομικά ζητήματα, ο ερευνητής έχει να ανταπεξέλθει και σε διάφορες τεχνικές προκλήσεις που εγείρει η τεχνολογία του υπολογιστικού νέφους και οι οποίες παρατίθενται στη συνέχεια.

4.3. Τεχνικές Προκλήσεις

Οι τεχνικές προκλήσεις που προκύπτουν κατά τη δικανική εξέταση στο νέφος, αποτελούν ένα ακόμη εμπόδιο για τον ερευνητή. Οι βασικότερες τεχνικές προκλήσεις (Arafat et al. 2017) συγκεντρώθηκαν στο παρακάτω απόσπασμα και περιγράφονται εν συντομία:

- **Ακεραιότητα δεδομένων** (Data Integrity): Το συγκεκριμένο πρόβλημα καίτοι αναφέρθηκε ως νομικό ζήτημα, αποτελεί εξίσου και τεχνική πρόκληση για τον ερευνητή. Η εξασφάλιση της ακεραιότητας των δεδομένων σε ένα δυναμικό περιβάλλον πολλαπλών ενοικιαστών (multi-tenants), όπου τα δεδομένα μοιράζονται μεταξύ πολλών διαφορετικών υπολογιστών οι οποίοι βρίσκονται σε διαφορετικές τοποθεσίες και στα οποία αποκτούν πρόσβαση πολλοί διαφορετικοί χρήστες, αναμφίβολα θεωρείται ένα πολύ δύσκολο εγχείρημα.

- **Πτητικά δεδομένα** (Volatile data): Σε όλα τα μοντέλα υπηρεσίας του υπολογιστικού νέφους, η συγκεκριμένη πρόκληση είναι παρούσα. Για παράδειγμα, στο μοντέλο «Υποδομή ως Υπηρεσία», σε περίπτωση που τερματιστεί η λειτουργία της εικονικής μηχανής (VM) που περιέχει τα χρήσιμα πτητικά δεδομένα, τότε αυτά θα χαθούν χωρίς να υπάρχει η δυνατότητα ανάκτησης τους. Αντίστοιχα προβλήματα εμφανίζονται και στα υπόλοιπα μοντέλα ανάπτυξης. Η τεχνολογία του υπολογιστικού νέφους στηρίζεται σε ένα πολύ δυναμικό περιβάλλον, το οποίο αποσκοπεί μεταξύ άλλων, στην ταχύτητα διάθεσης της υπηρεσίας. Στο δυναμικό αυτό περιβάλλον, τα περισσότερα δεδομένα είναι πτητικά, μιας και η μόνιμη αποθήκευση τους θα μπορούσε να δημιουργήσει καθυστερήσεις.

- **Συσχέτιση δεδομένων** (Data Correlation): Ο ερευνητής ψηφιακής εγκληματολογίας πρέπει να συσχετίσει όλα τα διαφορετικά δεδομένα που έχει στη κα-

τοχή του, προκειμένου να δημιουργήσει το τελικό χρονοδιάγραμμα της διάπραξης του εγκλήματος που εξετάζει. Ο ερευνητής προσπαθεί σε αυτό το στάδιο της εξέτασης αφενός να συγχρονίσει τις χρονοσφραγίδες (timestamps) όλων των δεδομένων που έχει συλλέξει και αφετέρου να τις ερμηνεύσει καταλλήλως. Όμως οι τυχόν διαφορετικές ζώνες ώρας των αρχείων καταγραφής (σε περίπτωση που εμπλέκονται υπολογιστές βρίσκονται σε διαφορετικές τοποθεσίες), η τυχόν ύπαρξη επιπλέον δεδομένων σε τρίτους παρόχους υπηρεσιών νέφους (συνηθισμένη πρακτική των παρόχων υπηρεσιών νέφους είναι να εξάγουν μέρος των δραστηριοτήτων τους σε άλλους αντίστοιχους παρόχους) και γενικά ο αδιαφανής τρόπος λειτουργίας του υπολογιστικού νέφους, αυξάνουν το επίπεδο δυσκολίας του συγκεκριμένου σταδίου μίας δικανικής εξέτασης.

- **Τμηματική συλλογή αποδεικτικών στοιχείων** (Partial evidence): Η συλλογή όλων των διαθέσιμων αποδεικτικών στοιχείων που υπάρχουν στο νέφος (μέσω της δημιουργίας εγκληματολογικών αντιγράφων στα αντίστοιχα εμπλεκόμενα ψηφιακά πειστήρια) είναι εξαιρετικά χρονοβόρα διαδικασία και καθόλου πρακτική. Τα στενά χρονικά όρια που συνοδεύουν συνήθως μία εγκληματολογική εξέταση στο νέφος, απαιτούν την αναζήτηση εναλλακτικών λύσεων. Μολονότι η τμηματική συλλογή αποδεικτικών στοιχείων αποτελεί μία ενδιάμεση λύση, ενέχει το πρόβλημα ότι ο ερευνητής μπορεί να οδηγηθεί σε λάθος συμπεράσματα λόγω απουσίας χρήσιμης αποδεικτικής πληροφορίας. Ο ερευνητής θα πρέπει να θέσει αυστηρά κριτήρια κατά την αναζήτηση των αποδεικτικών στοιχείων που επιθυμεί να συλλέξει για τη δικανική εξέταση.

Στο κεφάλαιο αυτό αναλύθηκαν ορισμένες από τις νομικές και τεχνικές δυσκολίες που καλείται να αντιμετωπίσει ο ερευνητής δικανικής πληροφορικής σε μία εγκληματολογική εξέταση στο νέφος. Σημειώνεται ότι η ανωτέρω λίστα δεν είναι εξαντλητική, αλλά παρουσιάζεται για τη μόρφωση άποψης. Ο ενδιαφερόμενος ερευνητής μπορεί να ανατρέξει στην προαναφερθείσα βιβλιογραφία για την περαιτέρω μελέτη των εν λόγω προκλήσεων. Παρόλα αυτά, με την ολοκλήρωση του κεφαλαίου 4 επιτυγχάνεται ο θεωρητικός στόχος [**Θ.2**]. Στη συνέχεια θα γίνει παρουσίαση των ευρημάτων που ενδέχεται να προκύψουν σε μία δικανική εξέταση στο νέφος.

Κεφάλαιο 5ο: Ευρήματα σε μία δικανική εξέταση στο Νέφος

5.1. Γενικά

Ο σκοπός της εγκληματολογικής εξέτασης ψηφιακών πειστηρίων είναι ο εντοπισμός ευρημάτων, τα οποία είτε επιβεβαιώνουν ή καταρρίπτουν τις υποθέσεις του προσώπου (φυσικού ή νομικού) που την παρήγγειλε. Μία εγκληματολογική εξέταση κατά κύριο λόγο παραγγέλνεται από το δικαστήριο (πολιτικό ή ποινικό) ή την αρμόδια αρχή επιβολής του νόμου. Δεν είναι σπάνιο όμως εγκληματολογική εξέταση να ζητείται και από έναν Οργανισμό, μία εταιρεία ή έναν ιδιώτη.

Ευρήματα δεν αποτελούν απαραίτητα όλα τα δεδομένα που βρίσκονται αποθηκευμένα σε ένα ψηφιακό πειστήριο. Αντίθετα, συνήθως μόνο ένα μέρος των δεδομένων αυτών, έχουν σχέση με την υπό εξέταση υπόθεση και κατά συνέπεια χαρακτηρίζονται ως ευρήματα. Μία διευκρίνιση στο σημείο αυτό είναι απαραίτητη. Όταν γίνεται λόγος για δεδομένα αποθηκευμένα σε ένα ψηφιακό πειστήριο, δεν νοούνται μόνο τα αρχεία εκείνα που αντιλαμβάνεται ένας μέσος χρήστης, όπως είναι τα αρχεία κειμένου, εικόνας ή βίντεο, κ.τ.λ. που είναι αποθηκευμένα σε αυτό. Τα δεδομένα που εντοπίζονται σε ένα ψηφιακό πειστήριο είναι πολλά περισσότερα και πιο χρήσιμα.

Σε ένα ψηφιακό πειστήριο λοιπόν, καταγράφονται πληροφορίες για τις οποίες ο χρήστης δεν γνωρίζει την ύπαρξη τους και οι οποίες μπορούν να αξιοποιηθούν από τον ερευνητή δικανικής πληροφορικής. Ένα απλό παράδειγμα τέτοιας πληροφορίας είναι οι καταγεγραμμένες αναζητήσεις του χρήστη στις διαδικτυακές μηχανές αναζήτησης (Google, κ.ά.), οι οποίες και καταδεικνύουν μεταξύ άλλων, τις προθέσεις και τις σκέψεις του χρήστη, ή μιλώντας με νομική ορολογία, τον δόλο που μπορεί να έχει ως προς την άδικη πράξη που εξετάζεται. Άλλα παραδείγματα χρήσιμων πληροφοριών που καταγράφονται σε ένα ψηφιακό πειστήριο είναι, το πότε διαγράφηκε ένα συγκεκριμένο αρχείο, το πότε «κατέβηκε» (download) ένα αρχείο από το Διαδίκτυο, πότε συνδέθηκε ένα συγκεκριμένο USB στον υπολογιστή, που βρισκόταν το συγκεκριμένο κινητό τηλέφωνο τη χρονική στιγμή τάδε, κ.τ.λ.. Όπως γίνεται κατανοητό, υπάρχει τεράστιος όγκος πληροφορίας σε ένα σύγχρονο ψηφιακό μέσο, μέρος της οποίας μπορεί να χρησιμοποιηθεί στην ψηφιακή εγκληματολογία.

Εκτός όμως από τα ευρήματα που μπορούν να προκύψουν εξετάζοντας τα ψηφιακά πειστήρια που βρέθηκαν στην κατοχή του κατηγορούμενου ατόμου (client-side artifacts), υπάρχουν και εκείνα που μπορούν να προκύψουν εξετάζοντας τους διακομιστές των διάφορων διαδικτυακών υπηρεσιών νέφους (π.χ. Google Drive) που έκανε χρήση το κατηγορούμενο άτομο (server-side ή cloud-side artifacts). Αναμφί-

βολα, η εγκληματολογική εξέταση των διακομιστών των υπηρεσιών νέφους που έ-κανε χρήση ένα κατηγορούμενο άτομο, είναι μία πρακτική που ακόμα και σήμερα α-ποφεύγεται, καθώς απαιτεί την επίλυση πολλών χρονοβόρων νομικών και τεχνικών ζητημάτων, όπως εκείνων που προαναφέρθηκαν.

Παρόλα αυτά, αν και η εγκληματολογική εξέταση των εξυπηρετητών κρίνεται εξαιρετικά δύσκολο να επιτευχθεί, ο ερευνητής έχει τη δυνατότητα σε ορισμένες περι-πτώσεις, να αποκτήσει πρόσβαση σε δεδομένα που υπάρχουν αποθηκευμένα στους διακομιστές μίας υπηρεσίας νέφους (χωρίς καν να απαιτείται η παρουσία του στη φυσική τοποθεσία των διακομιστών). Παραδείγματος χάρη, ένας ερευνητής χρησιμο-ποιώντας ειδικό εγκληματολογικό λογισμικό και τα στοιχεία εισόδου του επίμαχου λογαριασμού (credentials), έχει τη δυνατότητα να δημιουργήσει ένα εγκληματολο-γικό αντίγραφο του νέφους του ύποπτου χρήστη. Το εν λόγω εγκληματολογικό αντί-γραφο, αποτελεί στην ουσία ένα στιγμιότυπο των δεδομένων που έφερε αποθηκευ-μένα στο νέφος του ο χρήστης. Αυτή η ενδιάμεση λύση (δημιουργία εγκληματολογι-κού αντιγράφου του νέφους έναντι εγκληματολογικής εξέτασης των εξυπηρετητών), θα μπορούσε να θεωρηθεί ως χρυσή τομή για μία εγκληματολογική εξέταση στο νέ-φος (κυρίως στο SaaS μοντέλο υπηρεσίας), καθώς αυξάνει κατά πολύ τα δεδομένα που έχει στη διάθεση του για ανάλυση ο ερευνητής, ενώ παράλληλα παρακάμπτει ση-μαντικά νομικά κωλύματα. Με αυτήν τη λύση, ο ερευνητής βρίσκεται σε θέση να εξά-γει ασφαλέστερα συμπεράσματα για την υπόθεση που εξετάζει. Ωστόσο υπογραμμί-ζεται ότι, αφενός μέχρι σήμερα δεν υπάρχει εγκληματολογικό λογισμικό που να υπο-στηρίζει τη δημιουργία εγκληματολογικού αντιγράφου του νέφους ενός χρήστη, για όλες τις διαδικτυακές υπηρεσίες νέφους που υπάρχουν στην αγορά και αφετέρου πριν προβεί σε μία τέτοια ενέργεια ένας ερευνητής, θα πρέπει να έχει επαληθεύσει ότι συντρέχουν όλες οι απαραίτητες νομικές προϋποθέσεις (π.χ. ειδική διάταξη περί άρ-σης απορρήτου των επικοινωνιών), για την εξασφάλιση της νομιμότητας της εν λόγω διαδικασίας.

Τέλος, ευρήματα που σχετίζονται με τη χρήση υπηρεσιών νέφους, μπορούν να εντοπιστούν σε αρχεία καταγραφής της διαδικτυακής δραστηριότητας ενός δικτύου, όπου είναι συνδεδεμένος και ο ύποπτος χρήστης. Ένα τέτοιο παράδειγμα αποτελεί ένα σύγχρονο εταιρικό περιβάλλον, όπου ο υπεύθυνος ασφαλείας της εταιρείας, κα-ταγράφει τη διαδικτυακή κίνηση των συσκευών που είναι συνδεδεμένες στο εταιρικό δίκτυο (ενδεχομένως σε αρχεία διαμόρφωσης .pcap), για λόγους ασφαλείας της εται-ρείας.

Επομένως, τα ευρήματα που σχετίζονται με τη χρήση υπηρεσιών νέφους, μπο-ρούν να εντοπιστούν κατά κύριο λόγο στα ψηφιακά πειστήρια που βρέθηκαν στην κατοχή του υπόπτου, στο εγκληματολογικό αντίγραφο του νέφους ενός χρήστη και

σε τυχόν αρχεία καταγραφής της διαδικτυακής δραστηριότητας, στην περίπτωση που εξετάζεται εταιρικό περιβάλλον.

Κατά την ανάλυση δεδομένων και πληροφοριών που εντοπίζονται σε υπολογιστές, κινητά τηλέφωνα ή και σε άλλα εν δυνάμει ψηφιακά πειστήρια που βρίσκονται στην κατοχή ενός δράστη, τα ευρήματα μπορούν να αντληθούν από δύο κύριες πηγές δεδομένων. Οι δύο πιο συνηθισμένες πηγές δεδομένων είναι η πτητική μνήμη και η μη πτητική μνήμη. Η ειδοποιός διαφορά τους είναι ότι τα δεδομένα που βρίσκονται στην πτητική μνήμη ή αλλιώς πτητικά δεδομένα, αποθηκεύονται προσωρινά στη μνήμη και χάνονται αμέσως μετά την διακοπή παροχής ρεύματος στη συσκευή ή πολλές φορές ακόμα και όταν απλώς παύουν να χρησιμοποιούνται από τη συσκευή. Αντίθετα, τα δεδομένα που βρίσκονται στη μη πτητική μνήμη ή αλλιώς μη πτητικά δεδομένα, αποθηκεύονται «μόνιμα» στη συσκευή και διατηρούνται σε αυτή ακόμα και μετά τον τερματισμό της λειτουργίας της (CapitalNetworkSolutions n.d.). Παράδειγμα πτητικών δεδομένων είναι αυτά που βρίσκονται αποθηκευμένα στη μνήμη RAM, ενώ παράδειγμα μη πτητικών δεδομένων είναι τα αρχεία που βρίσκονται αποθηκευμένα σε ένα σκληρό δίσκο.

Κατά την ανάλυση των δεδομένων που έχει αποθηκεύσει στο νέφος του ένας χρήστης, τα ευρήματα που ενδέχεται να προκύψουν εξαρτώνται από δύο παράγοντες. Πρώτον, από το τι είδους δεδομένα καταχωρεί η εκάστοτε υπηρεσία νέφους για ένα χρήστη (π.χ. δραστηριότητα όπως οι προσπελάσεις/τροποποιήσεις αρχείων, διαμοιρασμός αρχείων, κ.ά.). Δεύτερον, από τις ρυθμίσεις που έχει επιλέξει ο χρήστης για τη συγκεκριμένη υπηρεσία νέφους (δηλ. από την εξατομίκευση χρήσης της υπηρεσίας). Για παράδειγμα, στη διαδικτυακή υπηρεσία νέφους της εταιρείας Google, ένας χρήστης μπορεί να έχει επιλέξει να μην αποθηκεύονται όλες οι φωτογραφίες που τραβάει με το κινητό του αυτόματα στο νέφος του, αλλά να γίνεται μόνο για συγκεκριμένα αρχεία και κατόπιν επιλογής του. Η διαφορά στα ευρήματα που θα προκύψουν από τα δεδομένα του εν λόγω χρήστη και ενός χρήστη που χρησιμοποιεί τις προεπιλεγμένες ρυθμίσεις της ανωτέρω υπηρεσίας νέφους, είναι προφανής.

Τέλος, κατά την ανάλυση αρχείων καταγραφής της διαδικτυακής δραστηριότητας σε ένα εταιρικό περιβάλλον, τα ευρήματα εξαρτώνται από το είδος των αρχείων καταγραφής (π.χ. τι πληροφορίες καταχωρούνται σε αυτά) και από τις περαιτέρω ρυθμίσεις του υπευθύνου ασφαλείας ως προς την καταγραφή τους (περιοδικότητα, χρονικό διάστημα αποθήκευσης τους, κ.ά.).

Κάτωθι, αναφέρονται συνοπτικά μερικά από τα ευρήματα που αναμένεται να προκύψουν κατά την εγκληματολογική εξέταση των ψηφιακών πειστηρίων που βρέθηκαν στην κατοχή ενός υπόπτου (σε πτητικά και μη πτητικά δεδομένα), όσον αφορά

τις υπηρεσίες νέφους. Επίσης, αναφέρονται συνοπτικά μερικά από τα ευρήματα που αναμένεται να προκύψουν κατά την εγκληματολογική εξέταση των δεδομένων του νέφους ενός χρήστη. Κλείνοντας, γίνεται μνεία για τα ευρήματα που μπορούν να προκύψουν από την ανάλυση των αρχείων καταγραφής της διαδικτυακής δραστηριότητας μίας εταιρείας, όσον αφορά τις υπηρεσίες νέφους. Ο σκοπός της παρουσίασης τους είναι η εξοικείωση του ερευνητή με αυτά και η ευαισθητοποίηση του ως προς τα δεδομένα που μπορεί να εντοπίσει σε μία δικανική εξέταση στο νέφος, ανάλογα με τις περιστάσεις αυτής.

5.2. Κατά την εξέταση των ψηφιακών πειστηρίων

5.2.1. Ευρήματα σε πτητικά δεδομένα

Αρχικά θα παρουσιαστούν συνοπτικά ορισμένα από τα ευρήματα που μπορούν να προκύψουν από την εξέταση της πτητικής μνήμης μίας σύγχρονης ψηφιακής συσκευής (π.χ. μνήμης RAM) και των δεδομένων που αυτή περιέχει, όσον αφορά την παρουσία και χρήση υπηρεσιών νέφους. Μερικά από αυτά τα ευρήματα, τα οποία μπορεί να αξιοποιήσει ένας ερευνητής δικανικής πληροφορικής, παρατίθενται κάτωθι (Chung et al. 2012, Dave et al. 2014, Gubanov 2013, Kaur and Singh 2016, Malik et al. 2015):

- **Πληροφορίες σχετικές με του χρήστες**: Πληροφορίες όπως ηλεκτρονικές διευθύνσεις (emails) των χρηστών καθώς και τους αντίστοιχους κωδικούς πρόσβασης, που χρησιμοποιούνται σε ένα φυλλομετρητή Ιστού (και οι οποίες μπορούν να χρησιμοποιηθούν για την εξαγωγή του εγκληματολογικού αντιγράφου του νέφους του). Επιπρόσθετα, πληροφορίες για τους συνδεδεμένους χρήστες του συστήματος,
- **Πληροφορίες σχετικές με τα αρχεία**: Λίστες αρχείων και πληροφορίες σχετικά με τα αρχεία, όπως για παράδειγμα ποια αρχεία έχουν προσπελαστεί πρόσφατα, ή ποια είναι ακόμη ανοιχτά και την παρούσα χρονική στιγμή,
- **Πληροφορίες για τις διεργασίες και εφαρμογές που εκτελούνται**: Ποιες εφαρμογές νέφους τρέχουν την παρούσα χρονική στιγμή στη μνήμη, τι πόρους καταναλώνουν, κ.τ.λ.,
- **Πληροφορίες σχετικές με τις συνδέσεις δικτύου**: Σε ποια δίκτυα είναι συνδεδεμένη η συσκευή, ποιες από αυτές τις συνδέσεις είναι ακόμη ενεργές και ποιες όχι, καθώς και ποιες από αυτές σχετίζονται με υπηρεσίες νέφους,
- **Πληροφορίες σχετικές με το μητρώο καταγραφής (registry-Σε περιβάλλον Windows)**: Δραστηριότητα που σχετίζεται με το μητρώο καταγραφής και

τις εγγραφές του, με έμφαση στις εγγραφές που σχετίζονται με υπηρεσίες νέφους,

- **Πληροφορίες σχετικά με δραστηριότητα στον Παγκόσμιο Ιστό:** Μπορούν να εντοπιστούν διαδικτυακές επισκέψεις που έχει κάνει ο χρήστης μέσω εφαρμογών φυλλομετρητή Ιστού και ενδεχομένως σχετίζονται με υπηρεσίες νέφους.

Η ανωτέρω λίστα με τα πιθανά ευρήματα που μπορούν να εξαχθούν από την πτητική μνήμη μίας συσκευής δεν είναι εξαντλητική (π.χ. κλειδιά κρυπτογραφημένων αρχείων, ύπαρξη malware, κ.ά.), αλλά είναι αρκετά περιεκτική όσον αφορά τα ευρήματα που σχετίζονται με υπηρεσίες νέφους. Επισημαίνεται ότι, η συλλογή της πτητικής μνήμης μία συσκευής, αφήνει ίχνη στην ψηφιακή συσκευή, για αυτό και χρειάζεται ιδιαίτερη προσοχή από τον ερευνητή στις ενέργειες που προβαίνει, προκειμένου να μην διακυβεύεται η αξιοπιστία του πειστηρίου. Κάτωθι, θα παρουσιαστούν μερικά από τα ευρήματα που σχετίζονται με μη πτητικά δεδομένα και μπορούν να αξιοποιηθούν σε μία εγκληματολογική εξέταση στο νέφος.

5.2.2. Ευρήματα σε μη πτητικά δεδομένα

Τα ευρήματα που μπορούν να εξαχθούν από τα μη πτητικά δεδομένα ενός ψηφιακού μέσου, είναι πολλά και ποικίλα. Ενδεικτικά, θα παρουσιαστούν ορισμένα από τα ευρήματα που μπορούν να προκύψουν και τα οποία μπορούν να αξιοποιηθούν σε μία εγκληματολογική εξέταση στο νέφος:

- **Αρχεία καταγραφής εφαρμογών νέφους**: Σε περιπτώσεις που υπάρχει εγκατεστημένη εφαρμογή υπηρεσιών νέφους, τα αρχεία καταγραφής της μπορούν να περιέχουν πολύτιμες πληροφορίες σχετικά με τη χρήση της εφαρμογής, ή ακόμα καλύτερα σχετικά με τη δραστηριότητα του χρήστη μέσω αυτής (π.χ. μεταφόρτωση αρχείων, προσπέλαση αρχείων, αναγνωριστικά χρηστών, μεγέθη των αρχείων, κ.ά.). Παρόμοια ευρήματα μπορούν να προκύψουν και από την ανάλυση των αρχείων βάσεων δεδομένων των εφαρμογών νέφους, τα οποία φέρουν αποθηκευμένα τα δεδομένα του χρήστη,
- **Πληροφορίες σχετικές με τα αρχεία ή αποθηκευμένες σε αυτά**: Πληροφορίες που σχετίζονται με τα αρχεία του χρήστη, όπως για παράδειγμα ποια αρχεία έχουν δημιουργηθεί ή προσπελασθεί πρόσφατα. Επίσης, σε αυτά μπορούν να εντοπιστούν πολύτιμες πληροφορίες, όπως τα στοιχεία εισόδου του χρήστη για κάποια διαδικτυακή υπηρεσία. Αυτού του είδους η πληροφορία, μπορεί ενδεχομένως να χρησιμοποιηθεί για τη δημιουργία του εγκληματολογικού αντιγράφου του νέφους του χρήστη,

- **Πληροφορίες σχετικές με το μητρώο καταγραφής (registry-Σε περιβάλλον Windows)**: Δραστηριότητα που σχετίζεται με το μητρώο καταγραφής και τις εγγραφές του, όπως για παράδειγμα πόσες φορές χρησιμοποιήθηκε μία εφαρμογή νέφους, ή πότε ήταν η τελευταία χρήση της. Επιπρόσθετα, οι ρυθμίσεις του χρήστη σχετικά με την εφαρμογή αυτή (π.χ. να ξεκινάει αυτόματα μετά την εκκίνηση του συστήματος, κ.ά.),
- **Πληροφορίες σχετικά με δραστηριότητα στον Παγκόσμιο Ιστό:** Μπορούν να εντοπιστούν διαδικτυακές επισκέψεις που έχει κάνει ο χρήστης μέσω εφαρμογών φυλλομετρητή Ιστού και ενδεχομένως σχετίζονται με υπηρεσίες νέφους. Ειδικότερα, μπορούν πολλές φορές να εξαχθούν περισσότερες πληροφορίες σχετικά με τις εν λόγω διαδικτυακές επισκέψεις του χρήστη, όπως για παράδειγμα εάν αυτές αφορούν την προβολή ενός αρχείου αποθηκευμένου στο νέφος του χρήστη, ή στην μεταφόρτωση (upload) του αρχείου στο νέφος. Ακόμη, υπάρχει η δυνατότητα εξαγωγής των στοιχείων εισόδου που χρησιμοποίησε ο χρήστης για να αποκτήσει πρόσβαση σε μία διαδικτυακή υπηρεσία νέφους (ή άλλου είδους υπηρεσία) και τα οποία έχει αποθηκεύσει σε κάποιο φυλλομετρητή Ιστού.

Η ανωτέρω λίστα με τα ευρήματα που μπορούν να εξαχθούν από τη μη πτητική μνήμη μίας συσκευής, αν και είναι συνοπτική, περιλαμβάνει ωστόσο τα περισσότερα ευρήματα που σχετίζονται με υπηρεσίες νέφους. Κάτωθι, παρατίθενται μερικά από τα ευρήματα που μπορούν να προκύψουν κατά την εξέταση ενός εγκληματολογικού αντιγράφου του νέφους ενός χρήστη.

5.3. Κατά την εξέταση εγκληματολογικού αντιγράφου του νέφους ενός χρήστη

Τα ευρήματα που μπορούν να εξαχθούν από το αντίγραφο του νέφους ενός χρήστη, είναι πάρα πολύ σημαντικά για μία ολοκληρωμένη δικανική εξέταση. Ο βασικότερος λόγος που τα δεδομένα αυτά θεωρούνται τόσο σημαντικά, είναι γιατί ενδέχεται να είναι και τα μόνα που έχουν απομείνει. Καθώς, είναι αρκετά πιθανό για ένα ύποπτο χρήστη να έχει προχωρήσει είτε στην ολοκληρωτική διαγραφή των επίμαχων αρχείων από τις συσκευές του, ή ακόμη χειρότερα, στην καταστροφή των συσκευών αυτών. Ενδεικτικά, θα παρουσιαστούν ορισμένα από τα ευρήματα που μπορούν να προκύψουν από ένα εγκληματολογικό αντίγραφο του νέφους ενός χρήστη:

- **Αρχεία αποθηκευμένα στο νέφος**: Μπορούν να αντληθούν τόσο τα αρχεία που έχουν αποθηκευτεί στο νέφος του χρήστη, όσο και λεπτομέρειες σχετικά

με ημερομηνίες μεταφόρτωσης (download/upload) ή τροποποίησης τους. Επίσης, μπορούν να αντληθούν οι αλφαριθμητικές ταυτότητες μοναδικότητας των αρχείων (MD5), καθώς και τα αναγνωριστικά που τους έχει καταχωρήσει η εφαρμογή. Με αυτό τον τρόπο μπορούν να συσχετισθούν αρχεία από διαφορετικές πηγές δεδομένων,

- **Διαμοιρασμός αρχείων μέσω της υπηρεσίας νέφους:** Σε περίπτωση που ένα αρχείο έχει διαμοιραστεί σε έτερους χρήστες μέσω της συγκεκριμένης υπηρεσίας νέφους, η πληροφορία αυτή μπορεί να εξαχθεί από το εγκληματολογικό αντίγραφο του νέφους,
- **Ημερομηνία και ώρα τελευταίας σύνδεσης στην υπηρεσία:** Αυτή η πληροφορία δεν καταχωρείται πάντα και εξαρτάται από την εκάστοτε υπηρεσία,
- **Τοποθεσία αρχείων εικόνας ή βίντεο:** Κάθε αρχείο εικόνας ή βίντεο που είναι αποθηκευμένο στο νέφος ενός χρήστη (ή και τοπικά στις συσκευές), μπορεί να φέρει ως πρόσθετη πληροφορία τις γεωγραφικές συντεταγμένες όπου και δημιουργήθηκε αρχικά,
- **Δραστηριότητα του χρήστη κατά τη χρήση της υπηρεσίας:** Ανάλογα με την εκάστοτε υπηρεσία νέφους, υπάρχει η δυνατότητα καταγραφής των ενεργειών στις οποίες προβαίνει ο χρήστης όταν χρησιμοποιεί τη συγκεκριμένη υπηρεσία νέφους (δημιουργία, διαγραφή, μεταφόρτωση, κ.ά.),

Στην ανωτέρω λίστα αναφέρονται τα βασικά ευρήματα που μπορούν να εξαχθούν από ένα αντίγραφο των δεδομένων μίας διαδικτυακής υπηρεσίας νέφους, για ένα συγκεκριμένο χρήστη. Κλείνοντας θα αναφερθούν τα αποτελέσματα που μπορεί να προκύψουν κατά την εξέταση των αρχείων καταγραφής ενός δικτύου, κατά την εγκληματολογική εξέταση σε ένα εταιρικό περιβάλλον, όσον αφορά τη χρήση υπηρεσιών νέφους.

5.4. Κατά την εξέταση αρχείων καταγραφής σε εταιρικό περιβάλλον

Τέλος παρατίθενται κάτωθι τα αποδεικτικά στοιχεία που μπορούν να προκύψουν κατά την εξέταση αρχείων καταγραφής σε εταιρικό ή άλλο περιβάλλον, σχετικά με δραστηριότητα στο νέφος. Επισημαίνεται ότι τα ευρήματα που ενδέχεται να προκύψουν από τα αρχεία καταγραφής, είναι αρκετά δύσκολο να επιβεβαιώσουν ή να καταρρίψουν από μόνα τους κάποια υπόθεση , αλλά δρουν συμπληρωματικά στα υπόλοιπα δεδομένα που αναμένεται να συλλεχθούν, συντελώντας σε μία πιο ολοκληρωμένη έρευνα (Spiekermann et al. 2015):

- **Διεύθυνση IP του παρόχου της υπηρεσίας**: Η μοναδική διεύθυνση IP του συγκεκριμένου εξυπηρετητή (server) του παρόχου της υπηρεσίας νέφους, στον οποίο συνδέθηκε ο ύποπτος χρήστης, μπορεί να βοηθήσει τον ερευνητή να εντοπίσει τη γεωγραφική τοποθεσία του συγκεκριμένου εξυπηρετητή. Αυτό είναι ιδιαίτερα χρήσιμο σε περιπτώσεις διεθνούς συνεργασίας μεταξύ των Αρχών Επιβολής του Νόμου, καθώς αφού εντοπιστεί ο συγκεκριμένος εξυπηρετητής, θα μπορέσει εν συνέχεια να κατασχεθεί από την αρμόδια Υπηρεσία.
- **Διεύθυνση IP του ύποπτου χρήστη**: Σε ένα εταιρικό περιβάλλον με δεκάδες ή ακόμη και εκατοντάδες συσκευές συνδεδεμένες στο ίδιο δίκτυο, ο εντοπισμός μίας συγκεκριμένης συσκευής ενός ύποπτου χρήστη, καθίσταται ιδιαίτερα δύσκολη υπόθεση. Συνδυάζοντας όμως τα δεδομένα που καταδεικνύουν τη χρήση υπηρεσιών νέφους και τη μοναδική διεύθυνση IP που χρησιμοποιεί μία συσκευή σε ένα εσωτερικό δίκτυο, ο εντοπισμός του ύποπτου χρήστη μπορεί να γίνει πιο εύκολα.
- **Πληροφορίες σχετικές με μεταφόρτωση (download/upload) αρχείων**: Αναλύοντας τα αρχεία καταγραφής, μπορούν να εντοπιστούν δεδομένα που να σχετίζονται με τη μεταφόρτωση αρχείων από το Διαδίκτυο ή σε αυτό.
- **Πληροφορίες σχετικές με χρήση εφαρμογών**: Πληροφορίες για τις εφαρμογές μέσω των οποίων αποκτάται πρόσβαση στις υπηρεσίες νέφους, αποθηκεύονται στα αρχεία καταγραφής. Για παράδειγμα, η εφαρμογή φυλλομετρητή (Web Browser->User-Agent) που χρησιμοποιεί η ύποπτη συσκευή, μπορεί να βοηθήσει τον ερευνητή να προσδιορίσει το είδος της συσκευής (Apple Safari, κ.ά.) και κατ' επέκταση τον ύποπτο χρήστη.
- **Πληροφορίες σχετικές με το πρωτόκολλο επικοινωνίας**: Οι πληροφορίες αυτές (π.χ. HTTP, TCP/IP, κ.ά.) ανήκουν στα εξωτερικά στοιχεία επικοινωνίας μεταξύ της συσκευής και της διαδικτυακής υπηρεσίας νέφους και μπορούν να χρησιμοποιηθούν συμπληρωματικά στα ανωτέρω, για την ανάλυση της μεταξύ τους επικοινωνίας.

Όπως γίνεται κατανοητό, τα αρχεία καταγραφής περιέχουν σημαντικές πληροφορίες που μπορούν να αξιοποιηθούν σε μία δικανική έρευνα. Σε αυτό το κεφάλαιο, παρουσιάστηκαν τα περισσότερα ευρήματα που μπορούν να προκύψουν σε μία εγκληματολογική εξέταση με έμφαση στις διαδικτυακές υπηρεσίες νέφους. Ειδικότερα, εξετάστηκαν οι διαφορετικές πηγές αποδεικτικών στοιχείων, τις οποίες μπορεί να αξιοποιήσει ο ερευνητής, προκειμένου να καταλήξει σε μία ασφαλή τοποθέτηση κατά την παρουσίαση των ευρημάτων της έρευνας του.

Κλείνοντας το κεφάλαιο αυτό αναφέρεται ότι, έπειτα από τη συνοπτική αλλά παράλληλα πλήρη επισκόπηση των πιθανών ευρημάτων μίας εγκληματολογικής εξέτασης στο νέφος, ο τελευταίος θεωρητικός στόχος [**Θ.3.**] της διπλωματικής εργασίας, κρίνεται επιτυχημένος. Κατόπιν των ανωτέρω, ολοκληρώνεται το θεωρητικό μέρος της εργασίας και ακολουθεί το ερευνητικό μέρος αυτής. Στο επόμενο κεφάλαιο, θα παρουσιαστεί η μεθοδολογία της έρευνας που χρησιμοποιήθηκε στην εργασία.

Κεφάλαιο 6ο: Μεθοδολογία

6.1. Γενικά

Στα προηγούμενα κεφάλαια έγινε θεωρητική προσέγγιση τόσο σε βασικές έννοιες της ψηφιακής εγκληματολογίας και της τεχνολογίας του νέφους, όσο και σε σημαντικά ζητήματα και πληροφορίες που άπτονται μίας δικανικής εξέτασης στο νέφος. Χρησιμοποιώντας το θεωρητικό υπόβαθρο των προηγούμενων κεφαλαίων, η μετάβαση στην έρευνα γίνεται με τρόπο αρμονικό για τον αναγνώστη.

Στο παρόν κεφάλαιο, θα επεξηγηθούν τα κομμάτια που συνθέτουν το πρακτικό μέρος της εργασίας. Αρχικά, θα καθοριστεί τόσο το ερευνητικό πρόβλημα που πραγματεύεται η παρούσα διπλωματική, όσο και ο ερευνητικός της στόχος. Στη συνέχεια θα αναφερθούν οι ερευνητικές ερωτήσεις της εργασίας. Δίνοντας απαντήσεις στις εν λόγω ερευνητικές ερωτήσεις, επιχειρείται η επίτευξη του ερευνητικού σκοπού της διπλωματικής.

Οι ανωτέρω απαντήσεις δεν δίνονται τυχαία, αλλά προκύπτουν έπειτα από την αξιολόγηση και ερμηνεία των ευρημάτων της πειραματικής διαδικασίας που πραγματοποιείται. Οι συνθήκες διεξαγωγής της έρευνας καθώς και οι περιορισμοί της, επεξηγούνται ομοίως σε αυτό το κεφάλαιο.

6.2. Ερευνητικό πρόβλημα

Όπως αναλύθηκε και προηγουμένως, οι υπηρεσίες νέφους χρησιμοποιούνται πολλές φορές στη διάπραξη εγκλημάτων. Η χρήση των υπηρεσιών νέφους σε παράνομες ενέργειες, ενδέχεται να αφήνει πίσω της αποδεικτικά στοιχεία, τα οποία είναι υψίστης σημασίας για έναν ερευνητή ψηφιακής εγκληματολογίας.

Αν ανατρέξει κάποιος στη βιβλιογραφία, θα παρατηρήσει ότι η εγκληματολογική εξέταση στο νέφος δεν έχει μελετηθεί ικανοποιητικά. Πιο συγκεκριμένα, υπάρχει έλλειψη πληροφόρησης σχετικά με την εγκληματολογική ανάλυση των υπηρεσιών νέφους (στο μοντέλο υπηρεσίας «Λογισμικό ως Υπηρεσία») και στα ίχνη δεδομένων που δημιουργούνται από τη χρήση του, ειδικά σε υπολογιστές που είναι εφοδιασμένοι με λειτουργικό σύστημα Windows 10 . Επιπρόσθετα, δεν έχουν μελετηθεί επαρκώς, οι τυχόν αλλαγές που επιφέρει στα αρχεία του χρήστη, η χρήση των υπηρεσιών νέφους του μοντέλου αυτού.

6.3. Ερευνητικός Σκοπός

Ο ερευνητικός σκοπός της παρούσας διπλωματικής εργασίας, είναι να συνδράμει στην αντιμετώπιση του ερευνητικού προβλήματος που περιεγράφηκε στο προηγούμενο υποκεφάλαιο. Η ικανοποίηση των ερευνητικών στόχων [**E.1**] και [**E.2**] που τέθηκαν στο κεφάλαιο 1, αποτελεί τον τρόπο με τον οποίο επιχειρείται η επίτευξη του ερευνητικού σκοπού της. Άρα το αρχικό ζητούμενο εδώ, είναι ο προσδιορισμός τυχόν δεδομένων που να αποδεικνύουν τόσο την πρόσβαση, όσο και τη χρήση υπηρεσιών νέφους σε αυτό το μοντέλο υπηρεσίας (SaaS).

Τα ευρήματα της έρευνας αυτής, μπορούν να αξιοποιηθούν από τους ερευνητές ψηφιακής εγκληματολογίας, προκείμενου να εμπλουτίσουν τις γνώσεις τους όσον αφορά την αναγνώριση και τον εντοπισμό αποδεικτικών στοιχείων που σχετίζονται με τη χρήση δημοφιλών υπηρεσιών νέφους, σε περιβάλλον Windows 10.

6.4. Ερευνητικές ερωτήσεις

Η ικανοποίηση των ερευνητικών στόχων [**E.1**] και [**E.2**] της διπλωματικής εργασίας, θα γίνει μέσω της απάντησης των κάτωθι ερευνητικών ερωτήσεων 1 και 2 αντίστοιχα.

6.4.1. Ερευνητική Ερώτηση 1

Υπάρχουν δεδομένα που να προκύπτουν από τη χρήση υπηρεσιών νέφους σε υπολογιστές που έχουν λειτουργικό σύστημα Windows 10 και τα οποία μπορούν να αποδείξουν τη χρήση των υπηρεσιών αυτών;

Η ανωτέρω ερώτηση οδηγεί σε δύο υποθέσεις:

- **Υπόθεση 1**: Δεν υπάρχουν εναπομείναντα ίχνη δεδομένων που να αποδεικνύουν τη χρήση υπηρεσιών νέφους και κατ' επέκταση να επιτρέπουν τον εντοπισμό περαιτέρω ευρημάτων σχετικών με αυτές (π.χ. εντοπισμός του παρόχου της υπηρεσίας νέφους, όνομα χρήστη, κ.τ.λ.).
- **Υπόθεση 2**: Υπάρχουν εναπομείναντα ίχνη δεδομένων που να αποδεικνύουν τη χρήση υπηρεσιών νέφους και τα οποία επιτρέπουν κατ' επέκταση τον εντοπισμό περαιτέρω ευρημάτων σχετικών με αυτές (π.χ. εντοπισμός του παρόχου της υπηρεσίας νέφους, όνομα χρήστη, κ.τ.λ.).

Από την υπόθεση 2 προκύπτουν οι κάτωθι υποερωτήσεις:

- Τι δεδομένα παραμένουν στον υπολογιστή του χρήστη μετά την εγκατάσταση του λογισμικού της υπηρεσίας νέφους και έπειτα από τη χρήση του, για μεταφόρτωση (download/upload) αρχείων ή και άλλου είδους δραστηριότητα (προσπέλαση αρχείων, διαγραφή αρχείων, διαμοιρασμός με άλλους χρήστες, κ.τ.λ.); Επίσης, τι δεδομένα παραμένουν στον υπολογιστή του χρήστη μετά την απεγκατάσταση του λογισμικού της υπηρεσίας νέφους;
- Τι δεδομένα παραμένουν στον υπολογιστή του χρήστη μετά τη χρήση υπηρεσιών νέφους μέσω ενός φυλλομετρητή Ιστού, για μεταφόρτωση (download/ upload) αρχείων ή και άλλου είδους δραστηριότητα (προσπέλαση αρχείων, διαγραφή αρχείων, διαμοιρασμός με άλλους χρήστες, κ.τ.λ.);
- Τι δεδομένα παραμένουν στην πτητική μνήμη του υπολογιστή του χρήστη, όταν χρησιμοποιείται το λογισμικό της εφαρμογής και τι δεδομένα όταν χρησιμοποιείται ένας φυλλομετρητή Ιστού;

6.4.2. Ερευνητική Ερώτηση 2

Επηρεάζονται τα τεχνικά χαρακτηριστικά (περιεχόμενο, μεταδεδομένα, hash, κ.τ.λ.) ενός αρχείου κατά τη μεταφόρτωση (download/ upload) του μέσω μίας υπηρεσίας νέφους;

Η ανωτέρω ερώτηση οδηγεί σε δύο υποθέσεις:

- **Υπόθεση 1**: Τα τεχνικά χαρακτηριστικά ενός αρχείου δεν επηρεάζονται κατά τη μεταφόρτωση (download/ upload) του μέσω μίας υπηρεσίας νέφους.
- **Υπόθεση 2**: Τα τεχνικά χαρακτηριστικά ενός αρχείου επηρεάζονται κατά τη μεταφόρτωση (download/ upload) του μέσω μίας υπηρεσίας νέφους.

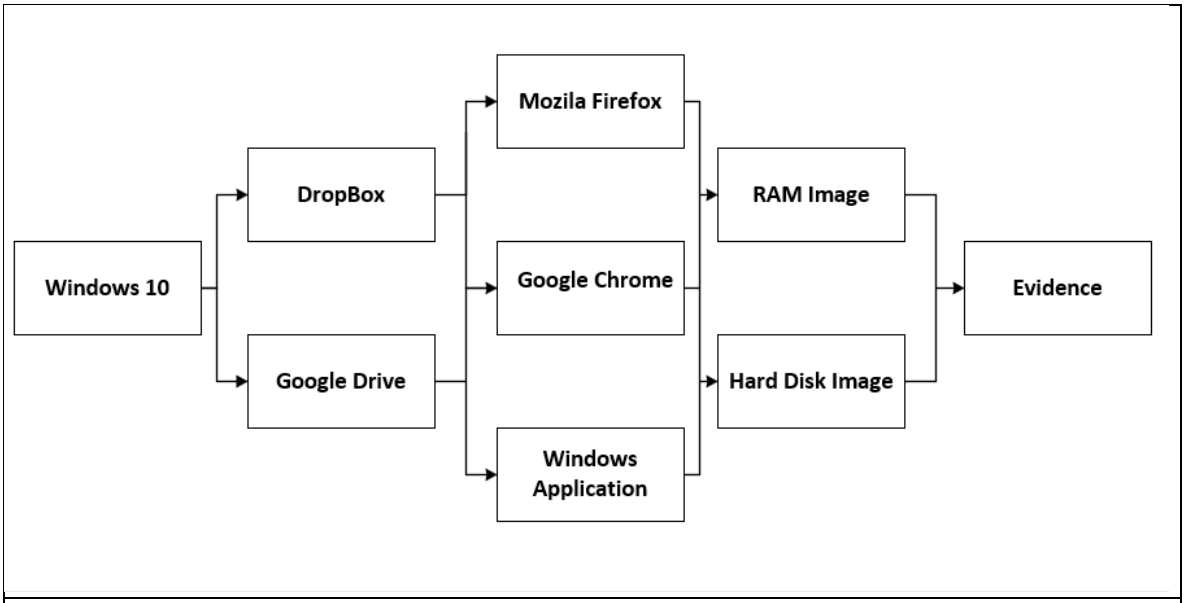
Από την υπόθεση 2 προκύπτει η κάτωθι υποερώτηση:

- Πώς επηρεάζονται οι χρονοσφραγίδες (timestamps) του αρχείου, το περιεχόμενο του και η αλφαριθμητική ταυτότητα μοναδικότητας (MD5) του, κατά τη διακίνηση μέσω μίας υπηρεσίας νέφους;

6.5. Πειραματική Διαδικασία

Η πειραματική διαδικασία είναι η ερευνητική μέθοδος που θα εφαρμοστεί, προκειμένου να απαντηθούν οι ανωτέρω ερωτήσεις. Αναλυτικότερα, θα διεξαχθεί μία σειρά πειραμάτων σε υπολογιστές που έχουν λειτουργικό σύστημα Windows 10 και χρησιμοποιούν ως υπηρεσία νέφους είτε το Dropbox ή το Google Drive.

Στο κάτωθι διάγραμμα (βλ. Εικόνα 2), απεικονίζεται σχηματικά η διαδικασία που ακολουθήθηκε. Αρχικά έγινε εγκατάσταση του λειτουργικού συστήματος Windows 10. Έπειτα, κάθε μία από τις δύο υπηρεσίες νέφους εξετάστηκαν σε πλήθος σεναρίων, άλλοτε με χρήση αποκλειστικά του λογισμικού που παρέχουν στα Windows 10 και άλλοτε με χρήση των φυλλομετρητών Mozilla Firefox και Google Chrome. Ύστερα από τη χρήση των υπηρεσιών νέφους, σε κάθε ένα από τα σενάρια αυτά, δημιουργείται εγκληματολογικό αντίγραφο τόσο της μνήμης RAM όσο και του σκληρού δίσκου του υπολογιστή. Τέλος, τα συλλεχθέντα εγκληματολογικά αντίγραφα εξετάζονται με εγκληματολογικά λογισμικά, προκειμένου να απαντηθούν οι ανωτέρω ερευνητικές ερωτήσεις.



Εικόνα 2
Πειραματική Διαδικασία Έρευνας

Για την εξέταση των προαναφερθέντων σεναρίων, δημιουργήθηκαν 18 εικονικές μηχανές (Virtual Machines) και εξετάστηκαν συνολικά 36 εγκληματολογικά αντίγραφα. Η χρήση των εικονικών μηχανών, παρείχε την απαραίτητη ευελιξία για εις βάθος μελέτη των υπηρεσιών νέφους Dropbox και Google Drive σε περιβάλλον Windows 10, καθόσον επιτρέπουν τη συσχέτιση των διαφορετικών ευρημάτων σε εύλογο χρονικό διάστημα. Αυτό έχει ως αποτέλεσμα την πιο ολοκληρωμένη απάντηση στις ερωτήσεις της έρευνας.

Καθίσταται σαφές ότι, εάν δεν χρησιμοποιούταν η τεχνολογία των εικονικών μηχανών αλλά μόνο το υλισμικό ενός υπολογιστή για την ανωτέρω πειραματική δια-

δικασία, ο χρόνος διεξαγωγής της αντίστοιχης έρευνας (επανεγκατάσταση λειτουργικών συστημάτων, διαγραφές/εγκαταστάσεις λογισμικών, κ.ά.) θα εκτείνονταν πέρα από τα αποδεκτά χρονικά όρια.

6.5.1. Μεθοδολογία απάντησης του πρώτου ερευνητικού ερωτήματος

Κάτωθι αναλύονται τα βήματα που πραγματοποιήθηκαν στην πειραματική διαδικασία και αποσκοπούν στην απάντηση της πρώτης ερευνητικής ερώτησης (βλ. Πίνακα 1), η οποία με τη σειρά της οδηγεί στην ικανοποίηση του ερευνητικού στόχου [**Ε.1**].

Α/Α Βημάτων	**Περιγραφή**
1.	Εγκατάσταση στον υπολογιστή (νοείται μία «καθαρή» εικονική μηχανή) του λογισμικού της υπηρεσίας νέφους.
2.	Μεταφόρτωση (download και upload) αρχείων από τον υπολογιστή στο νέφος μέσω του λογισμικού της υπηρεσίας.
3.	Δημιουργία εγκληματολογικού αντιγράφου της μνήμης RAM και του σκληρού δίσκου του υπολογιστή.
4.	Δικανική εξέταση των εγκληματολογικών αντιγράφων για τον εντοπισμό ευρημάτων και την εξαγωγή συμπερασμάτων.
5.	Επανάληψη της διαδικασίας από το βήμα 1, σε νέο υπολογιστή (νοείται νέα «καθαρή» εικονική μηχανή), με τη διαφορά ότι ενεργείται άλλου είδους δραστηριότητα (προσπέλαση των αρχείων, διαγραφή των αρχείων, διαμοιρασμός αρχείων, κ.ά.).
6.	Χρήση μία εκ των ανωτέρω εικονικών μηχανών και απεγκατάσταση του λογισμικού υπηρεσίας νέφους. Έπειτα εκ νέου εκτέλεση των βημάτων 3 και 4.

Πίνακας 1

Βήματα πειραματικής διαδικασίας κατά τη χρήση του λογισμικού της υπηρεσίας νέφους (Προς απάντηση της 1ης ερευνητικής ερώτησης)

Κατόπιν ολοκλήρωσης των ανωτέρω βημάτων, η διαδικασία επαναλαμβάνεται μετά τη χρήση των υπηρεσιών νέφους μέσω φυλλομετρητή Ιστού. Επομένως, τα αντίστοιχα βήματα παρουσιάζονται κάτωθι (βλ. Πίνακα 2):

Α/Α Βημάτων	**Περιγραφή**

1.	Εγκατάσταση στον υπολογιστή (νοείται μία «καθαρή» εικονική μηχανή) του φυλλομετρητή Ιστού που θα χρησιμοποιηθεί για τη χρήση της υπηρεσίας νέφους.
2.	Μεταφόρτωση (download και upload) αρχείων από τον υπολογιστή στο νέφος μέσω του φυλλομετρητή Ιστού.
3.	Δημιουργία εγκληματολογικού αντιγράφου της μνήμης RAM και του σκληρού δίσκου του υπολογιστή.
4.	Δικανική εξέταση των εγκληματολογικών αντιγράφων για τον εντοπισμό ευρημάτων και την εξαγωγή συμπερασμάτων.
5.	Επανάληψη της διαδικασίας από το βήμα 1, σε νέο υπολογιστή (νοείται νέα «καθαρή» εικονική μηχανή), με τη διαφορά ότι ενεργείται άλλου είδους δραστηριότητα (προσπέλαση των αρχείων, διαγραφή των αρχείων, διαμοιρασμός αρχείων, κ.ά.).
6.	Επανάληψη της διαδικασίας από το βήμα 1, σε νέο υπολογιστή (νοείται νέα «καθαρή» εικονική μηχανή), με τη διαφορά ότι χρησιμοποιείται διαφορετικός φυλλομετρητής Ιστού για την ίδια υπηρεσία νέφους.

Πίνακας 2

Βήματα πειραματικής διαδικασίας κατά τη χρήση της υπηρεσίας νέφους μέσω φυλλομετρητή Ιστού (Προς απάντηση της 1ης ερευνητικής ερώτησης)

6.5.1. Μεθοδολογία απάντησης του δεύτερου ερευνητικού ερωτήματος

Για την απάντηση στο δεύτερο ερευνητικό ερώτημα ακολουθείται παρόμοια μεθοδολογία. Για να απαντηθεί με ασφάλεια η ερευνητική ερώτηση αυτή, θεωρείται δεδομένο ότι το περιεχόμενο των αρχείων όσο αυτά βρίσκονται ή μεταφορτώνονται (download/upload) στο νέφος δεν αλλάζει από τον χρήστη. Εάν αυτή η «παράμετρος» δεν θεωρούνταν δεδομένη, θα ήταν αρκετά πιο δύσκολο να εξακριβωθούν οι αλλαγές που επιφέρει αποκλειστικά η χρήση των υπηρεσιών νέφους στα τεχνικά χαρακτηριστικά των αρχείων.

Επομένως, επιλέγονται συγκεκριμένα αρχεία (των οποίων τα τεχνικά χαρακτηριστικά έχουν ήδη καταγραφεί), τα οποία και «ανεβαίνουν» στο νέφος (μέσω φυλλομετρητή Ιστού). Στη συνέχεια, τα εν λόγω αρχεία «κατεβαίνουν» σε μία καθαρή εικονική μηχανή. Επιπρόσθετα, σε μία άλλη καθαρή εικονική μηχανή γίνεται εγκατάσταση του λογισμικού της υπηρεσίας νέφους και γίνεται συγχρονισμός με τα αρχεία που βρίσκονται ήδη αποθηκευμένα στο νέφος, από το προηγούμενο βήμα. Τέλος, εξετάζονται τα τεχνικά χαρακτηριστικά τόσο των αρχείων που «κατέβηκαν» όσο και αυτών που συγχρονίστηκαν και συγκρίνονται με αυτά που είχαν αρχικά «ανέβει» στο νέφος.

Κάτωθι περιγράφονται τα βήματα της πειραματικής διαδικασίας που εφαρμόστηκε για την απάντηση του δεύτερου ερευνητικού ερωτήματος (βλ. Πίνακες 3 και 4), η οποία με τη σειρά της οδηγεί στην ικανοποίηση του ερευνητικού στόχου [**Ε.2**].:

Α/Α Βημάτων	**Περιγραφή**
1.	Εγκατάσταση στον υπολογιστή (νοείται μία «καθαρή» εικονική μηχανή) του φυλλομετρητή Ιστού που θα χρησιμοποιηθεί για τη χρήση της υπηρεσίας νέφους.
2.	Καταγραφή των τεχνικών χαρακτηριστικών των αρχείων που θα «ανέβουν» στο νέφος.
3.	«Ανέβασμα» αρχείων από τον υπολογιστή στο νέφος μέσω του φυλλομετρητή Ιστού.
4.	Χρήση καθαρής εικονικής μηχανής και «κατέβασμα» των αρχείων στον υπολογιστή μέσω του φυλλομετρητή Ιστού.
5.	Εξέταση των τεχνικών χαρακτηριστικών των αρχείων που «κατέβηκαν» και σύγκριση τους με αυτά των αρχείων που «ανέβηκαν» στο προηγούμενο βήμα.

Πίνακας 3

Βήματα πειραματικής διαδικασίας κατά τη χρήση της υπηρεσίας νέφους μέσω φυλλομετρητή Ιστού (Προς απάντηση της 2ης ερευνητικής ερώτησης)

Α/Α Βημάτων	**Περιγραφή**
1.	Εγκατάσταση στον υπολογιστή (νοείται μία «καθαρή» εικονική μηχανή) του λογισμικού της υπηρεσίας νέφους.
2.	Συγχρονισμός των αρχείων που έχουν «ανέβει» στα προηγούμενα βήματα (βλ. Πίνακας 3) με το λογισμικό της υπηρεσίας νέφους.
3.	Εξέταση των τεχνικών χαρακτηριστικών των αρχείων που «συγχρονίστηκαν» και σύγκριση τους με αυτά των αρχείων που «ανέβηκαν» στα προηγούμενα βήματα (βλ. Πίνακας 3).

Πίνακας 4

Βήματα πειραματικής διαδικασίας κατά τη χρήση του λογισμικού της υπηρεσίας νέφους (Προς απάντηση της 2ης ερευνητικής ερώτησης)

6.6. Υλισμικό

Για την εξέταση των εγκληματολογικών αντιγράφων, καθώς και για τη διαχείριση των εικονικών μηχανών της διπλωματικής εργασίας, χρησιμοποιήθηκε ηλεκτρονικός υπολογιστής με τα κάτωθι χαρακτηριστικά (βλ. Πίνακα 5):

Τεχνικά Χαρακτηριστικά Υπολογιστή Έρευνας	Περιγραφή
Λειτουργικό Σύστημα	Windows 10 Pro 64-bit 10.0.17134 N/A Build 17134 Microsoft Corporation
Επεξεργαστής	AMD Ryzen 7 1700 Eight-Core Processor
Κάρτα Γραφικών	NVIDIA GeForce GTX 1050 Ti
Μητρική Κάρτα	ASUSTeK PRIME X370-PRO (AM4)
Μνήμη RAM	Corsair 32 GB DDR4-2132 (1066 MHz)
Αποθηκευτικός χώρος	1) Samsung SSD 850 EVO 500GB (SSD)
	2) TOSHIBA 3 TB Hard Drive
Αφαιρούμενα Αποθηκευτικά Μέσα	1) Kingston DTGE9 16GB USB 2.0
	2) Εξωτερικός Σκληρός δίσκος WD My Passport 2TB USB 3.0

Πίνακας 5
Χαρακτηριστικά του υπολογιστή της έρευνας

6.7. Λογισμικό

Στο κεφάλαιο αυτό, θα παρουσιαστούν εν συντομία τα λογισμικά που χρησιμοποιήθηκαν σε όλα τα διαφορετικά στάδια της πειραματικής διαδικασίας. Τα προγράμματα αυτά είναι:

Access Data FTK Imager

Το FTK Imager ένα λογισμικό ψηφιακής εγκληματολογίας που χρησιμοποιείται τόσο για την προεπισκόπηση και απεικόνιση δεδομένων που βρίσκονται αποθηκευμένα σε κάποιο μέσο είτε για τη δημιουργία εγκληματολογικών αντιγράφων, χωρίς να αλλοιώνονται τα πηγαία δεδομένα του μέσου. Επίσης, το λογισμικό προσφέρει μεθόδους επαλήθευσης των εγκληματολογικών αντιγράφων που δημιουργεί ώστε να διασφαλίζεται η πιστότητα του αντιγράφου και η ορθότητα της χρήσης του λογισμικού (AccessData, n.d.).

XWAYS-Forensics Winhex

Το WinHex είναι στον πυρήνα του, ένα πρόγραμμα επεξεργασίας δεδομένων σε δεκαεξαδική μορφή, ιδιαίτερα χρήσιμο στον τομέα της ψηφιακής εγκληματολογίας. Επιτρέπει μεταξύ άλλων, την ανάκτηση δεδομένων και την προβολή και επεξεργασία δεδομένων χαμηλού επιπέδου (X-WAYS, n.d.).

Magnet Forensics Axiom

Το εγκληματολογικό λογισμό πάνω στο οποίο στηρίχθηκε το μεγαλύτερο μέρος της εξέτασης των εγκληματολογικών αντιγράφων της πειραματικής διαδικασίας, είναι το Axiom (MagnetForensics n.d.). Μία σουίτα εργαλείων που υποστηρίζει μεταξύ άλλων, δημιουργία εγκληματολογικών αντιγράφων από τις περισσότερες διαθέσιμες πηγές δεδομένων, συμπεριλαμβανομένων των υπολογιστών, των smartphones, υπηρεσιών νέφους και συσκευών IoT. Επιπρόσθετα, επιτρέπει την εξέταση των εν λόγω εγκληματολογικών αντιγράφων. Αρχικά χρησιμοποιείται το εργαλείο Magnet Axiom Process για την επεξεργασία των εγκληματολογικών αντιγράφων. Αφού ολοκληρωθεί η επεξεργασία τους, χρησιμοποιείται το εργαλείο Magnet Axiom Examine για την προβολή των αποτελεσμάτων της επεξεργασίας.

Belkasoft Evidence Center

Πρόγραμμα που χρησιμοποιείται στην ψηφιακή εγκληματολογία και προσφέρει παρόμοιες δυνατότητες με το προηγούμενο (Belkasoft, 2019).

DB Browser for SQLite

Ένα λογισμικού ανοιχτού κώδικα που χρησιμοποιείται για την προβολή, επεξεργασία και δημιουργία SQLite βάσεων δεδομένων (SQLiteBrowser n.d.).

VMware Workstation Pro

Το εν λόγω λογισμικό χρησιμοποιείται για τη δημιουργία και διαχείριση εικονικών μηχανών (VMware n.d.). Ανάμεσα στις δυνατότητες που προσφέρει, είναι η δημιουργία στιγμιότυπου (Snapshot) μίας εικονικής μηχανής, καθώς και η δημιουργία κλώνου (Clone) της.

CCleaner

Το εν λόγω λογισμικό χρησιμοποιείται μεταξύ άλλων, για την προστασία της ιδιωτικότητας ενός χρήστη, παρέχοντας του τη δυνατότητα διαγραφής επιλεγμένων αρχείων και ιχνών (CCleaner n.d.). Επιπρόσθετα επιτρέπει την απεγκατάσταση προγραμμάτων.

Decwindbx

Ένα λογισμικό το οποίο χρησιμοποιείται για την αποκρυπτογράφηση δεδομένων που σχετίζονται με την υπηρεσία νέφους Dropbox (Picasso 2017).

Επισημαίνεται ότι όλα τα ανωτέρω προγράμματα εκτελέστηκαν στον ηλεκτρονικό υπολογιστή του ερευνητή (υπολογιστής έρευνας) εκτός του FTK Imager και του CCleaner. Το πρώτο εκτελέστηκε στις εικονικές μηχανές της πειραματικής διαδικασίας, μέσω της προαναφερθείσας μονάδας USB (Kingston), προκειμένου να δημιουργηθούν τα εγκληματολογικά αντίγραφα της μνήμης RAM και του σκληρού δίσκου. Το δε δεύτερο εκτελέστηκε ομοίως στις εικονικές μηχανές, μέσα στα πλαίσια διαγραφής των δεδομένων χρήσης των υπηρεσιών νέφους.

6.8. Δημιουργία των εικονικών μηχανών της έρευνας

Για τη δημιουργία των εικονικών μηχανών της πειραματικής διαδικασίας χρησιμοποιήθηκε το λογισμικό VMware Workstation 14.1.1 build-7528167. Αρχικά δημιουργήθηκε μία νέα εικονική μηχανή (Base-VM), στην οποία εγκαταστάθηκε λειτουργικό σύστημα Windows 10 (ειδικότερα Windows 10 Pro 10.0.16299 Build 16299). Στην εικονική μηχανή ανατέθηκε εικονικός δίσκος συνολικής χωρητικότητας 50GB και μνήμη RAM ίση με 4GB.

Κατόπιν, χρησιμοποιήθηκε η λειτουργία δημιουργίας πλήρους (full-clone) κλώνου που προσέφερε το εν λόγω λογισμικό για τη δημιουργία των υπόλοιπων εικονικών μηχανών. Η λειτουργία αυτή επιτρέπει σε κάθε κλώνο της αρχικής εικονικής μηχανής να λειτουργεί ανεξάρτητα από τις υπόλοιπες εικονικές μηχανές, σαν να ήταν ξεχωριστός υπολογιστής. Στη συνέχεια κάθε εικονική μηχανή χρησιμοποιήθηκε ανάλογα με τα σενάρια της έρευνας.

6.9. Αρχεία που χρησιμοποιήθηκαν στην έρευνα

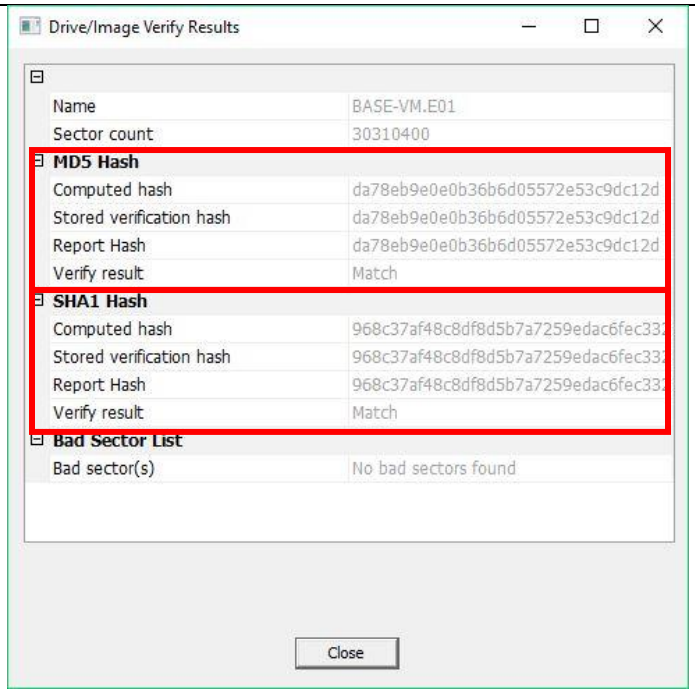
Για κάθε ένα από τα σενάρια της έρευνας που διεξήχθη, χρησιμοποιήθηκε ένας διαφορετικός αριθμός αρχείων. Ένας μέρος των αρχείων δημιουργήθηκαν στα πλαίσια της έρευνας και ένα άλλο «κατέβηκε» από τον ιστότοπο της DigitalCorpora (DigitalCorpora n.d.). Ο εν λόγω ιστότοπος χρησιμοποιείται για εκπαίδευση στην ψηφιακή εγκληματολογία.

Για όλα τα αρχεία που χρησιμοποιήθηκαν στην έρευνα, υπολογίστηκαν και καταγράφηκαν τα τεχνικά τους χαρακτηριστικά (μεταδεδομένα,hashes,κ.τ.λ.), μέσω του λογισμικού FTK Imager.

6.10. Δημιουργία εγκληματολογικών αντιγράφων

Έπειτα από τη χρήση των υπηρεσιών νέφους σε κάθε εικονική μηχανή και δημιουργίας της σχετικής δραστηριότητας, ανάλογα με το σενάριο που εξεταζόταν, συνδέθηκαν σε αυτές, η φορητή μονάδα USB και ο εξωτερικός σκληρός δίσκος. Στη συνέχεια,

από το USB εκτελέστηκε η φορητή έκδοση του λογισμικού FTK Imager και μέσω αυτού δημιουργήθηκαν τα εγκληματολογικά αντίγραφα της μνήμης RAM και του δίσκου της εκάστοτε εικονικής μηχανής. Τα εγκληματολογικά αντίγραφα αποθηκεύτηκαν απευθείας στον εξωτερικό σκληρό δίσκο. Έπειτα από τη δημιουργία τους, ακολούθησε η διαδικασία επαλήθευσης τους. Εάν η επαλήθευση ολοκληρωθεί επιτυχώς και η ταυτότητα του πειστήριου δίσκου ταυτίζεται με αυτή του εγκληματολογικού αντιγράφου, τότε θα εμφανιστεί το κάτωθι μήνυμα (Εικόνα 3) στην οθόνη. Πλέον τα αντίγραφα είναι έτοιμα για να εξεταστούν με τα εγκληματολογικά λογισμικά και παράλληλα τα αρχικά δεδομένα του δίσκου παραμένουν αναλλοίωτα από την όλη διαδικασία.



Εικόνα 3

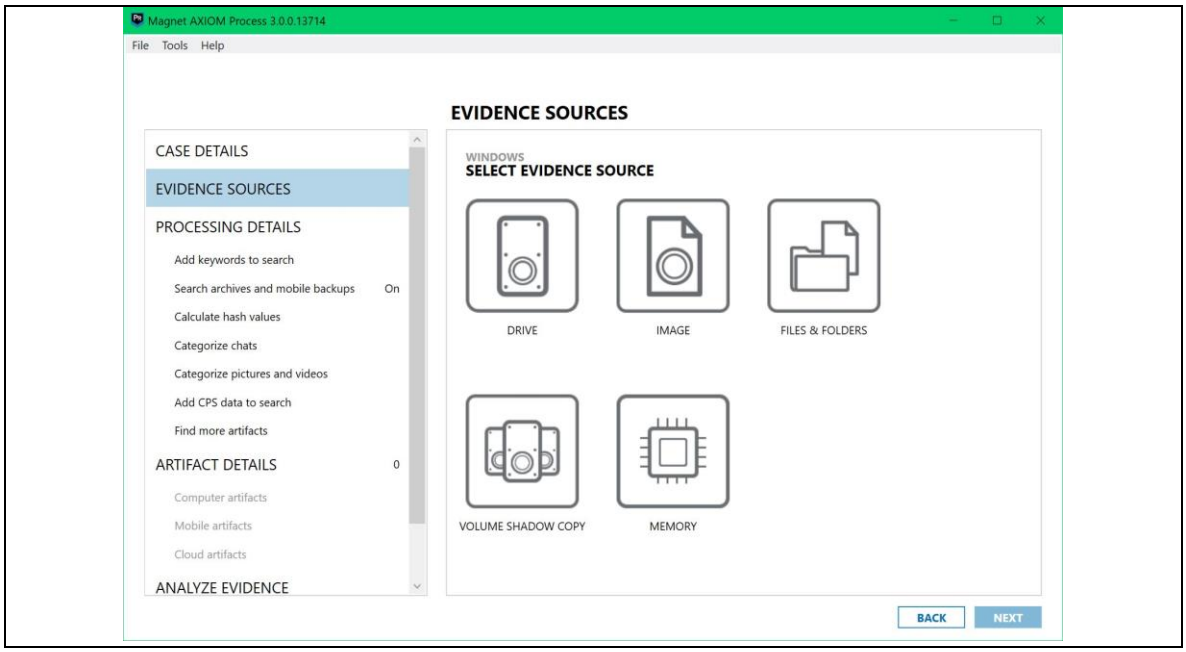
Αποτελέσματα διαδικασίας επαλήθευσης των αντιγράφων-FTK Imager

Επισημαίνεται ότι καταγράφηκαν οι ημερομηνίες και ώρες όλων των ανωτέρω ενεργειών (δηλ. σύνδεσης/αποσύνδεσης των αφαιρούμενων αποθηκευτικών μέσων, ώρα εκτέλεσης του FTK Imager, κ.ά.), προκειμένου να διασφαλιστεί η ορθότητα της διαδικασίας και η πληρότητα των αποτελεσμάτων. Όπως γίνεται αντιληπτό, όλες οι ανωτέρω ενέργειες έγιναν σύμφωνα με τα όσα ορίζουν τα πρότυπα και οι διεθνώς αναγνωρισμένες μεθοδολογίες της ψηφιακής εγκληματολογίας.

6.11. Εξέταση εγκληματολογικών αντιγράφων

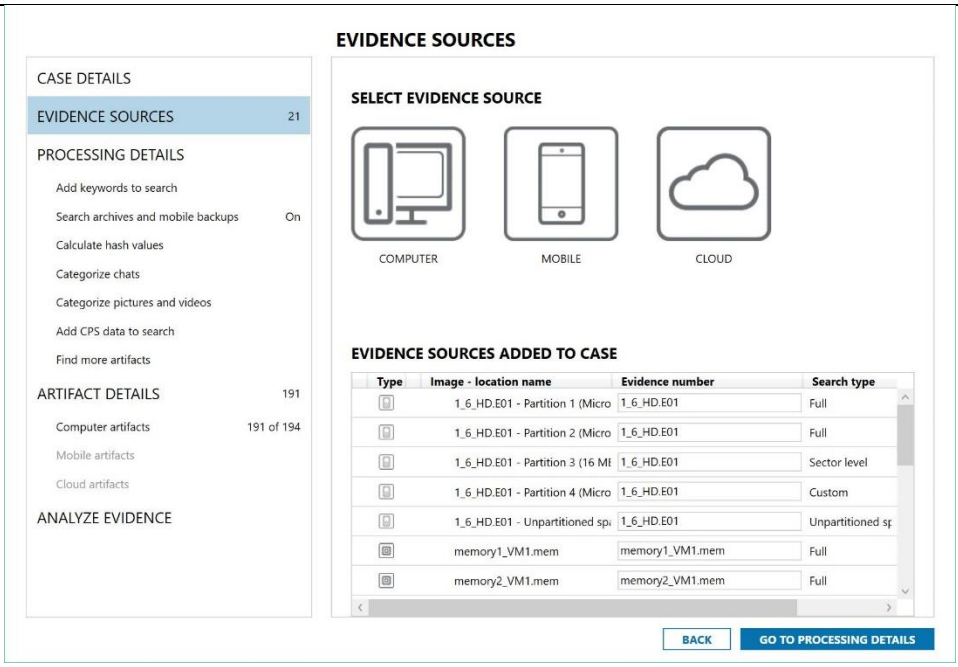
Έπειτα από τις ενέργειες του προηγούμενου κεφαλαίου και αφού επαληθευτούν τα εγκληματολογικά αντίγραφα ξεκινάει η διαδικασία εξέτασης τους. Για την εξέταση των εγκληματολογικών αντιγράφων χρησιμοποιήθηκαν κατά κύριο λόγο τα εγκληματολογικά λογισμικά Magnet Axiom 3.0.0.13714 και Winhex 19.6. Παρακάτω ακολουθεί σύντομη περιγραφή των βημάτων εξέτασης των εγκληματολογικών αντιγράφων της έρευνας:

Βήμα 1ο – Εκτέλεση του Magnet Axiom Process και φόρτωση των προς εξέταση εγκληματολογικών αντιγράφων. Το λογισμικό υποστηρίζει την επεξεργασία τόσο των αντιγράφων σκληρών δίσκων όσο και των αντιγράφων μνήμης RAM. Αφού προστεθούν όλα τα εγκληματολογικά αντίγραφα και καταχωρηθούν οι σχετικές πληροφορίες (βλ. Εικόνες 4 και 5), γίνεται μετάβαση στο επόμενο βήμα.



Εικόνα 4

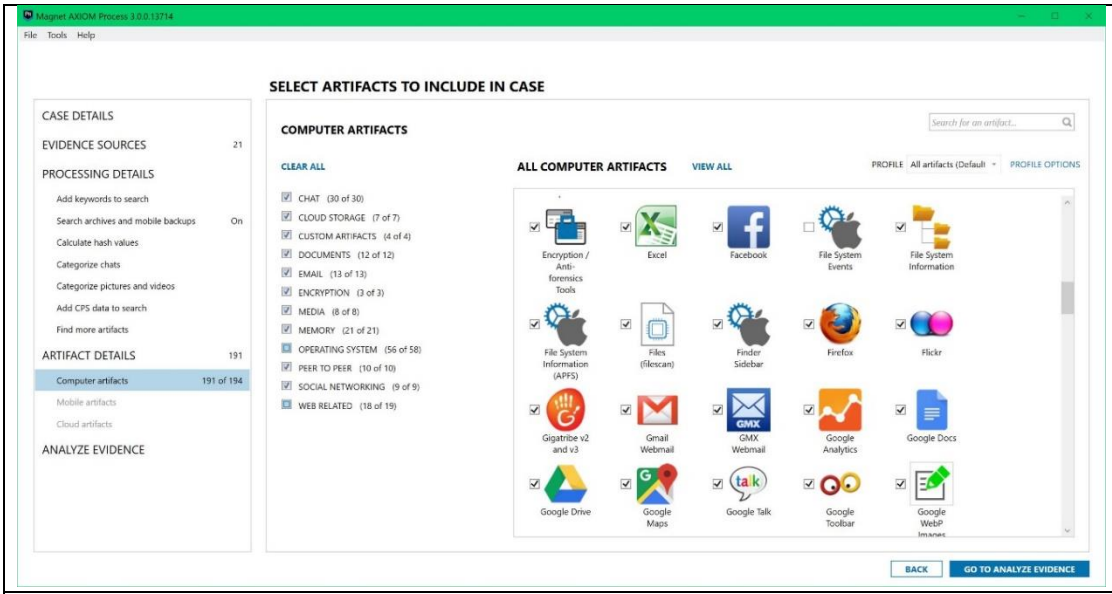
«Φόρτωση» των εγκληματολογικών αντιγράφων που θα τεθούν σε επεξεργασία Magnet Axiom Process



Εικόνα 5

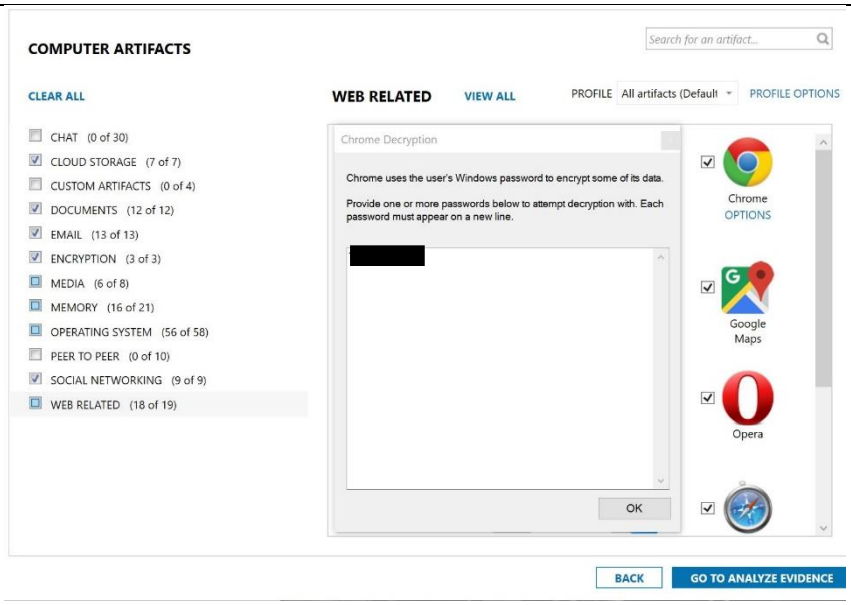
Προβολή των εγκληματολογικών αντιγράφων που είναι έτοιμα για επεξεργασία Magnet Axiom Process

Βήμα 2ο – Σε αυτό το βήμα επιλέγονται μέσω του λογισμικού οι ρυθμίσεις σχετικά με την επεξεργασία των εγκληματολογικών αντιγράφων. Ειδικότερα, σε αυτό το στάδιο επιλέγονται ποιες κατηγορίες δεδομένων καλείται να εντοπίσει το λογισμικό κατά την επεξεργασία των αντιγράφων (βλ. Εικόνα 6). Επιπρόσθετα, ο ερευνητής έχει τη δυνατότητα να επιλέξει πρόσθετες ρυθμίσεις όπως την επιλογή να γίνει αναζήτηση με λέξεις κλειδιά που εκείνος θα ορίσει. Εδώ αξίζει να σημειωθεί ότι σε Windows περιβάλλον, ορισμένες βάσεις δεδομένων που χρησιμοποιούν αφενός ο φυλλομετρητής Ιστού Google Chrome και αφετέρου η εφαρμογή της υπηρεσίας νέφους Dropbox (για αποθήκευση των δεδομένων τους), φέρουν τα δεδομένα τους κρυπτογραφημένα (Epifani 2013, ForensicsWiki 2015, Simon 2015). Για την αποκρυπτογράφηση τους, χρειάζεται μεταξύ άλλων ο κωδικός εισόδου (Windows Login Password) του χρήστη των Windows. Το εν λόγω λογισμικό επιτρέπει την αποκρυπτογράφηση τους, αρκεί σε αυτό το στάδιο ο ερευνητής να εισάγει τον κωδικό του χρήστη (βλ. Εικόνες 7 και 8). Αφού εισαχθούν οι εν λόγω πληροφορίες, μπορεί να ξεκινήσει τη διαδικασία της επεξεργασίας των αντιγράφων.



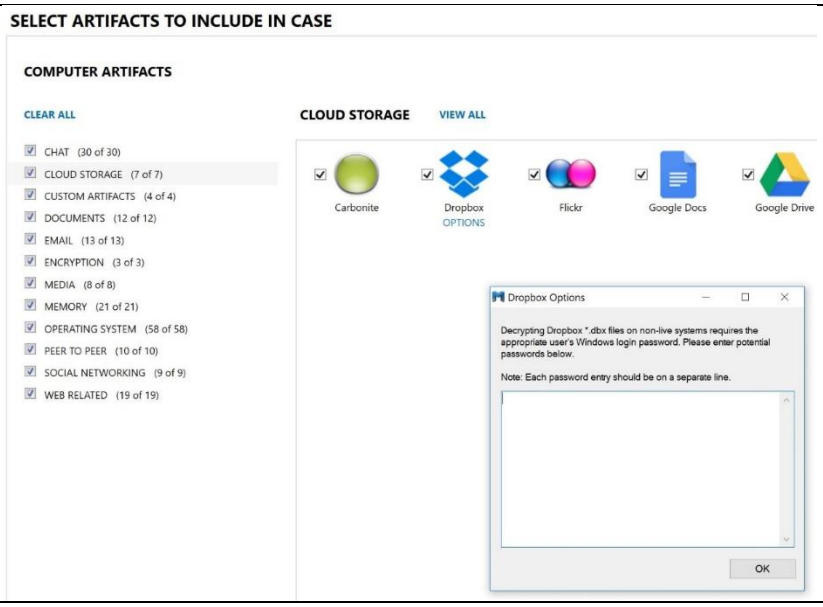
Εικόνα 6

Επιλογή των δεδομένων που θα αναζητήσει το λογισμικό κατά την επεξεργασία των εγκληματολογικών αντιγράφων-Magnet Axiom Process



Εικόνα 7

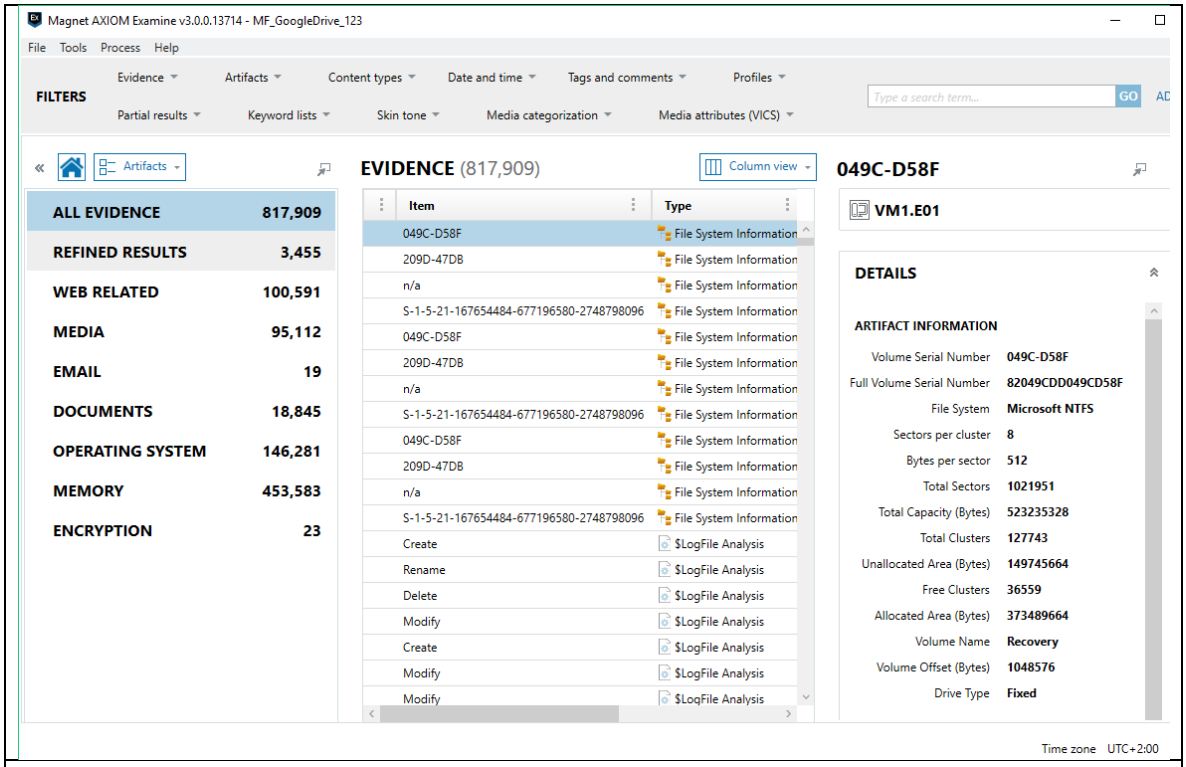
Ορισμός πιθανών κωδικών του χρήστη των Windows για αποκρυπτογράφηση των δεδομένων του φυλλομετρητή Google Chrome-Magnet Axiom Process



Εικόνα 8

Ορισμός πιθανών κωδικών του χρήστη των Windows για αποκρυπτογράφηση των δεδομένων της υπηρεσίας νέφους Dropbox-Magnet Axiom Process

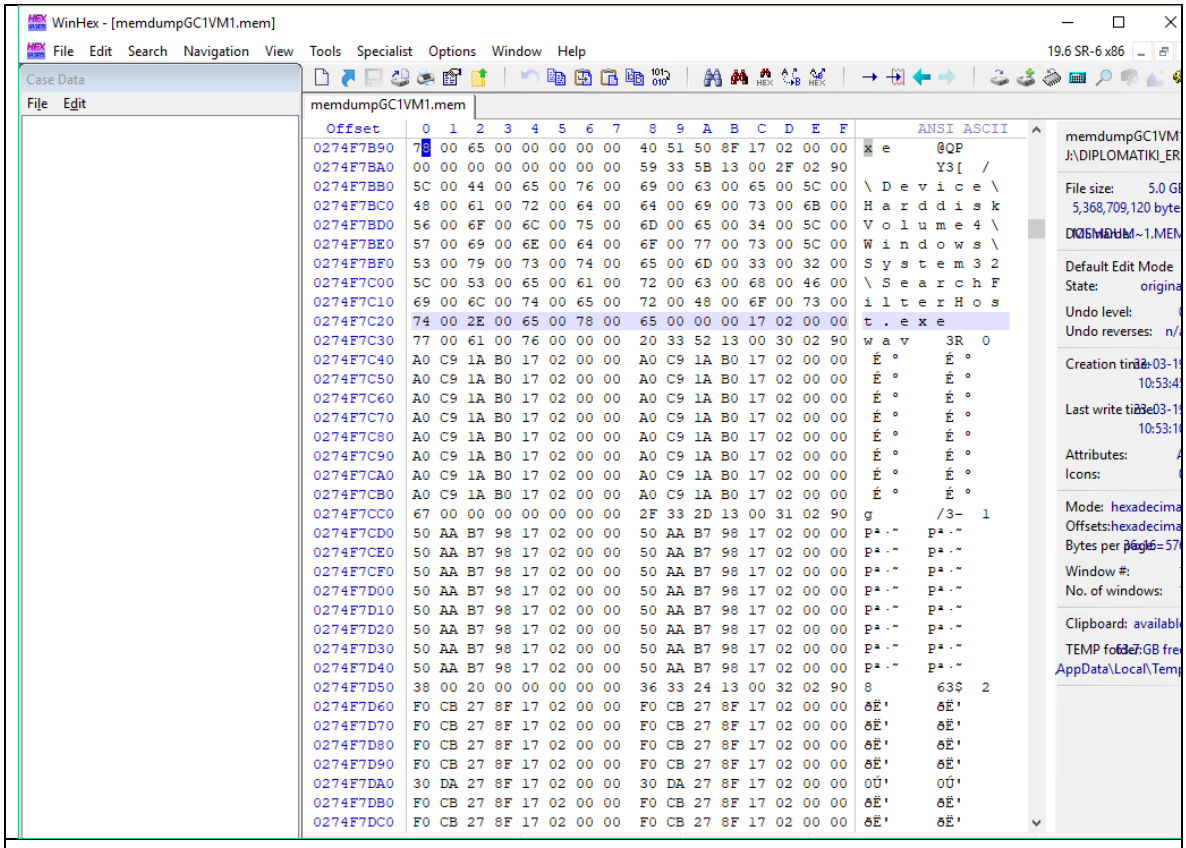
Βήμα 3ο – Αφού ολοκληρωθεί η διαδικασία της επεξεργασίας των αντιγράφων, εκτελείται το εργαλείο Magnet Axiom Examine. Το εν λόγω λογισμικό χρησιμοποιείται για την προβολή και αξιολόγηση των ευρημάτων που εντόπισε το εργαλείο Magnet Axiom Process (βλ. Εικόνα 9).



Εικόνα 9

Προβολή των ευρημάτων της επεξεργασίας των εγκληματολογικών αντιγράφων Magnet Axiom Examine

Βήμα 4ο – Ειδικά για τα εγκληματολογικά αντίγραφα της μνήμης RAM, εκτελέστηκε εκ των υστέρων και το λογισμικό Winhex. Στο εν λόγω λογισμικό έγινε χειροκίνητη αναζήτηση για ευρήματα που ενδεχομένως σχετίζονται με τα πτητικά δεδομένα της έρευνας (βλ. Εικόνα 10).



Εικόνα 10

Προβολή των δεδομένων των εγκληματολογικών αντιγράφων της μνήμης RAM Winhex

Βήμα 5ο – Στο τελευταίο βήμα έγινε σύγκριση και συσχετισμός των διαφορετικών ευρημάτων που συλλέχθηκαν στα προηγούμενα βήματα. Προς εξυπηρέτηση του σκοπού αυτού, έγινε εκτέλεση των λογισμικών DB Browser for SQLite, Belkasoft Evidence Center και Decwindbx. Επιπλέον, αναφέρεται ότι η σύγκριση των μοναδικών ταυτοτήτων των αρχείων, έγινε με τα λογισμικά Access Data FTK Imager και Magnet Axiom Examine.

Η ανωτέρω διαδικασία πραγματοποιήθηκε για την εξέταση των εγκληματολογικών αντιγράφων της πειραματικής διαδικασίας. Τα ευρήματα της διαδικασίας, παρουσιάζονται και επεξηγούνται στα επόμενα κεφάλαια.

6.12. Περιορισμοί της έρευνας

Η έρευνα της παρούσας διπλωματικής εργασίας πραγματοποιήθηκε κάτω από συγκεκριμένες συνθήκες και περιορισμούς. Αρχικά, τα ευρήματα που προέκυψαν στην παρούσα έρευνα, εξαρτώνται άμεσα από την έκδοση των λογισμικών που χρησιμοποιήθηκαν. Αυτό πρακτικά σημαίνει ότι, εάν τα ίδια εγκληματολογικά αντίγραφα εξεταστούν με μεταγενέστερη ή προγενέστερη έκδοση των εν λόγω λογισμικών, τα ευρήματα που θα προκύψουν, ενδέχεται να είναι διαφορετικά.

Εκτός όμως από την έκδοση των λογισμικών, τα ευρήματα που εντοπίστηκαν εξαρτώνται και από την έκδοση του λειτουργικού συστήματος. Γίνεται επομένως κατανοητό ότι, όλα τα κάτωθι ευρήματα αφορούν το σύστημα αρχείων NTFS και την έκδοση λειτουργικού συστήματος Windows 10 Pro 10.0.16299 Build 16299. Η αντίστοιχη εξέταση σε άλλες εκδόσεις λειτουργικών συστημάτων (Windows 7, Windows 8, MacOS, Linux, Android, κ.τ.λ.) και άλλων συστημάτων αρχείων (π.χ. EXT3) θα έχουν ως αποτέλεσμα διαφορετικά ευρήματα και κατ' επέκταση διαφορετικά συμπεράσματα.

Τέλος αναφέρεται ότι, η παρούσα έρευνα πραγματοποιήθηκε δημιουργώντας τον ελάχιστα δυνατό όγκο δεδομένων που χρειαζόταν για να ολοκληρωθούν τα σενάρια της πειραματικής διαδικασίας. Σε πραγματικές συνθήκες, σε ένα υπολογιστικό σύστημα συναντάται σημαντικά μεγαλύτερος όγκος δεδομένων και κατά συνέπεια, τα ευρήματα που εντοπίζονται δύναται να διαφέρουν.

Ολοκληρώνοντας το κεφάλαιο αυτό, έχει πλέον αποσαφηνιστεί ο ερευνητικός σκοπός της παρούσας εργασίας. Αναλυτικότερα, επεξηγήθηκαν τόσο τα ερευνητικά ερωτήματα όσο και η μεθοδολογία που υιοθετήθηκε για την απάντηση τους. Έγινε εκτενής αναφορά στις συνθήκες κάτω από τις οποίες πραγματοποιήθηκε η έρευνα (υλισμικό, λογισμικό). Ταυτόχρονα προσδιορίστηκαν και οι περιορισμοί που λήφθηκαν υπόψη. Κατόπιν των ανωτέρω, στα επόμενα κεφάλαια παρατίθενται λεπτομερώς, τα ευρήματα που προέκυψαν από την εξέταση των εγκληματολογικών αντιγράφων και τα συμπεράσματα που σχηματίστηκαν από τη μελέτη τους.

Κεφάλαιο 7ο: Εγκληματολογική εξέταση της υπηρεσίας νέφους Dropbox σε περιβάλλον Windows 10

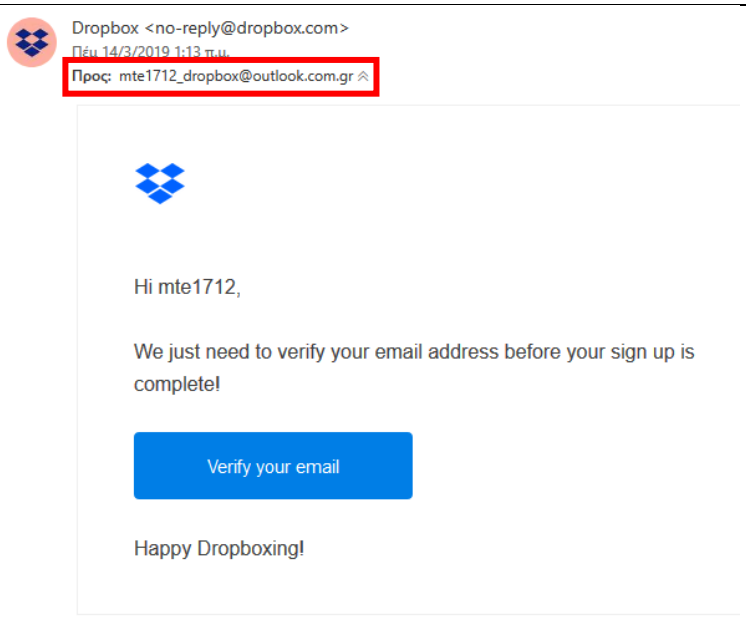
7.1. Γενικά

Το Dropbox (Dropbox 2019) είναι μία εταιρεία που προσφέρει υπηρεσίες νέφους. Ειδικότερα η εν λόγω εταιρεία παρέχει τη δυνατότητα αποθήκευσης δεδομένων στο νέφος, καθώς και τη δυνατότητα για συγχρονισμό και κοινή χρήση των αποθηκευμένων δεδομένων μεταξύ των διαφορετικών συσκευών που ο χρήστης έχει συνδέσει στον λογαριασμό του. Το Dropbox ως υπηρεσία υποστηρίζεται από όλες τις γνωστές πλατφόρμες (Windows, Android, OS X, iOS, κ.ά.).

Το Dropbox διατίθεται σε δωρεάν έκδοση η οποία προσφέρει μέχρι 2GB αποθηκευτικό χώρο, μαζί με δυνατότητες όπως η κοινή χρήση και ο συγχρονισμός των αποθηκευμένων δεδομένων του χρήστη. Διατίθεται φυσικά και σε επί πληρωμή έκδοση, η οποία δεν έχει περιορισμούς στη χρήση. Τέλος, παρέχεται και σε ειδική έκδοση για επαγγελματική χρήση, η οποία προσφέρει επιπρόσθετες δυνατότητες.

Για να χρησιμοποιήσει κάποιος την υπηρεσία Dropbox, πρέπει να εγγραφεί σε αυτήν. Για την εγγραφή χρειάζεται μία έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου και ορισμένες επιπλέον πληροφορίες από τον χρήστη (όνομα, επώνυμο και κωδικό πρόσβασης).

Στα πλαίσια της διπλωματικής εργασίας δημιουργήθηκε μία νέα διεύθυνση ηλεκτρονικού ταχυδρομείου (βλ. Εικόνα 11) η οποία και χρησιμοποιήθηκε για τη χρήση της ανωτέρω υπηρεσίας νέφους. Επιπρόσθετα, δημιουργήθηκαν δύο νέες διευθύνσεις ηλεκτρονικού ταχυδρομείου, οι οποίες χρησιμοποιήθηκαν ειδικά στα σενάρια διαμοιρασμού αρχείων μέσω της υπηρεσίας νέφους (mte1712_ShareItWithMe@outlook .com.gr και mte1712_ShareItWithMe2@gmail.com).



Εικόνα 11
Δημιουργία λογαριασμού στην υπηρεσία νέφους Dropbox στα πλαίσια της πειραματικής διαδικασίας

Ο σκοπός της εξέτασης του Dropbox είναι να εντοπιστούν ευρήματα που να σχετίζονται με τη χρήση της εν λόγω υπηρεσίας, όπως παραδείγματος χάρη, το όνομα του χρήστη, η διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί, τα αρχεία που έχουν μεταφορτωθεί μέσω αυτής, κ.ά. Τα ευρήματα αυτά εξυπηρετούν στην απάντηση των ερευνητικών ερωτημάτων της παρούσας διπλωματικής. Η εξέταση του Dropbox βασίστηκε στην υπάρχουσα βιβλιογραφία (Amirullah et al. 2016, Epifani 2013, Federici 2014, Malik et al. 2015, Marturana et al. 2012, Mehreen and Aslam 2015, Quick and Choo 2013), πλην όμως διαφοροποιείται ελαφρώς από αυτή, καθώς επικεντρώνεται στα δεδομένα που εντοπίζονται στο λειτουργικό σύστημα Windows 10 .

7.2. Προετοιμασία της εξέτασης

Αναφέρεται ότι στα πλαίσια της έρευνας δημιουργήθηκε δραστηριότητα (σε εννέα (9) εικονικές μηχανές) που αφορά σε μεταφορτώση (download/upload), προσπέλαση, επεξεργασία, δημιουργία, διαγραφή και διαμοιρασμό διαφόρων αρχείων (βλ. Κεφ. 6 για λεπτομέρειες) με χρήση της υπηρεσίας νέφους Dropbox. Κατόπιν συλλέχθηκαν εγκληματολογικά αντίγραφα των εν λόγω εικονικών μηχανών, τα οποία εξετάστηκαν προκειμένου να εντοπιστούν ίχνη της σχηματισθείσας δραστηριότητας.

Στα υποκεφάλαια που ακολουθούν παρουσιάζονται αναλυτικά όλα τα ευρήματα που προέκυψαν από την εγκληματολογική εξέταση του Dropbox και τα οποία σχετίζονται με τα ανωτέρω ερευνητικά ερωτήματα.

Γίνεται μνεία ότι, τα προγράμματα (και οι εκδόσεις τους) που χρησιμοποιήθηκαν για τη δημιουργία της δραστηριότητας στις εικονικές μηχανές, καθώς και για την εξέταση των αντιγράφων, αναφέρονται κάτωθι:

- Microsoft Windows 10 Pro 10.0.16299 N/A Build 16299,
- Mozilla Firefox 65.0.2 (64-Bit),
- Google Chrome 72.0.3626.121 (Official Build) (64-bit),
- Dropbox Client Application 69.4.102,
- CCleaner 5.55.7108 (64-Bit),
- DB Browser for SQLite 3.11.2,
- Magnet Axiom Process/Examine 3.0.0.13714,
- Winhex 19.6,
- AccessData FTK Imager 3.4.3.3,
- Belkasoft Evidence Center 9.5 και
- Decwindbx

7.3. Χρήση του λογισμικού της υπηρεσίας Dropbox

7.3.1. Γενική επισκόπηση των ευρημάτων που προέκυψαν

Έπειτα από την εγκατάσταση της εφαρμογής Dropbox (χρησιμοποιώντας τις εξ ορισμού ρυθμίσεις), δημιουργήθηκαν οι φάκελοι που περιγράφονται κάτωθι (βλ. Πίνακας 6).

Διαδρομή και όνομα φακέλου	**Περιγραφή**
C:\Program Files (x86)**Dropbox**	Αποτελεί τον φάκελο εγκατάστασης του λογισμικού. Περιλαμβάνει μεταξύ άλλων, το εκτελέσιμο αρχείο του λογισμικού.
C:\ProgramData**Dropbox**	Περιέχει κωδικοποιημένα αρχεία καταγραφής των αναβαθμίσεων του λογισμικού.
C:\Users\<username>**Dropbox**	Αποτελεί τον φάκελο που εξ ορισμού χρησιμοποιείται για τον συγχρονισμό των αρχείων του χρήστη. Περιλαμβάνει όλα τα αρχεία του χρήστη που έχουν συγχρονιστεί με τον λογαριασμό του στο νέφος. Ο χρήστης για να ανεβάσει τυχόν νέα αρχεία στο λογαριασμό του στο νέφος, το μόνο που έχει να κάνει είναι να

	μεταφέρει τα επιθυμητά αρχεία σε αυτόν τον φάκελο.
C:\Users\<username>\AppData\Local**Dropbox**	Περιλαμβάνει όλα τα αρχεία του λογισμικού που σχετίζονται αφενός με διάφορες ρυθμίσεις του λογισμικού και αφετέρου με τη δραστηριότητα του συγκεκριμένου χρήστη.
C:\Users\<username>\AppData\Roaming**Dropbox**	Δεν κατέστη εφικτός ο προσδιορισμός της λειτουργίας του εν λόγω φακέλου και των περιεχομένων του.

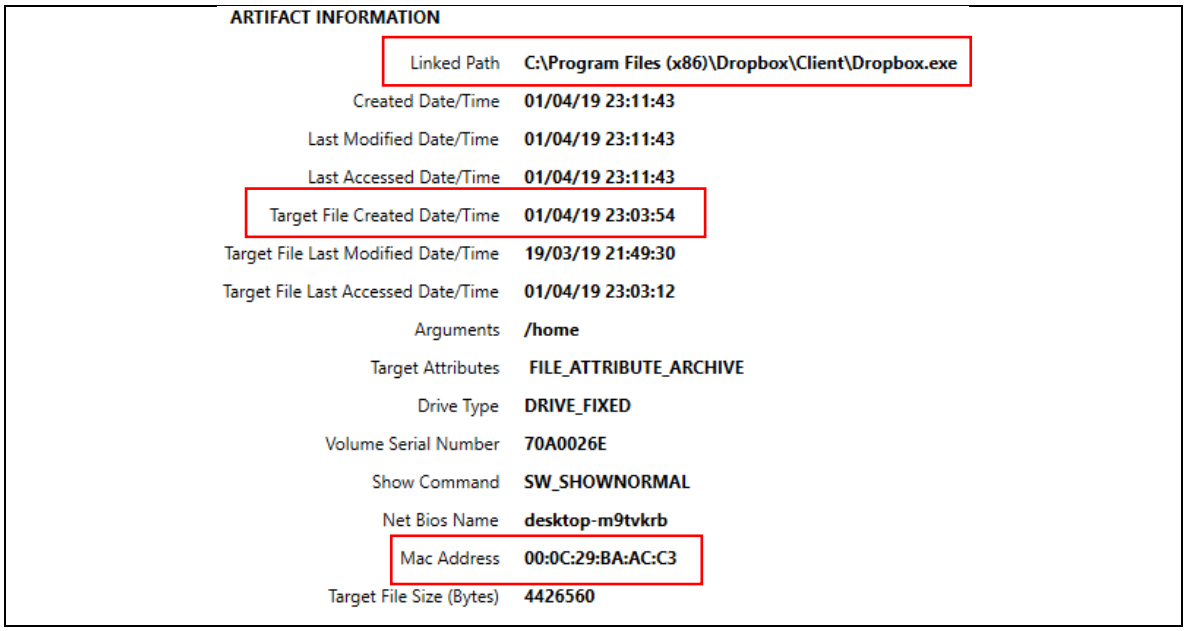
Πίνακας 6

Φάκελοι που δημιουργούνται έπειτα από την εγκατάσταση του λογισμικού της υπηρεσίας νέφους Dropbox

Επιπρόσθετα εντοπίστηκαν αρκετά στοιχεία που καταδεικνύουν τόσο την εγκατάσταση όσο και την εκτέλεση του λογισμικού Dropbox. Τα στοιχεία αυτά σχετίζονται άμεσα με το λειτουργικό σύστημα Windows 10. Ειδικότερα, βρέθηκαν:

- Αρχεία καταγραφής συμβάντων των Windows (Windows Event Logs),
- Αρχεία συντομεύσεων (.LNK files),
- Εγγραφές στο μητρώο καταγραφής των Windows (Windows Registry),
- Εγγραφές δραστηριότητας του λογισμικού του Dropbox (Prefetch Files), κ.ά.

Ενδεικτικά, παρουσιάζονται κάτωθι ορισμένα εκ των ανωτέρω ευρημάτων (βλ. Εικόνες 12-14).



Εικόνα 12

Αρχείο συντόμευσης (.LNK files)

Διαδρομή Αρχείου: C:\Users\<username>\Desktop\Dropbox.lnk

ARTIFACT INFORMATION

Event ID	**1040**
Security User ID	**S-1-5-21-167654484-677196580-2748798096-1001**
Created Date/Time	**01/04/19 23:02:32**
Event Description Summary	**Beginning a Windows Installer transaction.**
Level	**Information**
Keywords	**0x0080000000000000**
Provider Name	**MsiInstaller**
Task Category	**0**
Computer	**DESKTOP-M9TVKRB**
Event Data	**<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="MsiInstaller" /><EventID Qualifiers="0">1040</EventID><Level>4</Level><Task>0</Task><Keywords>0x0080000000000000</Keywords><TimeCreated SystemTime="2019-04-01T20:02:32.2080606Z" /><EventRecordID>570</EventRecordID><Channel>Application</Channel><Computer>DESKTOP-M9TVKRB</Computer><Security UserID="S-1-5-21-167654484-677196580-2748798096-1001" /></System><EventData><Data>C:\Program Files (x86)\Dropbox\Update\1.3.189.1\DropboxUpdateHelper.msi5968(NULL)(NULL)(NULL)(NULL)</Data><Binary></Binary>**

Εικόνα 13

Αρχείο καταγραφής συμβάντων των Windows (Windows Event Logs)

Διαδρομή Αρχείου: C:\Windows\System32\winevt\Logs\Application.evtx

ARTIFACT INFORMATION

Application Name	**DROPBOX.EXE**
Application Run Count	**13**
Last Run Date/Time	**02/04/19 00:14:31**
2nd Last Run Date/Time	**02/04/19 00:14:30**
3rd Last Run Date/Time	**02/04/19 00:14:30**
4th Last Run Date/Time	**02/04/19 00:02:01**
5th Last Run Date/Time	**02/04/19 00:02:01**

Εικόνα 14

Αρχείο δραστηριότητας του λογισμικού του Dropbox (Prefetch Files),

Διαδρομή Αρχείου: C:\Windows\Prefetch\DROPBOX.EXE-41A1197E.pf

Εντοπίστηκαν επιπλέον στη διαδρομή C:\Users\<username>\Dropbox, όλα τα αρχεία του χρήστη που ανήκουν στο λογαριασμό του και έχουν συγχρονιστεί με το λογισμικό του Dropbox στον υπολογιστή του. Από την εξέταση των μεταδεδομένων των αρχείων, μπορούν να εξαχθούν συμπεράσματα σχετικά με το πότε αυτά «κατέβηκαν» στον υπολογιστή του χρήστη από τον λογαριασμό του στο Dropbox ή το ανάποδο.

Μέχρι στιγμής, από τα προαναφερθέντα στοιχεία αποδεικνύεται η χρήση του λογισμικού Dropbox, όπως επίσης και η ύπαρξη αρχείων που σχετίζονται με το λογαριασμό ενός συγκεκριμένου χρήστη. Στη συνέχεια γίνεται προσπάθεια εντοπισμού τόσο των στοιχείων του εν λόγω χρήστη όσο και της δραστηριότητας του, μέσω της ανάλυσης των δεδομένων που προέκυψαν.

7.3.2. Εντοπισμός και ανάλυση της δραστηριότητας του χρήστη

Εντοπίστηκαν στοιχεία που βοήθησαν στην εξακρίβωση ορισμένων ενεργειών που πραγματοποίησε ο χρήστης, χρησιμοποιώντας την υπηρεσία Dropbox. Κάτωθι παρουσιάζονται (βλ. Εικόνες 15-18) τα δεδομένα που εντοπίστηκαν και μπορούν να αποδοθούν σε μία συγκεκριμένη ενέργεια του χρήστη:

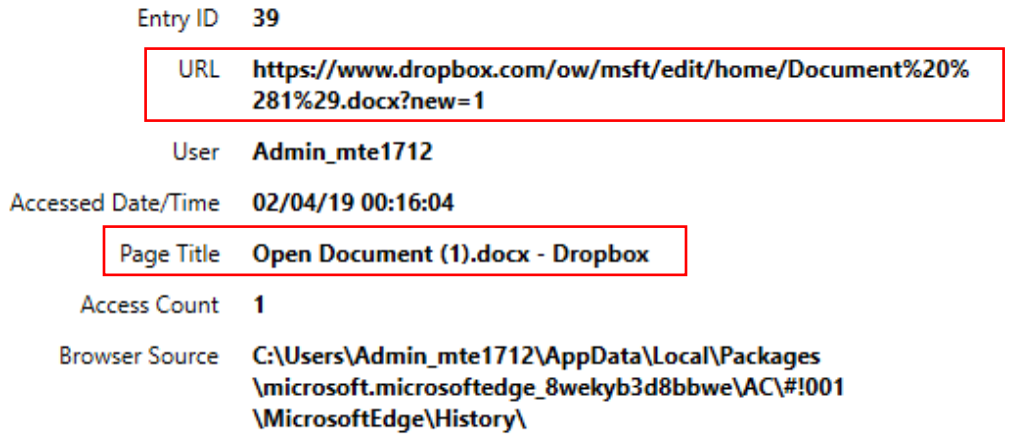
1. **Δημιουργία νέων αρχείων** (βλ. Εικόνες 15 και 16)
   - Εγγραφές στον φυλλομετρητή Ιστού αποδεικνύουν τη δημιουργία νέων αρχείων (επισημαίνεται ότι η εφαρμογή Dropbox δεν επιτρέπει την απευθείας δημιουργία νέων αρχείων μέσω αυτής. Αντί αυτού χρειάζεται πρόσβαση μέσω φυλλομετρητή Ιστού για τη δημιουργία νέων αρχείων).

Entry ID	43
URL	https://www.dropbox.com/ow/msft/edit/home/Book%20%281%29.xlsx?new=1
User	Admin_mte1712
Accessed Date/Time	02/04/19 00:17:32
Page Title	Open Book (1).xlsx - Dropbox
Access Count	1
Browser Source	C:\Users\Admin_mte1712\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\History\

Εικόνα 15

Δημιουργία νέου αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, στην υπηρεσία Dropbox

Διαδρομή Αρχείου: C:\Users\Admin_mte1712\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV01.dat



Εικόνα 16

Δημιουργία νέου αρχείου κειμένου μέσω φυλλομετρητή Ιστού, στην υπηρεσία Dropbox

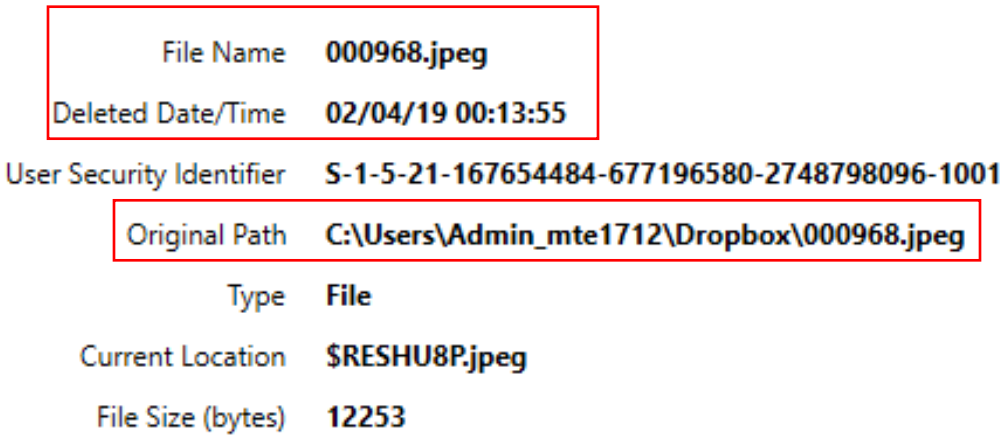
Διαδρομή Αρχείου: C:\Users\Admin_mte1712\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

2. **Διαγραφή αρχείων** (βλ. Εικόνες 17 και 18)
   - Στον κάδο ανακύκλωσης του χρήστη εντοπίστηκαν διαγεγραμμένα αρχεία τα οποία ήταν προηγουμένως συγχρονισμένα με το λογαριασμό του στο νέφος. Επισημαίνεται ότι κατέστη εφικτή η ανάκτηση της ημερομηνίας διαγραφής τους, όπως επίσης ανακτήθηκε και η διαδρομή στην οποία βρισκόταν αρχικά αποθηκευμένα, πριν να διαγραφούν.

File Name	Deleted Date/Time	Original Path
000968.jpeg	02/04/19 00:13:55	C:\Users\Admin_mte1712\Dropbox\000968.jpeg
000897 (1).jpeg	02/04/19 00:13:55	C:\Users\Admin_mte1712\Dropbox\000897 (1).jpeg
000900 (1).jpeg	02/04/19 00:13:55	C:\Users\Admin_mte1712\Dropbox\000900 (1).jpeg

Εικόνα 17

Διαγεγραμμένα αρχεία του χρήστη, τα οποία βρίσκονταν αποθηκευμένα στο Dropbox
Διαδρομή Αρχείου: C:\$Recycle.Bin\S-1-5-21-167654484-677196580-2748798096-1001



Εικόνα 18

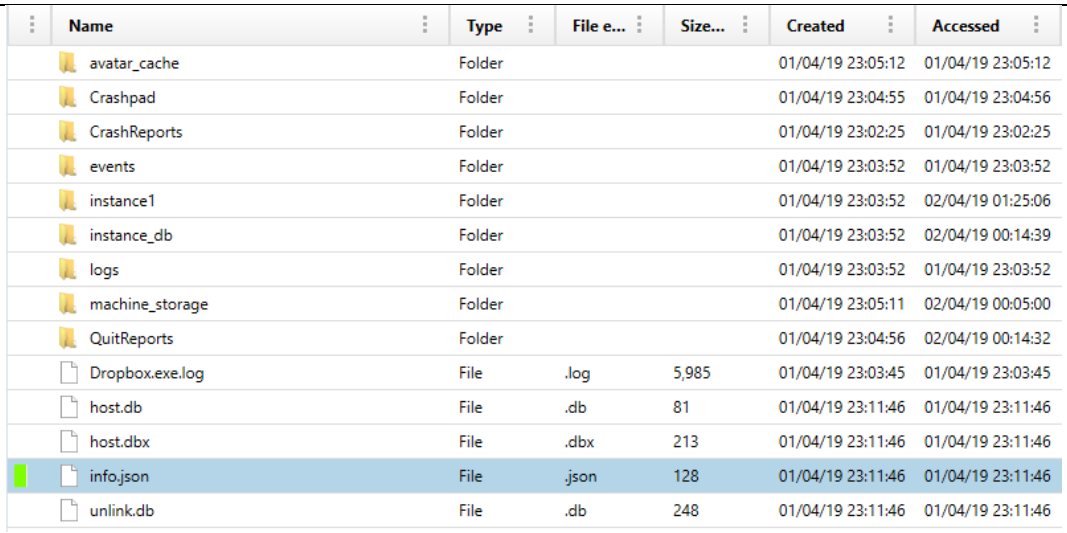
Διαγεγραμμένο αρχείο του χρήστη, το οποίο βρισκόταν αποθηκευμένο στο Dropbox
Διαδρομή Αρχείου: C:\$Recycle.Bin\S-1-5-21-167654484-677196580-2748798096-1001\$IESHU8P.jpeg

Η ανάλυση της δραστηριότητας του χρήστη συνεχίζεται και στο επόμενο υποκεφάλαιο.

7.3.3. Εξέταση των αρχείων του λογισμικού του Dropbox

Σε αυτό το υποκεφάλαιο γίνεται εξέταση των αρχείων που εμπεριέχονται στη διαδρομή C:\Users\<username>\AppData\Local\Dropbox. Αυτός ο φάκελος όπως αναφέρθηκε και προηγουμένως (βλ. Πίνακα 6), περιέχει φακέλους και αρχεία που σχετίζονται άμεσα με τη χρήση της εφαρμογής Dropbox. Αναλυτικά αναφέρονται τα εξής:

- Στην ανωτέρω διαδρομή εντοπίστηκε ένα αρχείο με ονομασία ***info.json*** (βλ. Εικόνα 19). Στο αρχείο αυτό αποθηκεύεται μεταξύ άλλων, ένα αναγνωριστικό το οποίο αντιστοιχεί στη συγκεκριμένη εγκατάσταση του λογισμικού Dropbox. Αυτό σημαίνει ότι μπορεί να διαπιστωθεί αν τα αρχεία που «ανέβηκαν» στο νέφος του λογαριασμού του χρήστη, προέρχονται από τη συγκεκριμένη εφαρμογή ή από άλλη (βλ. Εικόνα 20).



Name	Type	File e...	Size...	Created	Accessed
avatar_cache	Folder			01/04/19 23:05:12	01/04/19 23:05:12
Crashpad	Folder			01/04/19 23:04:55	01/04/19 23:04:56
CrashReports	Folder			01/04/19 23:02:25	01/04/19 23:02:25
events	Folder			01/04/19 23:03:52	01/04/19 23:03:52
instance1	Folder			01/04/19 23:03:52	02/04/19 01:25:06
instance_db	Folder			01/04/19 23:03:52	02/04/19 00:14:39
logs	Folder			01/04/19 23:03:52	01/04/19 23:03:52
machine_storage	Folder			01/04/19 23:05:11	02/04/19 00:05:00
QuitReports	Folder			01/04/19 23:04:56	02/04/19 00:14:32
Dropbox.exe.log	File	.log	5,985	01/04/19 23:03:45	01/04/19 23:03:45
host.db	File	.db	81	01/04/19 23:11:46	01/04/19 23:11:46
host.dbx	File	.dbx	213	01/04/19 23:11:46	01/04/19 23:11:46
info.json	File	.json	128	01/04/19 23:11:46	01/04/19 23:11:46
unlink.db	File	.db	248	01/04/19 23:11:46	01/04/19 23:11:46

Εικόνα 19

Διαδρομή που βρέθηκε το αρχείο info.json

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Dropbox

PREVIEW

{"personal": {"path": "C:\\Users\\Admin_mte1712\\Dropbox", "host": 51758901712, "is_team": false, "subscription_type": "Basic"}}

Εικόνα 20

Αναγνωριστικό της συγκεκριμένης εγκατάστασης του Dropbox

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Dropbox\info.json

- Στη διαδρομή C:\Users\<username>\AppData\Local\Dropbox\instance1 εντοπίστηκαν βάσεις δεδομένων, οι οποίες περιείχαν πολύ χρήσιμα στοιχεία για έναν ερευνητή. Πιο συγκεκριμένα, οι κυριότερες βάσεις δεδομένων που πρέπει να απασχολήσουν τον ερευνητή είναι αυτές που φαίνονται στον ακόλουθο πίνακα (βλ. Πίνακα 7). Αξίζει να σημειωθεί εδώ ότι, η πρόσβαση στα περιεχόμενα των βάσεων δεδομένων δεν ήταν αρχικά εφικτή, καθώς τα εν λόγω αρχεία ήταν κρυπτογραφημένα. Για την αποκρυπτογράφηση τους χρησιμοποιήθηκαν τα προγράμματα Belkasoft Evidence Center και decwindbx.

Διαδρομή και όνομα αρχείου βάσης δεδομένων	Περιγραφή
C:\Users\<username>\App Data\Local\Dropbox\instance1**config.dbx**	Περιλαμβάνει δεδομένα όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στην εφαρμογή Dropbox.
C:\Users\<username>\App Data\Local\Dropbox\instance1\ **filecache.dbx**	Περιέχει πληροφορίες για τα αρχεία που έχουν συγχρονιστεί, με το λογαριασμό του συνδεδεμένου χρήστη.

Πίνακας 7

Αρχεία βάσεων δεδομένων της εφαρμογής Dropbox που παρουσιάζουν ενδιαφέρον, για τον ερευνητή ψηφιακής εγκληματολογίας

Κατόπιν της αποκρυπτογραφήσεως τους, κάτωθι παρουσιάζονται μερικά από τα δεδομένα που έφεραν αποθηκευμένα (βλ. Εικόνες 21-23):

12	host_id	f38193caa8b21b176eed55508f839155
13	root_ns	5119861008
14	email	mte1712_dropbox@outlook.com.gr
15	userdisplayname	mte1712 Dropbox
16	displayname	DESKTOP-M9TVKRB
17	home_ns_path	
18	dropbox_path	C:\Users\Admin_mte1712\Dropbox

Εικόνα 21

Email και όνομα χρήστη του συνδεδεμένου λογαριασμού στο Dropbox- πίνακας config

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Dropbox\instance1\config.dbx

server_path	ineid_	eid_v	ineid	fileid	fileid_rev	date_added
Filter					Filter	Filter
5119861008:/dataset2/testdataset2.docx	140...	188...	p/X...	FS...	6	1554152941.5744
5119861008:/000897 (1).jpeg	112...	188...	uD...	FS...	1	1554153244.96413
5119861008:/000900 (1).jpeg	112...	188...	dvS...	FS...	1	1554153244.97996
5119861008:/000968.jpeg	112...	188...	Iwn...	FS...	1	1554153244.97996
5119861008:/document (1).docx	197...	188...	mE...	FS...	1	1554153377.51618
5119861008:/book (1).xlsx	844...	188...	rnp...	FS...	2	1554153479.34555
5119861008:/clienttest2.xlsx	197...	188...	ErX...	FS...	3	1554153482.22302

Εικόνα 22

Αρχεία που είτε έχουν διαγραφεί είτε έχουν μετανομοαστεί στην εφαρμογή Dropbox.
πίνακας-deleted_fileids
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Dropbox\instance1\ filecache.dbx

server_path	local_host_id	local_filename	local_ctime
Filter	Filter	Filter	Filter
5119861008:/dataset2/testdataset2.docx	51758901712	testDataset2.docx	1554152939
5119861008:/clienttest2.xlsx	2988542027	clienttest2.xlsx	1554153481
5119861008:/dataset2/testexcelgc.xlsx	2988542027	TestExcelGC.xlsx	1553332876
5119861008:/testexcel.xlsx	2988542027	TestExcel.xlsx	1553321566
5119861008:/testdoc2.docx	2988542027	TestDoc2.docx	1553321650
5119861008:/presentation_test.pptx	2988542027	Presentation_Test.pptx	1553321727
5119861008:/isthislove.pptx	2988542027	IsThisLove.pptx	1553208793
5119861008:/dataset2/incognitogccreated.docx	2988542027	IncognitoGCCreated.docx	1553336796
5119861008:/get started with dropbox.pdf	1	Get Started with Dropbox.pdf	1552518808
5119861008:/get started with dropbox paper.url	1	Get Started with Dropbox Paper.url	1552518808
5119861008:/dataset2/gcactivated.xlsx	2988542027	GCActivated.xlsx	1553336999

Εικόνα 23

Πληροφορίες αρχείων που έχουν μεταφορτωθεί στην εφαρμογή Dropbox.
πίνακας-file_journal
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Dropbox\instance1\ filecache.dbx

Από την ανωτέρω Εικόνα 21 αποδεικνύεται ότι ο συνδεδεμένος λογαριασμός με την εφαρμογή Dropbox, φέρει διεύθυνση ηλεκτρονικού ταχυδρομείου την mte1712_dropbox@outlook.com.gr. Επιπρόσθετα, στην Εικόνα 22 φαίνονται πότε διαγράφηκαν ή μετονομάστηκαν τα αρχεία που υπήρξαν συγχρονισμένα με την εφαρμογή Dropbox (η ώρα βρίσκεται σε μορφή ώρας epoch time, οπότε χρειάζεται μετατροπή). Τέλος, στην Εικόνα 23 φαίνεται από ποιο αναγνωριστικό (αναγνωριστικό εγκατάστασης – βλ. Εικόνα 20) της εφαρμογής Dropbox έγινε η μεταφόρτωση των αναγραφόμενων αρχείων και πότε έγινε αυτή (ο κωδικός 1 στο πεδίο local_host_id αντιστοιχεί πιθανότατα σε μεταφόρτωση μέσω φυλλομετρητή Ιστού).

Ενδέχεται να υπάρχουν και άλλα αποδεικτικά στοιχεία στις βάσεις δεδομένων που εντοπίστηκαν στην ανωτέρω διαδρομή. Ωστόσο αυτά που έχουν ήδη αναφερθεί, αρκούν για να αποδείξουν όχι μόνο τη χρήση της εφαρμογής Dropbox αλλά και επιπλέον τις ενέργειες στις οποίες προέβη ο χρήστης μέσω αυτής.

Στο επόμενο υποκεφάλαιο γίνεται εξέταση των πτητικών δεδομένων της μνήμης RAM και παρουσίαση των ευρημάτων που προέκυψαν από αυτή.

7.3.4. Εξέταση της μνήμης RAM

Κατά την εξέταση της μνήμης RAM εντοπίστηκε η διεύθυνση ηλεκτρονικού ταχυδρομείου του λογαριασμού που ήταν συνδεδεμένος στην εφαρμογή Dropbox και το όνομα του χρήστη στον οποίο άνηκε. Τα ευρήματα προέκυψαν αναζητώντας στα εγκληματολογικά αντίγραφα της μνήμης, τις συμβολοσειρές που απεικονίζονται κάτωθι (βλ. Πίνακας 8). Μερικά ευρήματα παρουσιάζονται στις εικόνες (βλ. Εικόνες 24 και 25).

Συμβολοσειρές (Strings)	Περιγραφή
Iemail	Αναζητώντας αυτές τις συμβολοσειρές εμφανίζεται η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στην εφαρμογή Dropbox
'email' =	
"email":	
"display_name":	
"userdisplayname"	Αναζητώντας αυτές τις συμβολοσειρές εμφανίζεται το όνομα του χρήστη της εφαρμογής Dropbox
"UserName":"	
++userdisplayname	
"display_name":	

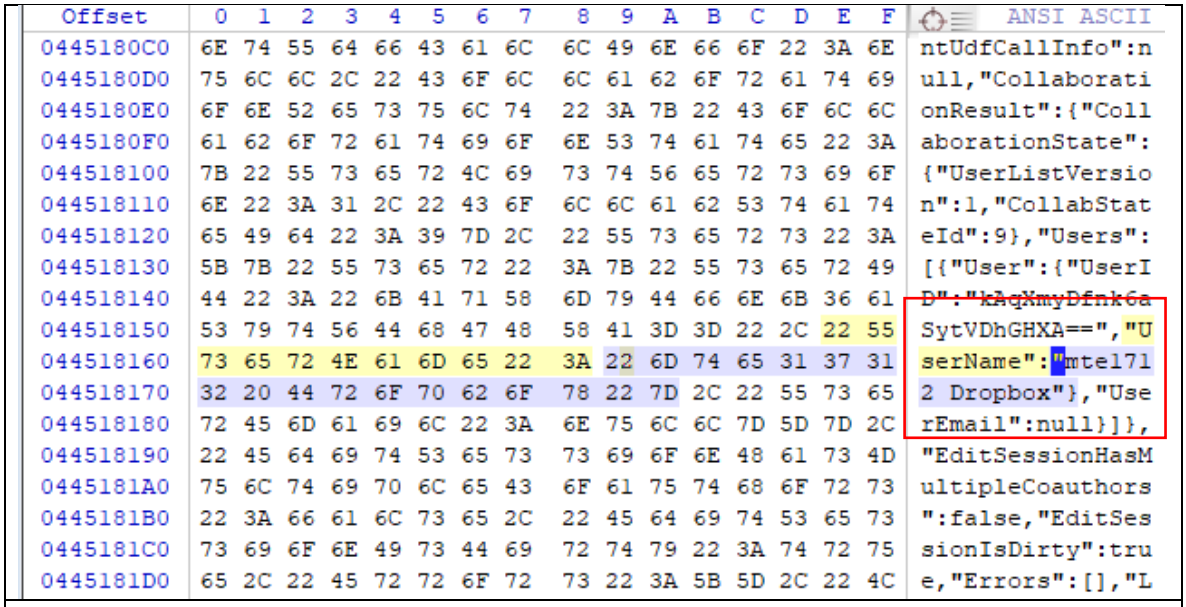
Πίνακας 8

Ευρήματα στη μνήμη RAM

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
1199C7000	2C	20	22	79	75	76	22	5D	2C	20	22	62	6C	6F	63	6B	, "yuv"], "block
1199C7010	73	65	72	76	65	72	22	3A	20	22	62	6C	6F	63	6B	2D	server": "block-
1199C7020	65	64	67	65	2D	61	6E	79	63	61	73	74	2E	64	72	6F	edge-anycast.dro
1199C7030	70	62	6F	78	2E	63	6F	6D	22	2C	20	22	73	73	63	76	pbox.com", "sscv
1199C7040	73	65	72	76	65	72	22	3A	20	22	63	6C	69	65	6E	74	server": "client
1199C7050	2D	77	65	62	2E	64	72	6F	70	62	6F	78	2E	63	6F	6D	-web.dropbox.com
1199C7060	22	2C	20	22	6D	65	74	61	73	65	72	76	65	72	22	3A	", "metaserver":
1199C7070	20	22	63	6C	69	65	6E	74	2E	64	72	6F	70	62	6F	78	"client.dropbox
1199C7080	2E	63	6F	6D	22	2C	20	22	65	6D	61	69	6C	22	3A	20	.com", "email":
1199C7090	22	6D	74	65	31	37	31	32	5F	64	72	6F	70	62	6F	78	"mte1712_dropbox
1199C70A0	40	6F	75	74	6C	6F	6F	6B	2E	63	6F	6D	2E	67	72	22	@outlook.com.gr"
1199C70B0	2C	20	22	69	6E	66	69	6E	69	74	65	5F	6D	6F	64	75	, "infinite_modu
1199C70C0	6C	65	5F	62	6C	61	63	6B	6C	69	73	74	22	3A	20	7B	le_blacklist": {
1199C70D0	22	76	65	72	73	69	6F	6E	22	3A	20	31	2C	20	22	62	"version": 1, "b
1199C70E0	6C	61	63	6B	5F	6C	69	73	74	22	3A	20	5B	5B	22	64	lack_list": [["d
1199C70F0	72	6F	70	62	6F	78	69	6E	63	6F	6D	70	61	74	2E	73	ropboxincompat.s
1199C7100	79	73	22	2C	20	22	2A	22	5D	2C	20	5B	22	61	63	66	ys", "*"], ["acf

Εικόνα 24

Η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Dropbox



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0445180C0	6E	74	55	64	66	43	61	6C	6C	49	6E	66	6F	22	3A	6E	ntUdfCallInfo":n
0445180D0	75	6C	6C	2C	22	43	6F	6C	6C	61	62	6F	72	61	74	69	ull,"Collaborati
0445180E0	6F	6E	52	65	73	75	6C	74	22	3A	7B	22	43	6F	6C	6C	onResult":{"Coll
0445180F0	61	62	6F	72	61	74	69	6F	6E	53	74	61	74	65	22	3A	aborationState":
044518100	7B	22	55	73	65	72	4C	69	73	74	56	65	72	73	69	6F	{"UserListVersio
044518110	6E	22	3A	31	2C	22	43	6F	6C	6C	61	62	53	74	61	74	n":1,"CollabStat
044518120	65	49	64	22	3A	39	7D	2C	22	55	73	65	72	73	22	3A	eId":9},"Users":
044518130	5B	7B	22	55	73	65	72	22	3A	7B	22	55	73	65	72	49	[{"User":{"UserI
044518140	44	22	3A	22	6B	41	71	58	6D	79	44	66	6E	6B	36	61	D":"kAqXmyDfnk6a
044518150	53	79	74	56	44	68	47	48	58	41	3D	3D	22	2C	22	55	SytVDhGHXA==","U
044518160	73	65	72	4E	61	6D	65	22	3A	22	6D	74	65	31	37	31	serName":"mte171
044518170	32	20	44	72	6F	70	62	6F	78	22	7D	2C	22	55	73	65	2 Dropbox"},"Use
044518180	72	45	6D	61	69	6C	22	3A	6E	75	6C	6C	7D	5D	7D	2C	rEmail":null}]},
044518190	22	45	64	69	74	53	65	73	73	69	6F	6E	48	61	73	4D	"EditSessionHasM
0445181A0	75	6C	74	69	70	6C	65	43	6F	61	75	74	68	6F	72	73	ultipleCoauthors
0445181B0	22	3A	66	61	6C	73	65	2C	22	45	64	69	74	53	65	73	":false,"EditSes
0445181C0	73	69	6F	6E	49	73	44	69	72	74	79	22	3A	74	72	75	sionIsDirty":tru
0445181D0	65	2C	22	45	72	72	6F	72	73	22	3A	5B	5D	2C	22	4C	e,"Errors":[],"L

Εικόνα 25

Το καταχωρημένο όνομα χρήστη του συνδεδεμένου λογαριασμού στο Dropbox

Εφόσον εντοπίστηκαν ικανοποιητικά ευρήματα σχετικά με τη χρήση της εφαρμογής Dropbox, θα ερευνηθεί στο επόμενο υποκεφάλαιο, εάν συμβαίνει το ίδιο και έπειτα από την απεγκατάσταση της εφαρμογής Dropbox.

7.3.5. Απεγκατάσταση του λογισμικού του Dropbox

Σε αυτό το υποκεφάλαιο γίνεται απεγκατάσταση της εφαρμογής Dropbox σε 2 εικονικές μηχανές και γίνεται προσπάθεια εντοπισμού παρόμοιων δεδομένων με αυτών που εντοπίστηκαν προηγουμένως. Στη μία εικονική μηχανή η απεγκατάσταση γίνεται μέσω του λειτουργικού συστήματος των Windows, ενώ στην άλλη μέσω τρίτου προγράμματος και ειδικότερα με χρήση του CCleaner.

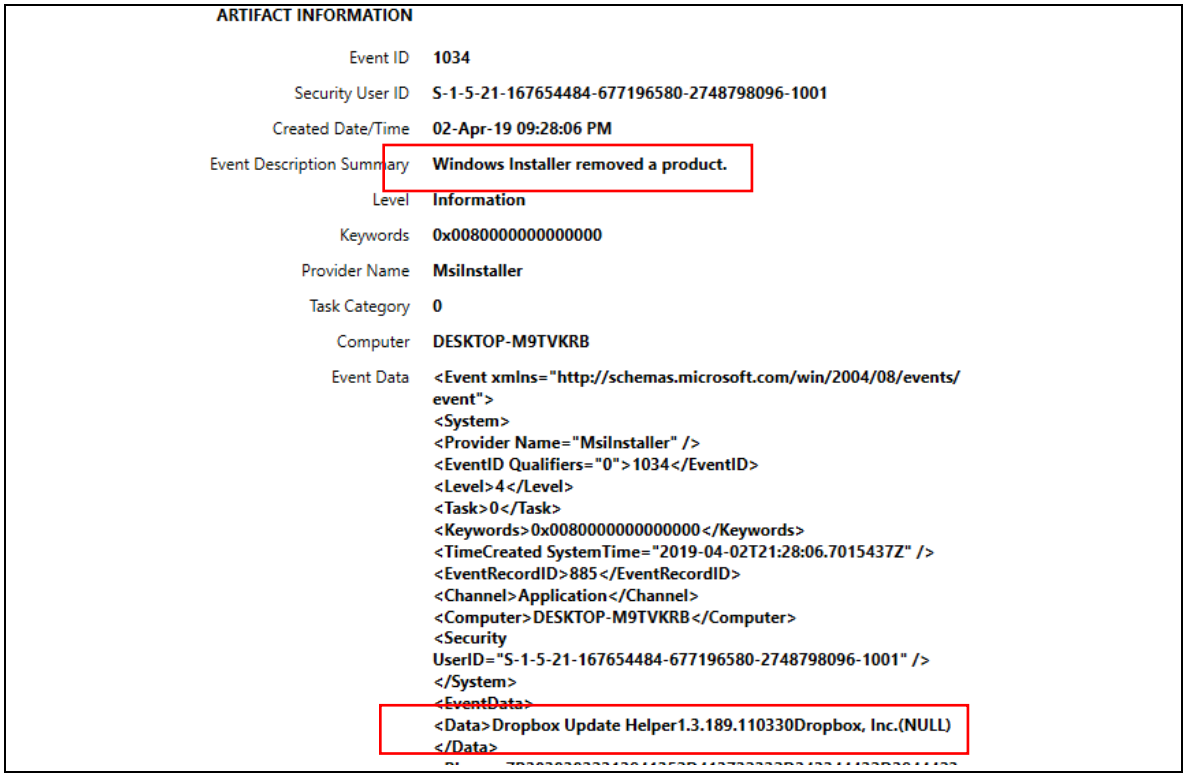
Έπειτα από την απεγκατάσταση της εφαρμογής Dropbox (μέσω του λειτουργικού συστήματος):

1. Διαγράφηκαν ορισμένοι από τους φακέλους και τα αρχεία που είχαν δημιουργηθεί κατά την εγκατάσταση του λογισμικού του Dropbox. Ωστόσο επισημαίνεται ότι με το λογισμικό Magnet Axiom κατέστη εφικτή η ανάκτηση των εν λόγω διαγεγραμμένων αρχείων.
2. Εντοπίστηκαν στοιχεία που καταδεικνύουν την απεγκατάσταση του λογισμικού του Dropbox. Τα στοιχεία αυτά σχετίζονται άμεσα με το λειτουργικό σύστημα Windows 10. Ειδικότερα, βρέθηκαν:
   - Αρχεία καταγραφής συμβάντων των Windows (Windows Event Logs),

- Εγγραφές στο μητρώο καταγραφής εκτελέσεων των προγραμμάτων (Amcache),
- Εγγραφές στο μητρώο καταγραφής των Windows (Windows Registry),
- Εγγραφές δραστηριότητας του λογισμικού του Dropbox (Prefetch Files), κ.ά.

Ενδεικτικά, παρουσιάζονται κάτωθι ορισμένα εκ των ανωτέρω ευρημάτων (βλ. Εικόνες 26-28).

3. Όσον αφορά τις βάσεις δεδομένων που περιλάμβαναν τα επίμαχα δεδομένα, επισημαίνεται ότι διαγράφηκαν όλες. Εδώ θα πρέπει να τονισθεί ότι, ακόμα και αν ανακτήθηκαν με το λογισμικό Magnet Axiom οι διαγεγραμμένες βάσεις δεδομένων, δεν κατέστη εφικτή η προβολή του περιεχομένου των περισσοτέρων εξ αυτών. Η μόνη βάση δεδομένων που ανακτήθηκε και κατέστη δυνατό να προβληθούν τα δεδομένα της (έπειτα από την αποκρυπτογράφηση τους) ήταν η «filecache.dbx».
4. Τέλος αναφέρεται ότι όλα τα αρχεία που είχαν συγχρονιστεί με την εφαρμογή Dropbox και βρίσκονταν στη διαδρομή C:\Users\<username>\Dropbox δεν διαγράφηκαν αλλά διατηρήθηκαν αναλλοίωτα ακόμα και έπειτα από τη διαγραφή του λογισμικού (κατά την απεγκατάσταση ο χρήστης ερωτάται αν προτιμά τη διαγραφή ή την παραμονή των αρχείων).

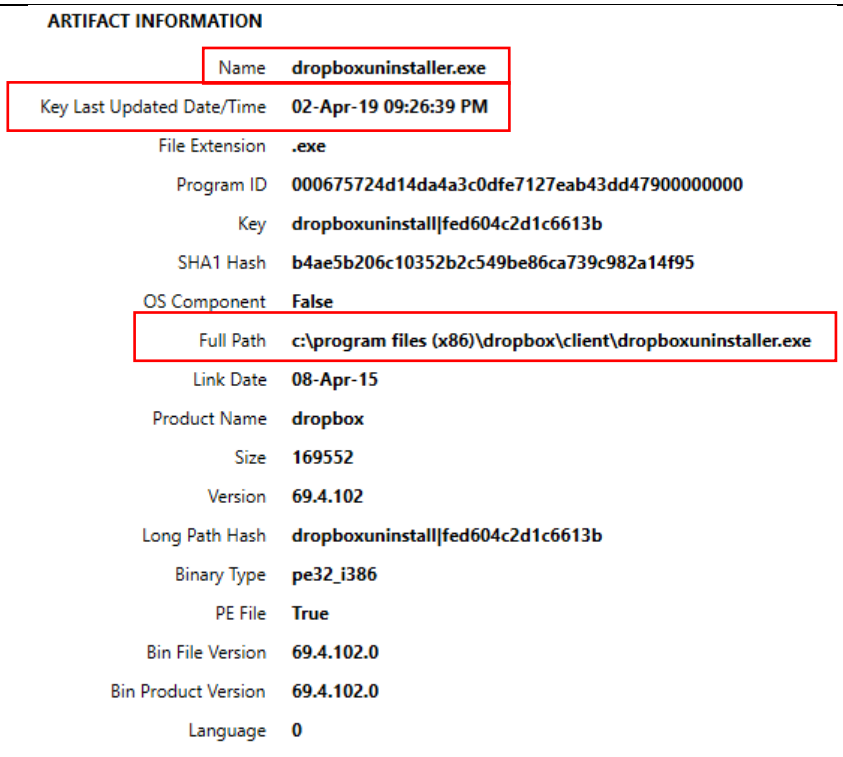


ARTIFACT INFORMATION

Event ID	**1034**
Security User ID	**S-1-5-21-167654484-677196580-2748798096-1001**
Created Date/Time	**02-Apr-19 09:28:06 PM**
Event Description Summary	**Windows Installer removed a product.**
Level	**Information**
Keywords	**0x0080000000000000**
Provider Name	**MsiInstaller**
Task Category	**0**
Computer	**DESKTOP-M9TVKRB**
Event Data	**<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">** **<System>** **<Provider Name="MsiInstaller" />** **<EventID Qualifiers="0">1034</EventID>** **<Level>4</Level>** **<Task>0</Task>** **<Keywords>0x0080000000000000</Keywords>** **<TimeCreated SystemTime="2019-04-02T21:28:06.7015437Z" />** **<EventRecordID>885</EventRecordID>** **<Channel>Application</Channel>** **<Computer>DESKTOP-M9TVKRB</Computer>** **<Security UserID="S-1-5-21-167654484-677196580-2748798096-1001" />** **</System>** **<EventData>** **<Data>Dropbox Update Helper1.3.189.110330Dropbox, Inc.(NULL)</Data>** **</Data>**

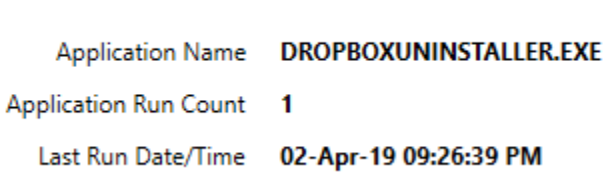
Εικόνα 26

Αρχείο καταγραφής συμβάντων των Windows (Windows Event Logs)
Διαδρομή Αρχείου: C:\Windows\System32\winevt\Logs\Application.evtx



Εικόνα 27

Εγγραφές στο μητρώο καταγραφής εκτελέσεων των προγραμμάτων (Am-cache)
Διαδρομή Αρχείου: C:\Windows\appcompat\Programs\Amcache.hve



Εικόνα 28

Αρχείο δραστηριότητας του λογισμικού του Dropbox (Prefetch Files),
Διαδρομή Αρχείου: C:\Windows\Prefetch\DROPBOXUNINSTALLER.EXE-2628D09B.pf

Έπειτα από την απεγκατάσταση της εφαρμογής Dropbox (μέσω του λογισμικού CCleaner) εντοπίστηκαν παρόμοια ευρήματα με τη διαφορά ότι για καμία από τις διαγεγραμμένες βάσεις δεδομένων που ανακτήθηκαν, δεν κατέστη εφικτή η προβολή των περιεχομένων τους.

Στη συνέχεια εξετάζονται οι φυλλομετρητές Ιστού, και το πώς η χρήση τους επηρεάζει την ύπαρξη ή μη αποδεικτικών στοιχείων, σχετικών με τη χρήση της υπηρεσίας νέφους Dropbox.

7.4. Χρήση των φυλλομετρητών Ιστού για πρόσβαση στην υπηρεσία Dropbox

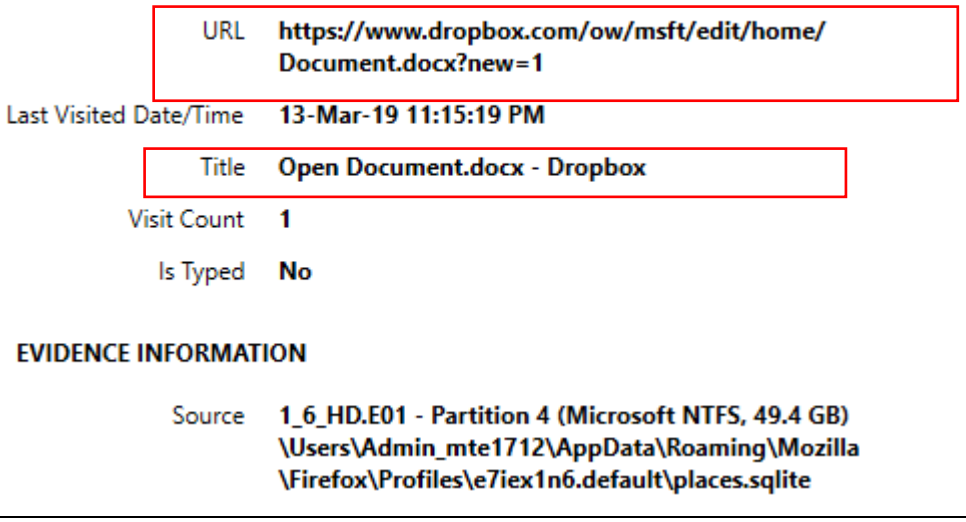
7.4.1. Εξέταση του Mozilla Firefox

Ο Mozilla Firefox είναι ένα από τους πιο δημοφιλής φυλλομετρητές Ιστού. Μαζί με τον φυλλομετρητή Google Chrome καταλαμβάνουν τις πρώτες θέσεις στις προτιμήσεις των χρηστών, στην πλατφόρμα υπολογιστή (StatCounter 2019).

Τα ευρήματα που αναμένεται να προκύψουν από την εξέταση των φυλλομετρητών Ιστού είναι λιγότερα από αυτά που εντοπίστηκαν κατά την εξέταση της εφαρμογής Dropbox. Αυτή η πεποίθηση οφείλεται αρχικώς στο ότι η εφαρμογή συγχρονίζει όλα τα αρχεία του λογαριασμού του χρήστη με τον υπολογιστή. Ακόμα και αν ο χρήστης δεν επιλέξει να προβάλει ή γενικά να αλληλοεπιδράσει με ορισμένα αρχεία του λογαριασμού του, αυτά θα βρίσκονται εκεί. Αντίθετα κατά τη χρήση ενός φυλλομετρητή Ιστού, ευρήματα μπορούν να προκύψουν μόνο για τα αρχεία με τα οποία ο χρήστης ασχολήθηκε. Επίσης, δεν υπάρχουν οι βάσεις δεδομένων της εφαρμογής, οι οποίες έφεραν αποθηκευμένες σημαντικές πληροφορίες για τη δραστηριότητα του χρήστη. Έτσι, ο ερευνητής περιορίζεται όσον αφορά τις πηγές αποδεικτικών στοιχείων που μπορεί να ερευνήσει.

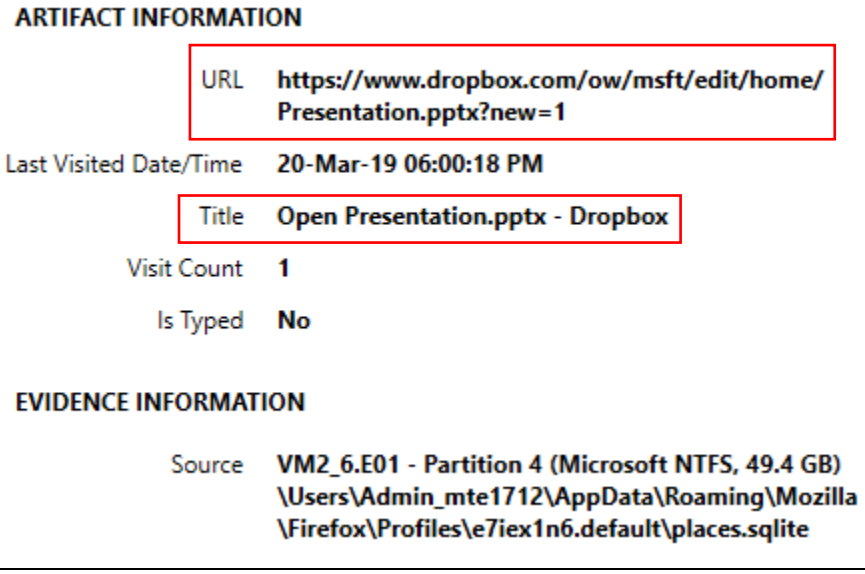
Έπειτα από τις ενέργειες που περιγράφονται στο Κεφάλαιο 6, πραγματοποιήθηκε δικανική εξέταση στα εγκληματολογικά αντίγραφα των εικονικών μηχανών, των φυλλομετρητών Ιστού. Τα ευρήματα που εντοπίστηκαν, βοήθησαν στην εξακρίβωση ορισμένων ενεργειών που πραγματοποίησε ο χρήστης, χρησιμοποιώντας την υπηρεσία Dropbox. Στη συνέχεια παρουσιάζονται (βλ. Εικόνες 29-34) τα στοιχεία που εντοπίστηκαν και μπορούν να αποδοθούν σε μία συγκεκριμένη ενέργεια του χρήστη:

1. **Δημιουργία νέων αρχείων μέσω του φυλλομετρητή Ιστού**
   - Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στη δημιουργία νέων αρχείων στο νέφος του χρήστη (βλ. Εικόνες 29 και 30).



Εικόνα 29

Δημιουργία νέου αρχείου κειμένου μέσω φυλλομετρητή Ιστού, στην υπηρεσία Dropbox
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Roaming\Mozilla\Firefox
\Profiles\e7iex1n6.default\places.sqlite



Εικόνα 30

Δημιουργία νέου αρχείου παρουσίασης μέσω φυλλομετρητή Ιστού, στην υπηρεσία Dropbox
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Roaming
Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite

2. Μεταφόρτωση (download) αρχείων μέσω του φυλλομετρητή Ιστού

- Εντοπίστηκαν στη κρυφή μνήμη (cache) του φυλλομετρητή Ιστού, εγγραφές οι οποίες μπορούν να αποδοθούν στη μεταφόρτωση (download) αρχείων από το νέφος του χρήστη (βλ. Εικόνες 31 και 32).

ARTIFACT INFORMATION

URL **https://www.dropbox.com/pri/get/000030.xls?_download_id=85614956130778336349168395864205981072231195113182463334397614098_notify_domain=www.dropbox.com&_subject_uid=2025775424&revision_id=BP5CXQNlugrkgoaosgl38iBjl_mINEYn8936PsLU6htXX8grqAMPppq34aaRrrpnF_K8I25k3JnytoSNjZ9b2fI8beVR1gCjxBCxgEULuM_B0uLMB5KaLSpj946dw2kcP6g&source=_private_jsinfo_helper&w=AAD6X9Ged4I2TRAe-RLnqnBfP-LhFO3ooiEK7VSoy6R2iw**

EVIDENCE INFORMATION

Source **VM2_6.E01 - Partition 4 (Microsoft NTFS, 49.4 GB)\Users\Admin_mte1712\AppData\Local\Mozilla\Firefox\Profiles\e7iex1n6.default\cache2\entries\F407FD84C1761547C7DC4618884519E26917B8FB**

Εικόνα 31

Μεταφόρτωση αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite

ARTIFACT INFORMATION

URL **https://www.dropbox.com/pri/get/000968.jpeg?_download_id=1903172158815531530459171868332914980610416196207663058444019335&_notify_domain=www.dropbox.com&_subject_uid=2025775424&revision_id=BP6eRlgUeha-2rQ6c6SeZtCSIKX6hbBfleUfelmXbUDU5DluAbcle6PV8t4ihdUI7IBiTXcgH5z8Y3WAzjW5n9hHt_9li1NXIPCNzWCpA2rJPu5NFn7QiOjeYm_cHg43IVI&source=_private_jsinfo_helper&w=AACUK1IhNFmTAYjxg-GfPPgdGpsAy_9KpgGO1R5QNwTi_g**

EVIDENCE INFORMATION

Source **VM2_6.E01 - Partition 4 (Microsoft NTFS, 49.4 GB)\Users\Admin_mte1712\AppData\Local\Mozilla\Firefox\Profiles\e7iex1n6.default\cache2\entries\6D86607B222A320945E555721FB165BC14546035**

Εικόνα 32

Μεταφόρτωση αρχείου εικόνας μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Mozilla\ Firefox\Profiles\ e7iex1n6.default\cache2\entries\6D86607B222A320945E555721FB165BC14546035

3. Προβολή αρχείων μέσω του φυλλομετρητή Ιστού

- Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στην προβολή αρχείων που υπάρχουν αποθηκευμένα στο νέφος του χρήστη (βλ. Εικόνες 33 και 34).

ARTIFACT INFORMATION

URL	**https://www.dropbox.com/home?preview=000081.txt**
Last Visited Date/Time	**14/03/19 01:20:46**
Title	**000081.txt**
Visit Count	**1**
Is Typed	**No**

EVIDENCE INFORMATION

Source	**1_6_HD.E01 - Partition 4 (Microsoft NTFS, 49.4 GB)\Users\Admin_mte1712 \AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite**

Εικόνα 33

Προβολή αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox
Διαδρομή Αρχείου: C:\Users\<username>\AppData\ \Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite

ARTIFACT INFORMATION

URL	**https://www.dropbox.com/home?preview=000009.pdf**
Last Visited Date/Time	**14/03/19 01:19:54**
Title	**000009.pdf**
Visit Count	**1**
Is Typed	**No**

EVIDENCE INFORMATION

Source	**1_6_HD.E01 - Partition 4 (Microsoft NTFS, 49.4 GB)\Users\Admin_mte1712 \AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite**

Εικόνα 34

Προβολή αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox
Διαδρομή Αρχείου: C:\Users\<username>\AppData
\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite

Ωστόσο η δραστηριότητα που αναλύεται ανωτέρω, δεν έχει διαπιστωθεί μέχρι στιγμής, σε ποιον λογαριασμό ανήκει. Αυτό εξακριβώθηκε κατά την εξέταση της μνήμης RAM. Εκεί εντοπίστηκαν τα δεδομένα που έστειλε ο φυλλομετρητής Ιστού στον εξυπηρετητή της υπηρεσίας Dropbox (μέσω ενός cookie). Μεταξύ των δεδομένων αυτών βρίσκεται τόσο η διεύθυνση ηλεκτρονικού ταχυδρομείου του λογαριασμού στον οποίο ανήκει η προαναφερθείσα δραστηριότητα, όσο και ο κωδικός πρόσβασης σε αυτόν (σε απλό κείμενο). Στην εικόνα που ακολουθεί (βλ. Εικόνα 35), προβάλλονται τα εν λόγω ευρήματα της μνήμης RAM.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
08589B480	00	00	00	00	00	00	00	00	04	00	00	00	50	4F	53	54	POST
08589B490	01	00	00	00	01	00	00	00	01	00	00	00	00	00	00	00	
08589B4A0	FE	03	00	00	69	73	5F	78	68	72	3D	74	72	75	65	26	þ is_xhr=true&
08589B4B0	74	3D	61	42	55	53	4D	4B	4A	4B	6B	74	4E	47	78	36	t=aBUSMKJKktNGx6
08589B4C0	51	70	72	37	6B	37	37	61	45	5A	26	66	6E	61	6D	65	Qpr7k77aEZ&fname
08589B4D0	3D	6D	74	65	31	37	31	32	26	6C	6E	61	6D	65	3D	44	=mte1712&lname=D
08589B4E0	72	6F	70	62	6F	78	26	65	6D	61	69	6C	3D	6D	74	65	ropbox&email=mte
08589B4F0	31	37	31	32	5F	64	72	6F	70	62	6F	78	25	34	30	6F	1712_dropbox%40o
08589B500	75	74	6C	6F	6F	6B	2E	63	6F	6D	2E	67	72	26	70	61	utlook.com.gr&pa
08589B510	73	73	77	6F	72	64	3D	4D	46	4B	6F	64	69	6B	6F	73	ssword=[redacted]
08589B520	50	72	6F	73	76	61	73	69	73	26	74	6F	73	5F	61	67	[redacted]&tos_ag
08589B530	72	65	65	3D	74	72	75	65	26	67	2D	72	65	63	61	70	ree=true&g-recap
08589B540	74	63	68	61	2D	72	65	73	70	6F	6E	73	65	2D	76	33	tcha-response-v3
08589B550	3D	30	33	41	4F	4C	54	42	4C	51	36	36	64	50	6A	6B	=03AOLTBLQ66dPjk
08589B560	33	4D	70	42	75	32	67	35	56	33	30	4C	49	4B	36	6E	3MpBu2g5V30LIK6n
08589B570	67	44	46	59	54	5F	73	6D	78	4B	2D	6D	64	6B	70	43	gDFYT_smxK-mdkpC
08589B580	75	39	32	49	6B	6F	2D	46	52	4A	74	39	74	6E	33	66	u92Iko-FRJt9tn3f
08589B590	69	5F	4B	67	47	59	61	37	73	5A	58	5F	69	4E	78	77	i_KgGYa7sZX_iNxw
08589B5A0	63	2D	37	51	51	34	59	32	55	37	77	55	45	31	46	67	c-7QQ4Y2U7wUE1Fg

Εικόνα 35

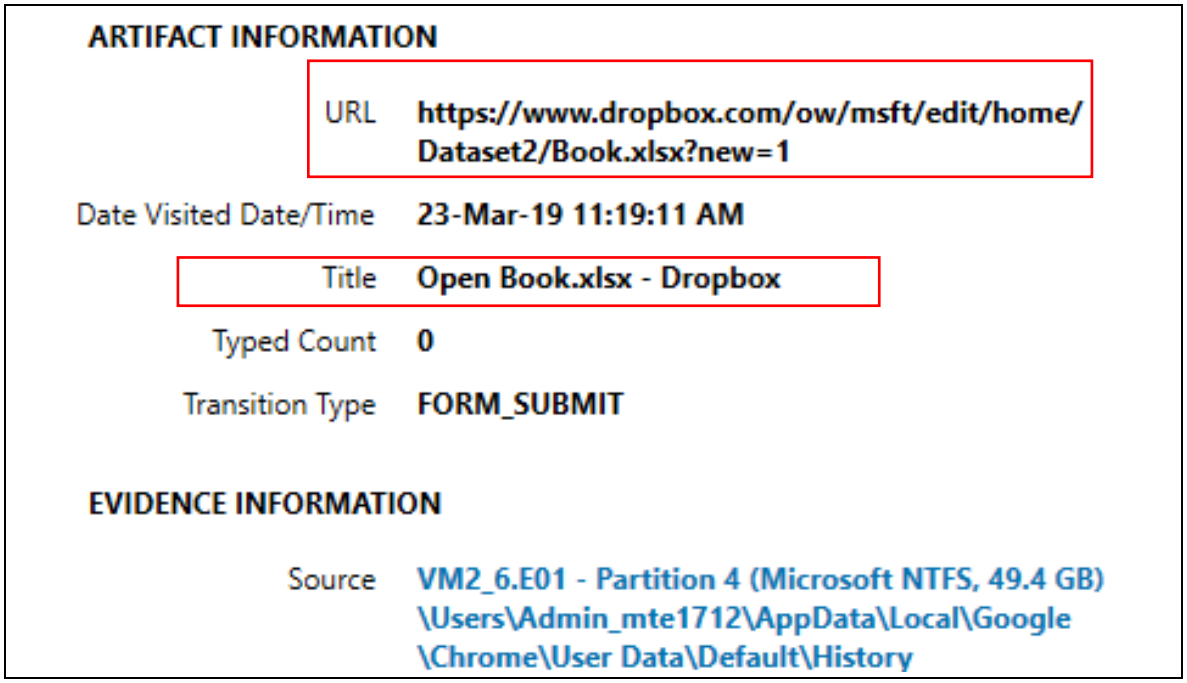
Στοιχεία εισόδου στον λογαριασμό του χρήστη στο Dropbox

Υπάρχει η πιθανότητα να βρεθούν αποθηκευμένα τα στοιχεία εισόδου του χρήστη και στις βάσεις δεδομένων του φυλλομετρητή Ιστού, ωστόσο σε αυτά τα σενάρια δεν επιλέχθηκε από τον χρήστη η αποθήκευση τους. Ακολουθεί η εξέταση του φυλλομετρητή Ιστού Google Chrome.

7.4.2. Εξέταση του Google Chrome

Όπως και με τον Mozilla Firefox, έτσι και με τον Google Chrome, τα ευρήματα που δύναται να εντοπιστούν, σχετίζονται άμεσα με τη δραστηριότητα που πραγματοποίησε ο χρήστης μέσω αυτού. Στην προκειμένη περίπτωση, κατά την εξέταση των δεδομένων του φυλλομετρητή Google Chrome, εντοπίστηκαν αποδεικτικά στοιχεία, τα οποία βοήθησαν στην εξακρίβωση ορισμένων ενεργειών που πραγματοποίησε ο χρήστης, χρησιμοποιώντας την υπηρεσία Dropbox. Στη συνέχεια προβάλλονται (βλ. Εικόνες 36-41) τα δεδομένα που βρέθηκαν και μπορούν να αποδοθούν σε μία συγκεκριμένη ενέργεια του χρήστη:

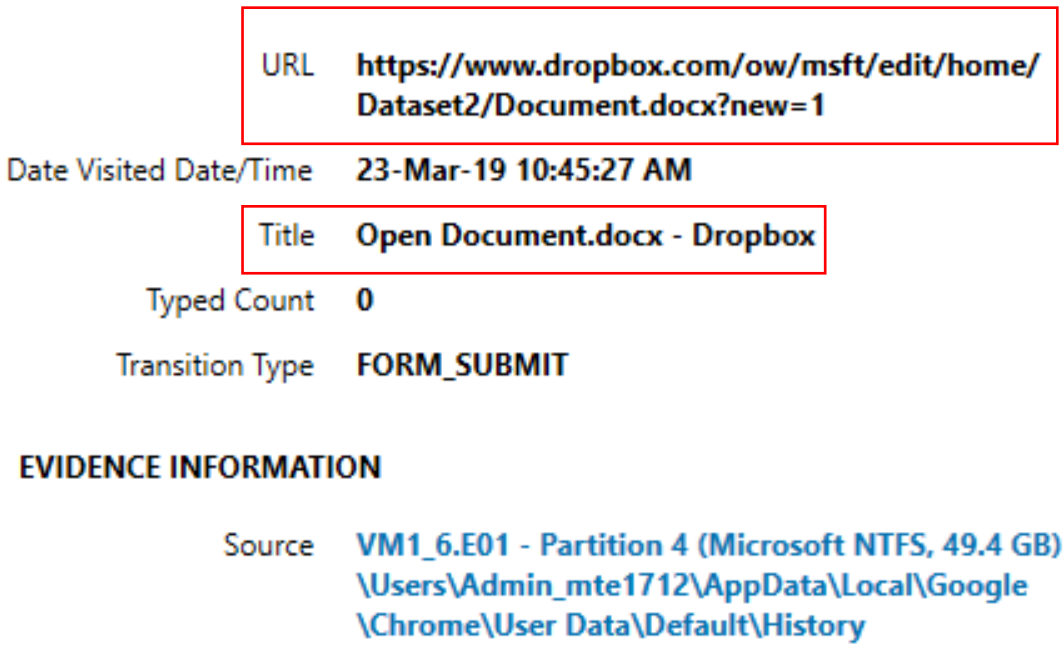
1. **Δημιουργία νέων αρχείων μέσω του φυλλομετρητή Ιστού**
   - Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στη δημιουργία νέων αρχείων στο νέφος του χρήστη (βλ. Εικόνες 36 και 37).



Εικόνα 36

Δημιουργία νέου αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, στην υπηρεσία Dropbox

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History



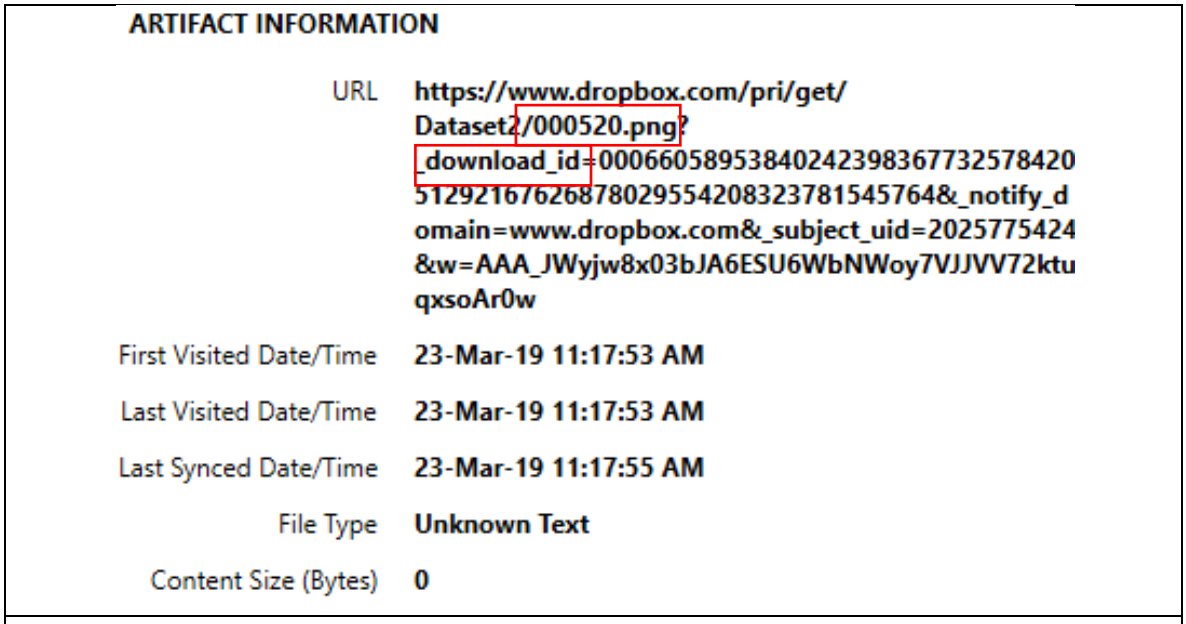
Εικόνα 37

Δημιουργία νέου αρχείου κειμένου μέσω φυλλομετρητή Ιστού, στην υπηρεσία Dropbox

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

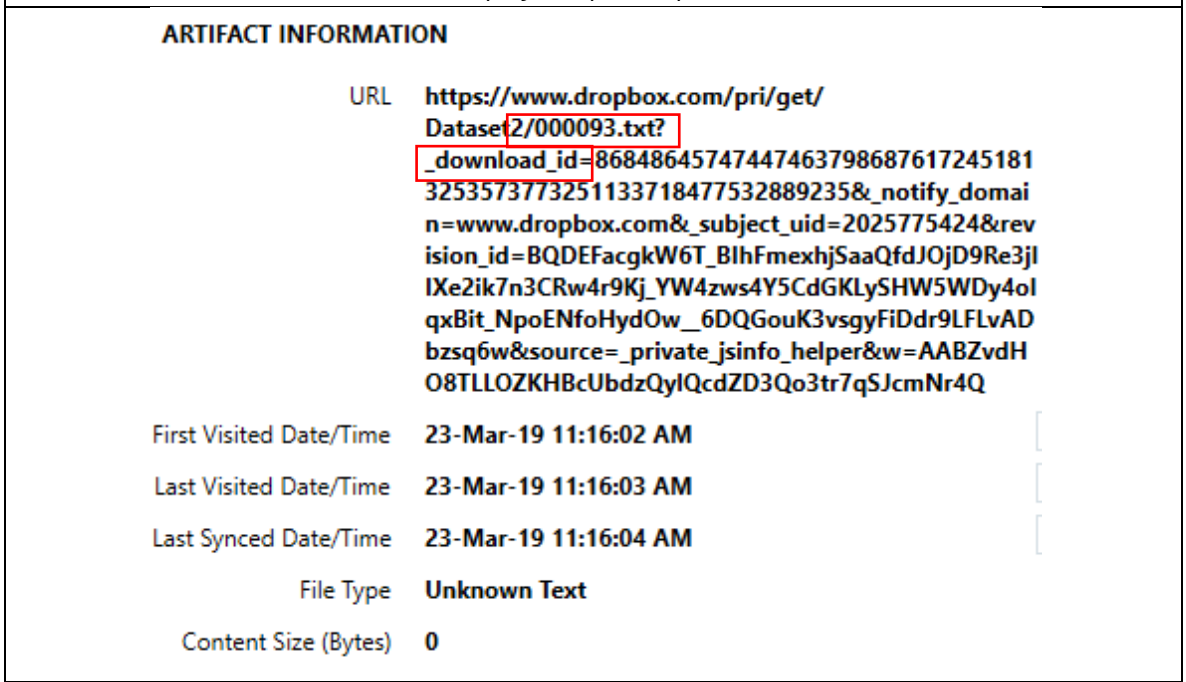
2. Μεταφόρτωση (download) αρχείων μέσω του φυλλομετρητή Ιστού

- Εντοπίστηκαν στη κρυφή μνήμη (cache) του φυλλομετρητή Ιστού, εγγραφές οι οποίες μπορούν να αποδοθούν στη μεταφόρτωση (download) αρχείων από το νέφος του χρήστη (βλ. Εικόνες 38 και 39).



Εικόνα 38

Μεταφόρτωση αρχείου εικόνας μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox Διαδρομή Αρχείου: C:\Users\<username>\ AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

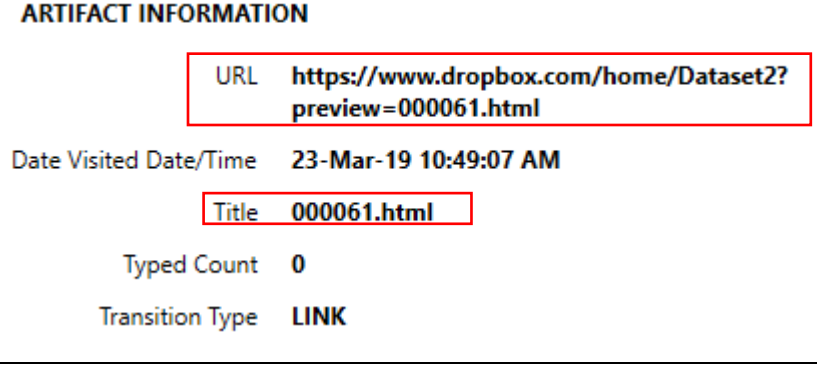


Εικόνα 39

Μεταφόρτωση αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox Διαδρομή Αρχείου: C:\Users\<username>\ AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

3. Προβολή αρχείων μέσω του φυλλομετρητή Ιστού

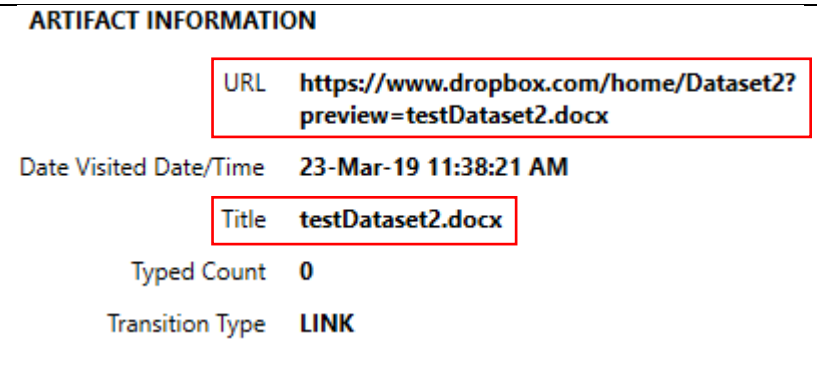
- Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στην προβολή αρχείων που υπάρχουν αποθηκευμένα στο νέφος του χρήστη (βλ. Εικόνες 40 και 41).



Εικόνα 40

Προβολή αρχείου υπερκειμένου (.html) μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History



Εικόνα 41

Προβολή αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Dropbox

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

Σε αυτόν τον φυλλομετρητή δεν εντοπίστηκαν ευρήματα στο αντίγραφο της μνήμης RAM. Και εδώ υπάρχει η πιθανότητα να βρεθούν αποθηκευμένα τα στοιχεία εισόδου του χρήστη, στις βάσεις δεδομένων του φυλλομετρητή Ιστού, ωστόσο σε αυτά τα σενάρια δεν επιλέχθηκε από τον χρήστη η αποθήκευση τους.

7.5. Εξέταση των μεταδεδομένων των αρχείων

Πριν τη μεταφόρτωση (upload) των αρχείων στο νέφος, καταγράφηκαν οι αλφαριθμητικές ταυτότητες μοναδικότητας (MD5) τους, προκειμένου να απαντηθεί η δεύτερη ερευνητική ερώτηση. Όπως επισημάνθηκε και στο Κεφάλαιο 6, το αντικείμενο μελέτης σε αυτό το υποκεφάλαιο αποτελούν όσα αρχεία δεν τέθηκαν υπό επεξεργασία (πάσης φύσεως επεξεργασία, π.χ. μετονομασία, περικοπή, διαγραφή, κ.ά.) από τον χρήστη, για το διάστημα που αυτά παρέμειναν στο νέφος. Τα αρχεία αυτά στη συνέχεια μεταφορτώθηκαν (download) από το νέφος και έγινε η σύγκριση των τεχνικών χαρακτηριστικών τους με αυτά των αρχικών αρχείων. Κάτωθι παρουσιάζονται σε 2 πίνακες τα τεχνικά χαρακτηριστικά των αρχείων πριν «ανέβουν» στο νέφος (βλ. Πίνακας 9) και αφότου «κατέβηκαν» από αυτό (βλ. Πίνακας 10).

Όνομα αρχείου	**Ημερομηνία Δημιουργίας (File Created)**	**Ημερομηνία Τελευταίας Προσπέλασης (Last Accessed)**	**Ημερομηνία Τελευταίας Τροποποίησης (Last Modified)**	**MD5**
000884.jpeg	13-Mar-19 00:16:05	13-Mar-19 00:17:26	27-Apr-05 14:30:46	4056fef8a39b35cd6c65177ca7f3afec
000883.jpeg	13-Mar-19 00:16:05	13-Mar-19 00:17:26	02-Sep-05 09:36:58	87d2f8d38aabbf7ff8e58b915243b576
000030.xls	13-Mar-19 00:16:01	13-Mar-19 00:18:58	20-Jan-04 10:59:24	d7a93125e7c02c80b83ef110db39c6dc
000140.pdf	13-Mar-19 00:16:02	13-Mar-19 00:18:33	17-Apr-08 12:53:56	01c93f6449bab1d2a2ca9c9b9c09009b
000081.txt	13-Mar-19 00:16:01	13-Mar-19 00:18:35	05-Feb-09 17:12:54	6b116ec9cb7ee877c159aa512d09bac2
000001.doc	13-Mar-19 00:16:00	13-Mar-19 00:19:01	05-Feb-09 17:12:26	baf525bef9a80cd6aa0743e5720eb0fd
000176.pdf	13-Mar-19 00:16:02	13-Mar-19 00:18:22	11-Feb-08 08:45:00	5772a0192e77531fa281ea7283b4a5bf
000093.txt	13-Mar-19 00:16:01	13-Mar-19 00:18:35	26-Jul-06 09:18:38	3a2b3579acd4f465d5f9272ff8aedba7

Πίνακας 9

Τεχνικά χαρακτηριστικά των αρχείων πριν «ανέβουν» στο νέφος

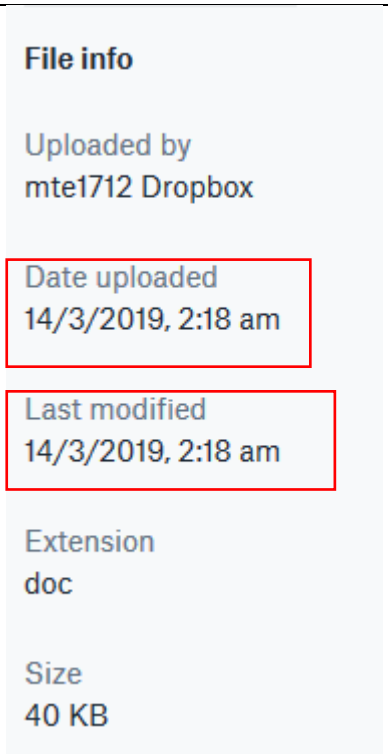
Όνομα αρχείου	Ημερομηνία Δημιουργίας (File Created)	Ημερομηνία Τελευταίας Προσπέλασης (Last Accessed)	Ημερομηνία Τελευταίας Τροποποίησης (Last Modified)	MD5
000884.jpeg	01-Apr-19 21:19:57	01-Apr-19 21:19:57	01-Apr-19 21:19:57	4056fef8a39b35cd6c65177ca7f3afec
000883.jpeg	01-Apr-19 21:19:11	01-Apr-19 21:19:11	01-Apr-19 21:19:11	87d2f8d38aabbf7ff8e58b915243b576
000030.xls	01-Apr-19 21:20:21	01-Apr-19 21:20:21	01-Apr-19 21:20:22	d7a93125e7c02c80b83ef110db39c6dc
000140.pdf	01-Apr-19 21:20:33	01-Apr-19 21:20:33	01-Apr-19 21:20:33	01c93f6449bab1d2a2ca9c9b9c09009b
000081.txt	20/03/19 19:51:50	20/03/19 19:51:50	20/03/19 19:51:53	6b116ec9cb7ee877c159aa512d09bac2
000001.doc	20/03/19 19:52:46	20/03/19 19:52:46	20/03/19 19:52:47	baf525bef9a80cd6aa0743e5720eb0fd
000176.pdf	23-Mar-19 11:15:05	23-Mar-19 11:15:05	23-Mar-19 11:15:06	5772a0192e77531fa281ea7283b4a5bf
000093.txt	23-Mar-19 11:16:03	23-Mar-19 11:16:03	23-Mar-19 11:16:04	3a2b3579acd4f465d5f9272ff8aedba7
000113.doc	23-Mar-19 11:16:37	23-Mar-19 11:16:37	23-Mar-19 11:16:41	38d36f9721cda07b1f55911c894d59bd

Πίνακας 10

Τεχνικά χαρακτηριστικά των αρχείων αφού «κατέβουν» από το νέφος

Συγκρίνοντας τους 2 πίνακες, παρατηρείται ότι οι αλφαριθμητικές ταυτότητες μοναδικότητας (MD5) των αρχείων παραμένουν ίδιες. Επομένως, μπορεί να εξαχθεί με ασφάλεια το συμπέρασμα ότι η μεταφόρτωση (download/upload) αρχείων στο νέφος, δεν τις επηρεάζει.

Από την άλλη μεριά, η μεταφόρτωση (download/upload) αρχείων από και προς το νέφος, επηρεάζει τις χρονοσφραγίδες των εν λόγω αρχείων. Ειδικότερα, οι χρονοσφραγίδες των αρχείων μεταβάλλονται δύο φορές. Η μία φορά είναι όταν από τη συσκευή του χρήστη «ανέβουν» και αποθηκευτούν στο νέφος, Και η άλλη φορά είναι όταν «κατέβουν» από το νέφος στη συσκευή του χρήστη. Για παράδειγμα, το αρχείο με ονομασία «000001.doc» πριν «ανέβει» στο νέφος, φέρει τις χρονοσφραγίδες του Πίνακα 9. Όταν «ανέβηκε» στο νέφος, οι χρονοσφραγίδες τους μεταβλήθηκαν όπως φαίνονται στη κάτωθι εικόνα (βλ. Εικόνα 42). Και όταν το αρχείο αυτό, «κατέβηκε» από το νέφος, οι χρονοσφραγίδες τους μεταβλήθηκαν εκ νέου, όπως φαίνεται στον Πίνακα 10.



Εικόνα 42
Προβολή των χρονοσφραγίδων του αρχείου «000001.doc», όσο βρίσκεται αποθηκευμένο στο νέφος της υπηρεσίας Dropbox

Τέλος αναφέρεται ότι το περιεχόμενο των εν λόγω αρχείων δεν αλλοιώθηκε κατά την μεταφόρτωση (download/upload) τους από και προς το νέφος. Στο επόμενο υποκεφάλαιο γίνεται μία συγκέντρωση των αποτελεσμάτων της δικανικής εξέτασης της υπηρεσίας νέφους Dropbox.

7.6. Σύνοψη δικανικής εξέτασης

Στο κεφάλαιο 7 πραγματοποιήθηκε εγκληματολογική εξέταση της υπηρεσίας νέφους Dropbox. Πιο συγκεκριμένα, εξετάστηκαν 18 εγκληματολογικά αντίγραφα, προερχόμενα από 9 εικονικές μηχανές που χρησιμοποιούσαν τις υπηρεσίες του Dropbox, είτε μέσω της εφαρμογής που προσφέρει στο λειτουργικό σύστημα Windows 10, είτε μέσω των δημοφιλέστερων φυλλομετρητών Ιστού για υπολογιστές (Google Chrome, Mozilla Firefox).

Ο σκοπός της εξέτασης ήταν ο εντοπισμός ευρημάτων που να αποδεικνύουν αφενός τη χρήση των υπηρεσιών νέφους και αφετέρου να προσδιορίζουν τη δραστηριότητα που πραγματοποίησε ο χρήστης μέσω αυτών. Επίσης, εξετάστηκε κατά πόσο επηρεάζει τα τεχνικά χαρακτηριστικά ενός αρχείου, η μεταφόρτωση του στο Dropbox.

Τα αποτελέσματα της δικανικής εξέτασης ήταν αρκετά ενθαρρυντικά. Εντοπίστηκαν αρκετά δεδομένα που να καταδεικνύουν τη χρήση του Dropbox αλλά και τις ενέργειες που πραγματοποίησε ο χρήστης μέσω αυτού. Συνολικά τα ευρήματα που προέκυψαν από τη δικανική εξέταση του Dropbox, παρουσιάζονται στο Παράρτημα Α. Στο επόμενο κεφάλαιο, θα ακολουθήσει μία παρόμοια εγκληματολογική εξέταση, αλλά αυτή τη φορά στην υπηρεσία νέφους Google Drive.

Κεφάλαιο 8ο: Εγκληματολογική εξέταση της υπηρεσίας νέφους Google Drive σε περιβάλλον Windows 10

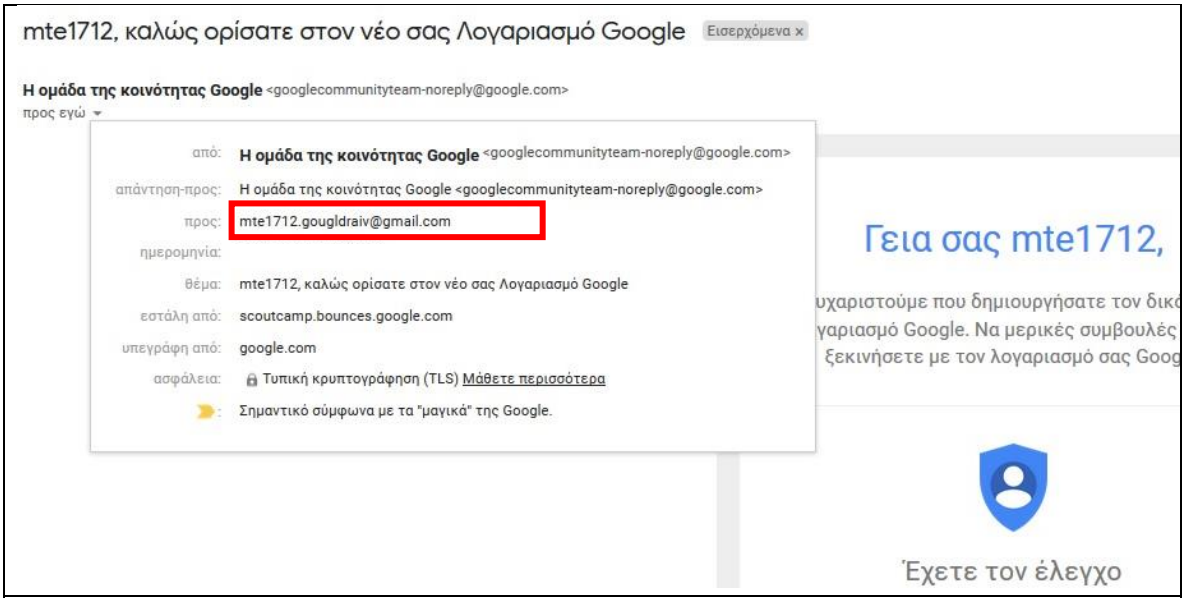
8.1. Γενικά

Το Google Drive (GoogleDrive 2019) είναι μία υπηρεσία της εταιρείας Google που προσφέρει υπηρεσίες νέφους. Ειδικότερα η εν λόγω υπηρεσία παρέχει τη δυνατότητα αποθήκευσης δεδομένων στο νέφος, καθώς και τη δυνατότητα για συγχρονισμό και κοινή χρήση των αποθηκευμένων δεδομένων μεταξύ των διαφορετικών συσκευών που ο χρήστης έχει συνδέσει στον λογαριασμό του. Η εταιρεία Google προσφέρει και άλλες υπηρεσίες που στηρίζονται στο νέφος, όπως η υπηρεσία Google Docs, η οποία προσφέρει τη δυνατότητα δημιουργίας αρχείων (κειμένου, λογιστικών φύλλων, κ.ά.) που μπορούν να επεξεργάζονται ταυτόχρονα από πολλούς διαφορετικούς χρήστες, η υπηρεσία Google Photos για διαχείριση φωτογραφιών, κ.ά.. Το Google Drive ως υπηρεσία υποστηρίζεται από όλες τις γνωστές πλατφόρμες (Windows, Android, OS X, iOS, κ.ά.).

Το Google Drive διατίθεται σε δωρεάν έκδοση η οποία προσφέρει μέχρι 15GB αποθηκευτικό χώρο, μαζί με τη δυνατότητα πρόσβασης και χρήσης σε άλλες υπηρεσίες της εταιρείας Google. Διατίθεται φυσικά και σε επί πληρωμή έκδοση, η οποία δεν έχει περιορισμούς στη χρήση. Η εφαρμογή της Google Drive που αντιστοιχεί σε αυτές τις εκδόσεις, ονομάζεται Backup and Sync from Google. Τέλος, παρέχεται και σε ειδική έκδοση για επαγγελματική χρήση, η οποία προσφέρει επιπρόσθετες δυνατότητες. Η εφαρμογή της Google Drive που αντιστοιχεί σε αυτή την έκδοση ονομάζεται Drive File Stream.

Για να χρησιμοποιήσει κάποιος την υπηρεσία Google Drive, πρέπει να εγγραφεί σε αυτήν. Για την εγγραφή χρειάζεται έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου της υπηρεσίας Gmail (της εταιρείας Google) και ορισμένες επιπλέον πληροφορίες από τον χρήστη (π.χ. κωδικό πρόσβασης).

Στα πλαίσια της διπλωματικής εργασίας δημιουργήθηκε μία νέα διεύθυνση ηλεκτρονικού ταχυδρομείου (βλ. Εικόνα 43) η οποία και χρησιμοποιήθηκε για τη χρήση της ανωτέρω υπηρεσίας νέφους. Επιπρόσθετα, χρησιμοποιήθηκαν δύο διευθύνσεις ηλεκτρονικού ταχυδρομείου, οι οποίες αξιοποιήθηκαν ειδικά στα σενάρια διαμοιρασμού αρχείων μέσω της υπηρεσίας νέφους (mte1712_ShareItWithMe@outlook .com.gr και mte1712_ShareItWithMe2@gmail.com).



Εικόνα 43

Δημιουργία λογαριασμού στην υπηρεσία νέφους Google Drive στα πλαίσια της πειραματικής διαδικασίας

Όπως και με το Dropbox προηγουμένως, ο σκοπός της εξέτασης του Google Drive είναι να εντοπιστούν ευρήματα που να σχετίζονται με τη χρήση της εν λόγω υπηρεσίας, όπως παραδείγματος χάρη, το όνομα του χρήστη, η διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί, τα αρχεία που έχουν μεταφορτωθεί μέσω αυτής, κ.ά. Τα ευρήματα αυτά εξυπηρετούν στην απάντηση των ερευνητικών ερωτημάτων της παρούσας διπλωματικής. Η εξέταση του Google Drive βασίστηκε στην υπάρχουσα βιβλιογραφία (Chang 2016, Epifani 2013, Federici 2014, Quick and Choo 2014, Rathod 2017, Skulkin and Mikhaylov 2018), πλην όμως διαφοροποιείται ελαφρώς από αυτή, καθώς επικεντρώνεται στα δεδομένα που εντοπίζονται στο λειτουργικό σύστημα Windows 10 .

8.2. Προετοιμασία της εξέτασης

Αναφέρεται ότι στα πλαίσια της έρευνας δημιουργήθηκε δραστηριότητα (σε εννέα (9) εικονικές μηχανές) που αφορά σε μεταφορτώση (download/upload), προσπέλαση, επεξεργασία, δημιουργία, διαγραφή και διαμοιρασμό διαφόρων αρχείων (βλ. Κεφ. 6 για λεπτομέρειες) με χρήση της υπηρεσίας νέφους Google Drive. Κατόπιν συλλέχθηκαν εγκληματολογικά αντίγραφα των εν λόγω εικονικών μηχανών, τα οποία εξετάστηκαν προκειμένου να εντοπιστούν ίχνη της σχηματισθείσας δραστηριότητας. Στα υποκεφάλαια που ακολουθούν παρουσιάζονται αναλυτικά όλα τα ευρήματα που

προέκυψαν από την εγκληματολογική εξέταση του Google Drive και τα οποία σχετίζονται με τα ανωτέρω ερευνητικά ερωτήματα.

Γίνεται μνεία ότι, τα προγράμματα (και οι εκδόσεις τους) που χρησιμοποιήθηκαν για τη δημιουργία της δραστηριότητας στις εικονικές μηχανές, καθώς και για την εξέταση των αντιγράφων, αναφέρονται κάτωθι:

- Microsoft Windows 10 Pro 10.0.16299 N/A Build 16299,
- Mozilla Firefox 65.0.2 (64-Bit),
- Google Chrome 72.0.3626.121 (Official Build) (64-bit),
- Backup and Sync from Google (Google Drive) Client Application 3.43.2448.9071,
- CCleaner 5.55.7108 (64-Bit),
- DB Browser for SQLite 3.11.2,
- Magnet Axiom Process/Examine 3.0.0.13714,
- Winhex 19.6 και
- AccessData FTK Imager 3.4.3.3

8.3. Χρήση του λογισμικού της υπηρεσίας Google Drive

8.3.1. Γενική επισκόπηση των ευρημάτων που προέκυψαν

Έπειτα από την εγκατάσταση της εφαρμογής Backup and Sync from Google της Google Drive (χρησιμοποιώντας τις εξ ορισμού ρυθμίσεις), δημιουργήθηκαν οι φάκελοι που περιγράφονται κάτωθι (βλ. Πίνακας 11).

Διαδρομή και όνομα φακέλου	**Περιγραφή**
C:\Program Files\Google**Drive**	Αποτελεί τον φάκελο εγκατάστασης του λογισμικού. Περιλαμβάνει μεταξύ άλλων, το εκτελέσιμο αρχείο του λογισμικού.
C:\Program Files (x86)\Google\ **Drive**	Περιέχει πληροφορίες σχετικές με τις αναβαθμίσεις του εν λόγω λογισμικού.
C:\Users\<username>**Google-Drive**	Αποτελεί τον φάκελο που εξ ορισμού χρησιμοποιείται για τον συγχρονισμό των αρχείων του χρήστη. Περιλαμβάνει όλα τα αρχεία του χρήστη που έχουν συγχρονιστεί με τον λογαριασμό του στο νέφος. Ο χρήστης για να ανεβάσει τυχόν νέα αρχεία στο λογαριασμό του στο νέφος, το μόνο που έχει να κάνει είναι να μεταφέρει τα επιθυμητά αρχεία σε αυτόν τον φάκελο.

C:\Users\<username>\AppData\Local\Google**Drive**	Περιλαμβάνει όλα τα αρχεία του λογισμικού που σχετίζονται αφενός με διάφορες ρυθμίσεις του λογισμικού και αφετέρου με τη δραστηριότητα του συγκεκριμένου χρήστη.

Πίνακας 11

Φάκελοι που δημιουργούνται έπειτα από την εγκατάσταση του λογισμικού (Backup and Sync from Google) της υπηρεσίας νέφους Google Drive

Επιπρόσθετα εντοπίστηκαν αρκετά στοιχεία που καταδεικνύουν τόσο την εγκατάσταση όσο και την εκτέλεση του λογισμικού Google Drive. Τα στοιχεία αυτά σχετίζονται άμεσα με το λειτουργικό σύστημα Windows 10. Ειδικότερα, βρέθηκαν:

- Αρχεία καταγραφής συμβάντων των Windows (Windows Event Logs),
- Αρχεία συντομεύσεων (.LNK files),
- Εγγραφές στο μητρώο καταγραφής των Windows (Windows Registry),
- Εγγραφές δραστηριότητας του λογισμικού του Dropbox (Prefetch Files), κ.ά.

Ενδεικτικά, παρουσιάζονται κάτωθι ορισμένα εκ των ανωτέρω ευρημάτων (βλ. Εικόνες 44-46).

ARTIFACT INFORMATION

Linked Path	**C:\Program Files\Google\Drive\googledrivesync.exe**
Created Date/Time	**04-Apr-19 11:18:11 PM**
Last Modified Date/Time	**04-Apr-19 11:18:11 PM**
Last Accessed Date/Time	**04-Apr-19 11:18:11 PM**
Target File Created Date/Time	**07-Dec-18 02:37:32 AM**
Target File Last Modified Date/Time	**07-Dec-18 02:37:32 AM**
Target File Last Accessed Date/Time	**04-Apr-19 11:18:10 PM**
Target Attributes	**FILE_ATTRIBUTE_ARCHIVE**
Drive Type	**DRIVE_FIXED**
Volume Serial Number	**70A0026E**
Show Command	**SW_SHOWNORMAL**
Net Bios Name	**desktop-m9tvkrb**
Mac Address	**00:0C:29:14:2A:98**
Target File Size (Bytes)	**46504696**

Εικόνα 44

Αρχείο συντόμευσης (.LNK files)

Διαδρομή Αρχείου: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Backup and Sync from Google\Backup and Sync from Google.lnk

ARTIFACT INFORMATION

Event ID	**1033**
Security User ID	**S-1-5-21-167654484-677196580-2748798096-1001**
Created Date/Time	**04-Apr-19 11:18:21 PM**
Event Description Summary	**Windows Installer installed the product.**
Level	**Information**
Keywords	**0x0080000000000000**
Provider Name	**MsiInstaller**
Task Category	**0**
Computer	**DESKTOP-M9TVKRB**

Event Data


```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="MsiInstaller" />
<EventID Qualifiers="0">1033</EventID>
<Level>4</Level>
<Task>0</Task>
<Keywords>0x0080000000000000</Keywords>
<TimeCreated SystemTime="2019-04-04T20:18:21.2168913Z" />
<EventRecordID>474</EventRecordID>
<Channel>Application</Channel>
<Computer>DESKTOP-M9TVKRB</Computer>
<Security UserID="S-1-5-21-167654484-677196580-2748798096-1001" />
</System>
<EventData>
<Data>Backup and Sync from Google3.43.2448.907110330Google, Inc.(NULL)</Data>
<Binary>7B3639334341444230 2D393632422D344143312D413933392D393532344232353843393937 7D303030306538373766626376235663435363537306363366464353034356566306338353030303030393034</Binary>
</EventData>
</Event>
```


Εικόνα 45

Αρχείο καταγραφής συμβάντων των Windows (Windows Event Logs)

Διαδρομή Αρχείου: C:\Windows\System32\winevt\Logs\Application.evtx

ARTIFACT INFORMATION

Application Name	**GOOGLEDRIVESYNC.EXE**
Application Run Count	**4**
Last Run Date/Time	**05-Apr-19 12:04:57 AM**
2nd Last Run Date/Time	**05-Apr-19 12:04:48 AM**
3rd Last Run Date/Time	**04-Apr-19 11:18:42 PM**
4th Last Run Date/Time	**04-Apr-19 11:18:31 PM**

Εικόνα 46
Αρχείο δραστηριότητας του λογισμικού (Backup and Sync from Google) της υπηρεσίας νέφους Google Drive
Διαδρομή Αρχείου: C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-FE5C9C83.pf

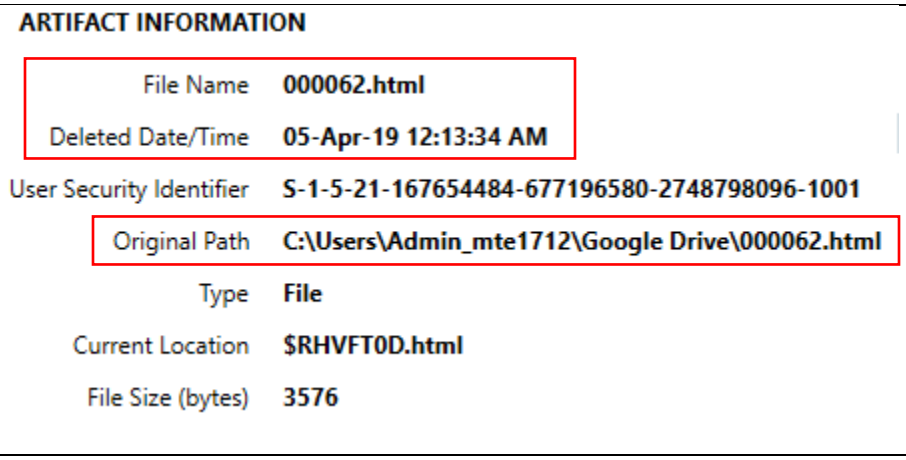
Εντοπίστηκαν επιπλέον στη διαδρομή C:\Users\<username>\Google Drive, όλα τα αρχεία του χρήστη που ανήκουν στο λογαριασμό του και έχουν συγχρονιστεί με το λογισμικό του Google Drive στον υπολογιστή του. Από την εξέταση των μεταδεδομένων των αρχείων, μπορούν να εξαχθούν συμπεράσματα σχετικά με το πότε αυτά «κατέβηκαν» στον υπολογιστή του χρήστη από τον λογαριασμό του στο Google Drive ή το ανάποδο.

Μέχρι στιγμής, από τα προαναφερθέντα στοιχεία αποδεικνύεται η χρήση του λογισμικού Google Drive, όπως επίσης και η ύπαρξη αρχείων που σχετίζονται με το λογαριασμό ενός συγκεκριμένου χρήστη. Στη συνέχεια γίνεται προσπάθεια εντοπισμού τόσο των στοιχείων του εν λόγω χρήστη όσο και της δραστηριότητας του, μέσω της ανάλυσης των δεδομένων που προέκυψαν.

8.3.2. Εντοπισμός και ανάλυση της δραστηριότητας του χρήστη

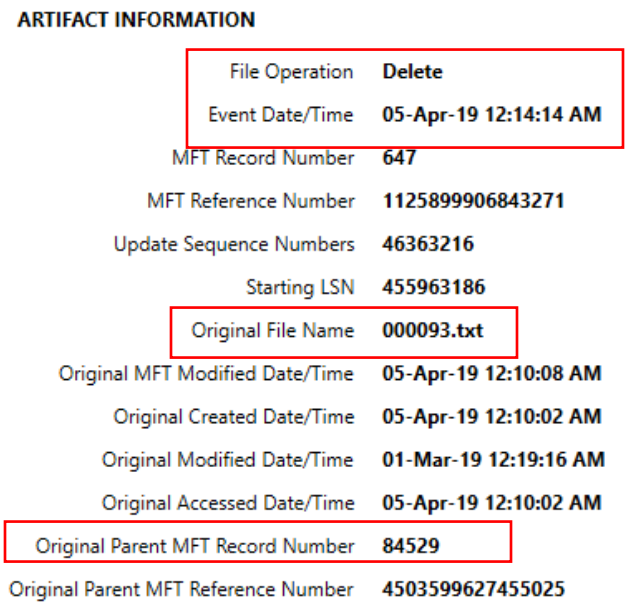
Εντοπίστηκαν στοιχεία που βοήθησαν στην εξακρίβωση ορισμένων ενεργειών που πραγματοποίησε ο χρήστης, χρησιμοποιώντας την υπηρεσία Google Drive. Κάτωθι παρουσιάζονται (βλ. Εικόνες 47-50) τα δεδομένα που εντοπίστηκαν και μπορούν να αποδοθούν σε μία συγκεκριμένη ενέργεια του χρήστη:

1. **Διαγραφή αρχείων** (βλ. Εικόνες 47 και 48)
   - Στον κάδο ανακύκλωσης του χρήστη, καθώς και στο αρχείο καταγραφής του λειτουργικού συστήματος Windows 10, με ονομασία $Logfile, εντοπίστηκαν εγγραφές διαγεγραμμένων αρχείων, τα οποία ήταν προηγουμένως συγχρονισμένα με το λογαριασμό του στο νέφος. Επισημαίνεται ότι κατέστη εφικτή η ανάκτηση της ημερομηνίας διαγραφής τους, όπως επίσης ανακτήθηκε για ένα εξ αυτών και η διαδρομή στην οποία βρισκόταν αρχικά αποθηκευμένο, πριν να διαγραφεί.



Εικόνα 47

Διαγεγραμμένο αρχείο του χρήστη, το οποίο βρισκόταν αποθηκευμένο στο Google Drive Διαδρομή Αρχείου: C:\$Recycle.Bin\S-1-5-21-167654484-677196580-2748798096-1001\ $IHVFT0D.html



Εικόνα 48

Διαγεγραμμένο αρχείο του χρήστη, το οποίο βρισκόταν αποθηκευμένο στο Google Drive Διαδρομή Αρχείου: C:\$LogFile

Η ανάλυση της δραστηριότητας του χρήστη συνεχίζεται και στο επόμενο υποκεφάλαιο.

8.3.3. Εξέταση των αρχείων του λογισμικού του Google Drive

Σε αυτό το υποκεφάλαιο γίνεται εξέταση των αρχείων που εμπεριέχονται στη διαδρομή C:\Users\<username>\AppData\Local\Google\Drive. Αυτός ο φάκελος όπως αναφέρθηκε και προηγουμένως (βλ. Πίνακα 11), περιέχει φακέλους και αρχεία που σχετίζονται άμεσα με τη χρήση της εφαρμογής Backup and Sync from Google της Google Drive. Αναλυτικά αναφέρονται τα εξής:

- Εντός φακέλου που βρισκόταν στην ανωτέρω διαδρομή, εντοπίστηκε ένα αρχείο καταγραφής της εν λόγω εφαρμογής. Το αρχείο αυτό, φέρει ονομασία «sync_log .log» και περιέχει πολύ χρήσιμα δεδομένα για έναν ερευνητή. Ειδικότερα, στο αρχείο «sync_log.log» καταγράφονται πληροφορίες όπως το πότε συνδέθηκε ο χρήστης της εφαρμογής, ποια διεύθυνση ηλεκτρονικού ταχυδρομείου ήταν συνδεδεμένη με το λογισμικό, ποιες ενέργειες πραγματοποίησε ο χρήστης μέσω αυτής και πότε, κ.ά.. Ενδεικτικά παρουσιάζονται κάτωθι (βλ. Εικόνες 49-53) ορισμένες από τις πληροφορίες που αποθηκεύονται στο ανωτέρω αρχείο καταγραφής.

```
2019-04-04 23:28:23,471 +0300 INFO pid=9012 9060:LaunchThreads   user.py:82
Initializing User instance with new credentials. mtel712.gougldraiv@gmail.com
2019-04-04 23:28:23,471 +0300 INFO pid=9012 9060:LaunchThreads   sync_app.py:1287
Configuring sync app from feature switches.
2019-04-04 23:28:23,471 +0300 INFO pid=9012 9060:LaunchThreads   sync_app.py:1305
Feature Switches:
FeatureSwitchSettings(
StoragePolicyEnabled=True,
accept_blob_download_gzip_encoding=True,
add_delete_mode_property_to_machine_root=True,
additional_mime_types=[],
allow_hq_download_modify=False,
backup_polling_interval_secs=7200,
change_buffer_journal_disabled_platforms=['win'],
change_filters=['DRIVE_SYNC'],
cloud_graph_disk_generation=8,
cloud_watcher_backoff_wait_time_sec=300,
crash_log_size_limit=10000000,
crash_throttle_percentage=0.0,
download_change_throttle_sec=0.05,
download_url=u'
```

Εικόνα 49

Σύνδεση λογαριασμού στο Google Drive μέσω της εφαρμογής

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.log

```
2019-04-05 00:10:03,223 +0300 INFO pid=9012 7836:DifferThread
aggregator.py:56 --------> Received change FSChange(Direction.UPLOAD,
Action.CREATE, local_id=LocalID(inode=1125899906843271L,
volume='serial:1889534574'), path=u'\\\\?\\C:\\Users\\Admin_mtel712\\Google
Drive', name=u'000093.txt', parent_local_id=LocalID(inode=4503599627455025L,
volume='serial:1889534574'), is_folder=False, modified=1551392356, size=32010,
generator_module=Generator.LOCAL_EVENT_GENERATOR, shared=False)
2019-04-05 00:10:03,223 +0300 INFO pid=9012 7836:DifferThread
change_buffer_base.py:488 Adding change to change buffer:
FSChange(Direction.UPLOAD, Action.CREATE,
local_id=LocalID(inode=1125899906843271L, volume='serial:1889534574'),
path=u'\\\\?\\C:\\Users\\Admin_mtel712\\Google Drive', name=u'000093.txt',
parent_local_id=LocalID(inode=4503599627455025L, volume='serial:1889534574'),
is_folder=False, modified=1551392356, size=32010,
generator_module=Generator.LOCAL_EVENT_GENERATOR, shared=False, hash=-112722832
2019-04-05 00:10:03,239 +0300 INFO pid=9012 7836:DifferThread
aggregator.py:56 --------> Received change FSChange(Direction.UPLOAD,
Action.CREATE, local_id=LocalID(inode=7318349394477701L,
volume='serial:1889534574'), path=u'\\\\?\\C:\\Users\\Admin_mtel712\\Google
Drive', name=u'000061.html', parent_local_id=LocalID(inode=4503599627455025L,
volume='serial:1889534574'), is_folder=False, modified=1551392356, size=2788,
generator_module=Generator.LOCAL_EVENT_GENERATOR, shared=False)
```

Εικόνα 50

«Ανέβασμα» αρχείων στο Google Drive μέσω του συνδεδεμένου λογαριασμού στην εφαρμογή

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.log

```
2019-04-05 18:03:25,368 +0300 INFO pid=2596 6536:CloudWatcher
aggregator.py:56 --------> Received change FSChange(Direction.DOWNLOAD,
Action.CREATE, name=u'testSync.docx',
route=[ImmutableCloudEntry(doc_id=14yTPRw_JL7gbzXWbLSzvD8fYQO7vLc3s,filename=test
ync.docx,modified=1554476604,created=None,acl_role=owner,doc_type=DocType.BLOB,re
oved=False,parent_doc_ids=frozenset([u'root']),child_doc_ids=unavailable,size=116
8,checksum=84c19d407abbf1c2073lddaee148132c,change_stamp=512,is_zombie=False,shar
d=False,recursive_size=None,version=3,original_size=None,original_checksum=None,d
wnload_restricted=False,down_sample_status=None,last_changed_locally=False,from_t
mbstone=False,photos_storage_policy=StoragePolicyMode.ORIGINAL)],
mapped_path=MappedCloudPath(mapped=\\?\C:\Users\Admin_mtel712\Google Drive,
is_complete=False), doc_id=u'14yTPRw_JL7gbzXWbLSzvD8fYQO7vLc3s',
parent_local_id=LocalID(inode=4503599627455025L, volume='serial:1889534574'),
is_folder=False, size=11628, doc_type=DocType.BLOB, hash=-673079009)
```

Εικόνα 51

«Κατέβασμα» αρχείου μέσω του συνδεδεμένου λογαριασμού στο Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.log

```
2019-04-05 00:13:58,786 +0300 INFO pid=9012 7836:DifferThread
change_buffer_base.py:488 Adding change to change buffer:
FSChange(Direction.UPLOAD, Action.DELETE,
local_id=LocalID(inode=28147497671106809L, volume='serial:1889534574'),
path=u'\\\\?\\C:\\Users\\Admin_mtel712\\Google Drive', name=u'000074.html',
parent_local_id=LocalID(inode=4503599627455025L, volume='serial:1889534574'
is_folder=False, generator_module=Generator.LOCAL_EVENT_GENERATOR,
hash=-1734233806)
```

Εικόνα 52

Διαγραφή αρχείου μέσω του συνδεδεμένου λογαριασμού στο Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.log

```
2019-04-04 23:28:51,221 +0300 INFO pid=9012 7360:CloudWatcher
cloud_watcher.py:1183 CloudWatcher generated FSChange(Direction.DOWNLOAD,
Action.CREATE, name=u'000230.txt',
route=[CloudEntry(doc_id=lEmVTadZCpYf2Hv4vpLv-VZ38cA_AoXdH,filename=000230.txt,mo
ified=1553811547,created=None,acl_role=owner,doc_type=DocType.BLOB,removed=False,
arent_doc_ids=set([u'root']),child_doc_ids=unavailable,size=28277,checksum=e6a06b
10fe6c3686f00f3cb704a97e4,change_stamp=None,is_zombie=False,shared=True,recursive
size=None,version=4,original_size=None,original_checksum=None,download_restricted
False,down_sample_status=None,last_changed_locally=False,from_tombstone=False,pho
os_storage_policy=StoragePolicyMode.ORIGINAL)],
mapped_path=MappedCloudPath(mapped=\\?\C:\Users\Admin_mtel712\Google Drive,
is_complete=False), doc_id=u'lEmVTadZCpYf2Hv4vpLv-VZ38cA_AoXdH',
parent_local_id=LocalID(inode=4503599627455025L, volume='serial:1889534574'),
is_folder=False, size=28277, generator_module=Generator.INITIAL_CLOUD_DIFF,
doc_type=DocType.BLOB)
2019-04-04 23:28:51,221 +0300 INFO pid=9012 7360:CloudWatcher
cloud_watcher.py:1183 CloudWatcher generated FSChange(Direction.DOWNLOAD,
Action.CREATE, name=u'000218.txt',
route=[CloudEntry(doc_id=lWZpbCtBsalFyZTv2sAXLqK4Zm7hOAvNi,filename=000218.txt,mo
ified=1553811547,created=None,acl_role=owner,doc_type=DocType.BLOB,removed=False,
arent_doc_ids=set([u'root']),child_doc_ids=unavailable,size=24340,checksum=76e953
6b44b5e80a756bblaf286f190,change_stamp=None,is_zombie=False,shared=True,recursive
size=None,version=8,original_size=None,original_checksum=None,download_restricted
False,down_sample_status=None,last_changed_locally=False,from_tombstone=False,pho
os_storage_policy=StoragePolicyMode.ORIGINAL)],
mapped_path=MappedCloudPath(mapped=\\?\C:\Users\Admin_mtel712\Google Drive,
is_complete=False), doc_id=u'lWZpbCtBsalFyZTv2sAXLqK4Zm7hOAvNi',
parent_local_id=LocalID(inode=4503599627455025L, volume='serial:1889534574'),
is_folder=False, size=24340, generator_module=Generator.INITIAL_CLOUD_DIFF,
doc_type=DocType.BLOB)
```

Εικόνα 53

Αρχεία τα οποία διαμοιράζονται στον συνδεδεμένο λογαριασμό στο Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.log

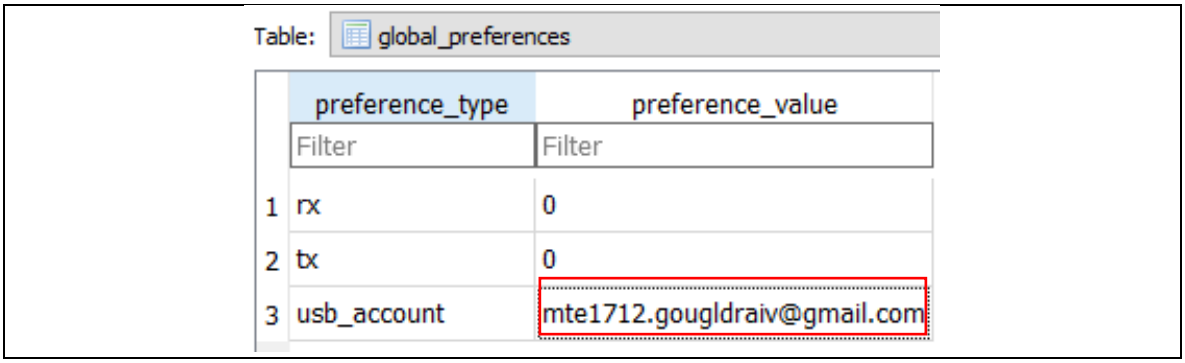
- Σε φακέλους που βρίσκονταν στην ανωτέρω διαδρομή, εντοπίστηκαν βάσεις δεδομένων που περιείχαν εξίσου χρήσιμες πληροφορίες για έναν ερευνητή. Πιο συγκεκριμένα, οι κυριότερες βάσεις δεδομένων που πρέπει να απασχολήσουν τον ερευνητή είναι αυτές που φαίνονται στον ακόλουθο πίνακα (βλ. Πίνακα 12).

Διαδρομή και όνομα αρχείου βάσης δεδομένων	**Περιγραφή**
C:\Users\<username>\AppData\Local\Google\Drive\user_default\ **snapshot.db**	Περιέχει πληροφορίες για τα αρχεία που έχουν συγχρονιστεί, με το λογαριασμό του συνδεδεμένου χρήστη. Περιλαμβάνει εντός του και τα δεδομένα που περιέχει η βάση δεδομένων cloud_graph.db
C:\Users\<username>\AppData\Local\Google\Drive\cloud_graph\ **cloud_graph.db**	Περιέχει πληροφορίες για τα αρχεία που έχουν συγχρονιστεί, με το λογαριασμό του συνδεδεμένου χρήστη. Τα δεδομένα του περιέχονται και στη βάση δεδομένων snapshot.db
C:\Users\<username>\AppData\Local\Google\Drive\user_default\ **sync_config.db**	Περιλαμβάνει δεδομένα όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Google Drive.
C:\Users\<username>\AppData\Local\Google\Drive**global.db**	Περιλαμβάνει δεδομένα όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Google Drive.

Πίνακας 12

Αρχεία βάσεων δεδομένων του λογισμικού της υπηρεσίας Google Drive που παρουσιάζουν ενδιαφέρον, για τον ερευνητή ψηφιακής εγκληματολογίας

Κατόπιν της ανάλυσης τους, κάτωθι παρουσιάζονται μερικά από τα δεδομένα που έφεραν αποθηκευμένα (βλ. Εικόνες 54-57):



Εικόνα 54

Email του συνδεδεμένου λογαριασμού στο Google Drive- πίνακας global_preferences
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\global.db

Table: data

	entry_key	data_key	
	Filter	Filter	Filter
1	storage_policy_mode	value	original
2	user_email	value	mte1712.gougldraiv@gmail.com
3	shown_setup_overlays	setup_overla...	google_drive_setup_overlay

Εικόνα 55

Email του συνδεδεμένου λογαριασμού στο Google Drive- πίνακας data
Διαδρομή Αρχείου:
C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_config.db

Table: cloud_entry

	doc_id	filename	modified	reate	cl_rol	oc_typ	emove	size	hecksu	shared
	Filter	Filter	Filter				...	...	...	Filter
1	1EmVTadZCpYf...	000230.txt	1553811547	NULL	0	1	0	28277	e6a0...	1
2	1WZpbCtBsalFy...	000218.txt	1553811547	NULL	0	1	0	24340	76e9...	1
3	1St6xGICQVwb...	1stLastDoc	1553811381	NULL	0	6	0	NULL	NULL	1
4	1FQ6lCfCsn2sQ...	5.xlsx	1553811486	NULL	0	1	0	8297	a682...	1
5	1a7lv_54Zu1KC...	000062.html	1553811486	NULL	0	1	0	3576	7e7e...	1
6	1p0n9I_L-CxGL...	1.docx	1553811348	NULL	0	1	0	11590	16e3...	1
7	1VVj3qoIzQ_0h...	Πρώτο Έγγραφο	1553811211	NULL	0	6	0	NULL	NULL	1
8	1wtNdWc3V0UI...	000196.pdf	1553504841	NULL	0	1	0	40291	483b...	1
9	1y0CkVuYqZDi...	1stExcel	1553504780	NULL	0	4	0	NULL	NULL	1
10	1rEWTSHmNAz...	1stPresentation	1553504780	NULL	0	2	0	NULL	NULL	1
11	root	root	NULL	NULL	NULL	0	NULL	NULL	NULL	0

Εικόνα 56

Αρχεία που έχουν διαμοιράζονται σε άλλους χρήστες μέσω της εφαρμογής στο Google Drive. πίνακας-cloud_entry
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\snapshot.db

filename	modified	created	acl_role	doc_type	removed	size	checksum
Filter	Filter	Fil...	Fil...	Fil...	Fil...	Fil...	Filter
000068.html	1551392356	NULL	0	1	0	2758	fb0f00696613e519b0dd87788e6b1700
000290.ppt	1553498977	NULL	0	1	0	98304	f15eca4ca12b880f879b6e556b773c2d
000230.txt	1553811547	NULL	0	1	0	28277	e6a06b210fe6c3686f00f3cb704a97e4
Getting started	1553498725	NULL	0	1	0	1560010	df1f432d0c63e3d1ff27e01d10ec8e10
testSync 2.pptx	1554476749	NULL	0	1	0	0	d41d8cd98f00b204e9800998ecf8427e
000248.doc	1553637359	NULL	0	1	0	1015808	cbc340fd5a7157a2553a8ee99e897cb8
000301.ppt	1553637356	NULL	0	1	0	209408	c94d140d402f2c08001643291675ad5c
000246 (1).jpeg	1553637357	NULL	0	1	0	24618	c508a19de274262e51498ac7b7358105
Google Drive.lnk	1554409703	NULL	0	1	0	1768	c3fa7bc3806bb2e708afbf94249c905b
000508.jpeg	1553498982	NULL	0	1	0	19192	963a42b967899933385a5e6cc56d0a74
testSync1.xlsx	1554476697	NULL	0	1	0	6628	8c7c3b8d11ff28e2eb1200601d1e7866
000349.pdf	1553637356	NULL	0	1	0	39259	8734047463328a2e48f550cc658e780d
testSync.docx	1554476604	NULL	0	1	0	11628	84c19d407abbf1c20731ddaee148132c
000127.doc	1553498976	NULL	0	1	0	32768	83e7d35c3a98ff424d8455835b937838
000061.html	1551392356	NULL	0	1	0	2788	811e129201981dcc2d42342d1744b10a
000218.txt	1553811547	NULL	0	1	0	24340	76e953c6b44b5e80a756bb1af286f190

Εικόνα 57

Αλφαριθμητικές ταυτότητες μοναδικότητας αρχείων (MD5) που έχουν μεταφορτωθεί μέσω της εφαρμογής στο Google Drive. πίνακας- cloud_entry
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Drive\user_default\snapshot.db

Από τις ανωτέρω Εικόνες 49, 54 και 55 αποδεικνύεται ότι ο συνδεδεμένος λογαριασμός με το Google Drive, φέρει διεύθυνση ηλεκτρονικού ταχυδρομείου την «mte1712.gougldraiv@gmail.com». Επιπρόσθετα, στις υπόλοιπες εικόνες φαίνονται ξεκάθαρα ποιες ενέργειες πραγματοποίησε ο χρήστης μέσω της εφαρμογής. Ακόμη, φαίνονται ποια αρχεία είναι συγχρονισμένα με το λογαριασμό στο Google Drive και ποια από αυτά διαμοιράζονται σε άλλους χρήστες. Τέλος, στην Εικόνα 57 φαίνονται οι αλφαριθμητικές ταυτότητες μοναδικότητας (MD5) των αρχείων που είναι συγχρονισμένα με τον ανωτέρω λογαριασμό. Η ύπαρξη τους επιτρέπει τη σύγκριση με τις αλφαριθμητικές ταυτότητες μοναδικότητας τυχόν άλλων επίμαχων αρχείων.

Ενδέχεται να υπάρχουν και άλλα αποδεικτικά στοιχεία στις βάσεις δεδομένων που εντοπίστηκαν στην ανωτέρω διαδρομή. Ωστόσο αυτά που έχουν ήδη αναφερθεί, αρκούν για να αποδείξουν όχι μόνο τη χρήση της υπηρεσίας Google Drive, αλλά και για να υποδείξουν πολλές από τις ενέργειες που φέρεται να έκανε ο χρήστης μέσω αυτής.

Στο επόμενο υποκεφάλαιο γίνεται εξέταση των πτητικών δεδομένων της μνήμης RAM και παρουσίαση των ευρημάτων που προέκυψαν από αυτή.

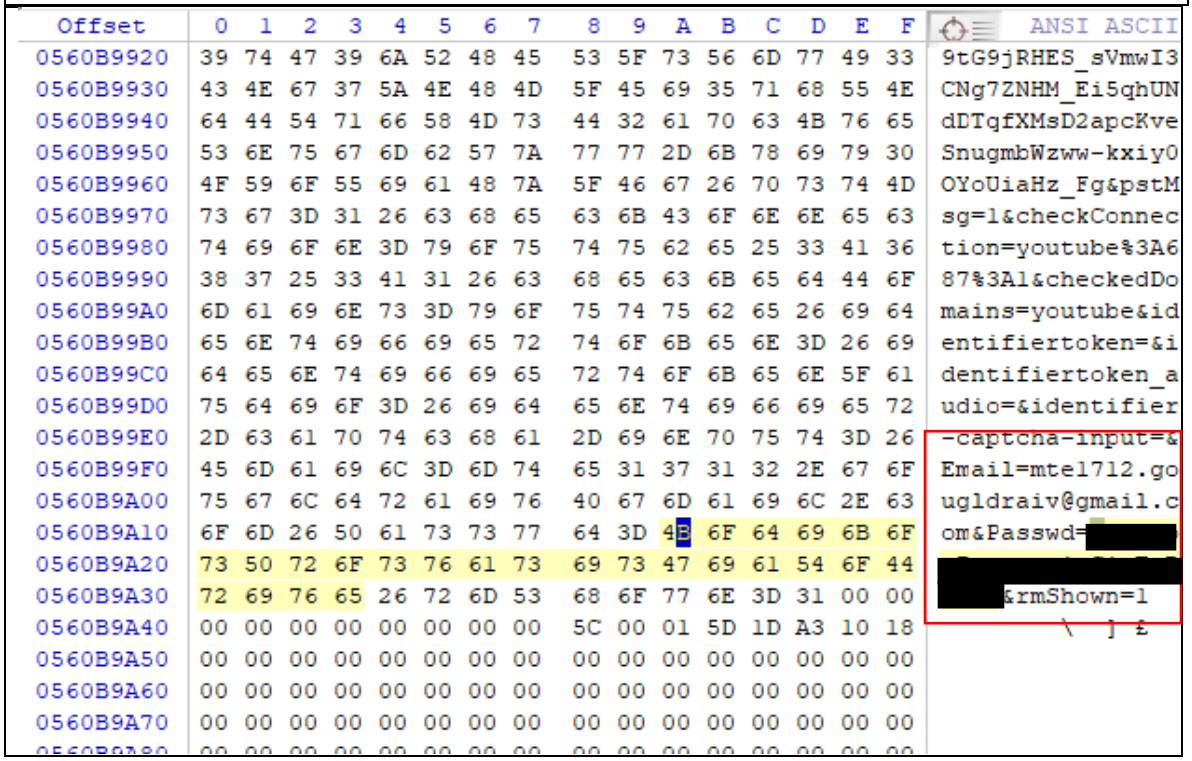
8.3.4. Εξέταση της μνήμης RAM

Κατά την εξέταση της μνήμης RAM εντοπίστηκε η διεύθυνση ηλεκτρονικού ταχυδρομείου του λογαριασμού που ήταν συνδεδεμένος στο Google Drive και ο κωδικός πρόσβασης που χρησιμοποιούνταν σε αυτόν. Τα ευρήματα προέκυψαν αναζητώντας στα εγκληματολογικά αντίγραφα της μνήμης, τις συμβολοσειρές που απεικονίζονται κάτωθι (βλ. Πίνακας 13). Μερικά ευρήματα παρουσιάζονται παρακάτω (βλ. Εικόνα 58).

Συμβολοσειρές (Strings)	Περιγραφή
email_address=u	Αναζητώντας αυτές τις συμβολοσειρές εμφανίζεται η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Google Drive
"emailAddress":	
"email":	
&Email=	
&Passwd=	Αναζητώντας αυτές τις συμβολοσειρές εμφανίζεται ο κωδικός πρόσβασης του χρήστη στο Google Drive

Πίνακας 13

Ευρήματα στη μνήμη RAM



Εικόνα 58
Η διεύθυνση ηλεκτρονικού ταχυδρομείου και ο κωδικός πρόσβασης του συνδεδεμένου λογαριασμού στο Google Drive

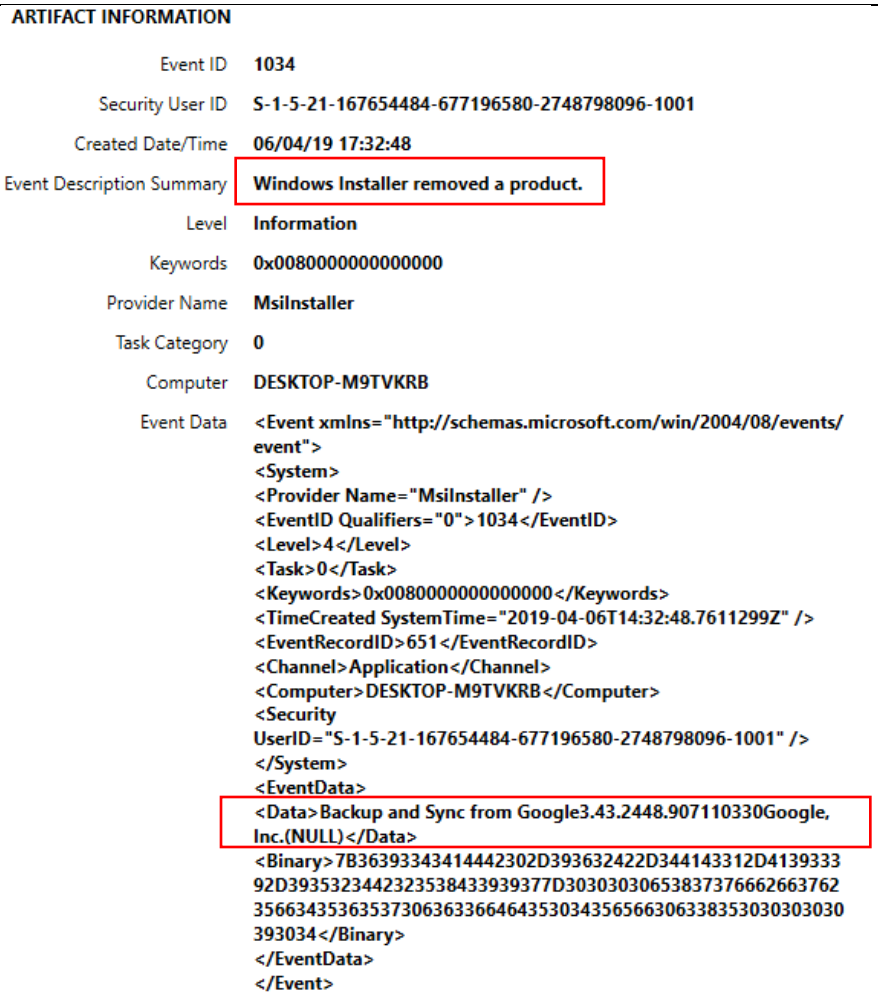
Εφόσον εντοπίστηκαν ικανοποιητικά ευρήματα σχετικά με τη χρήση της εφαρμογής της υπηρεσίας Google Drive, θα ερευνηθεί στο επόμενο υποκεφάλαιο, εάν συμβαίνει το ίδιο και έπειτα από την απεγκατάσταση της εφαρμογής Backup and Sync from Google της Google Drive.

8.3.5. Απεγκατάσταση του λογισμικού του Google Drive

Σε αυτό το υποκεφάλαιο γίνεται απεγκατάσταση της εφαρμογής Backup and Sync from Google της Google Drive σε 2 εικονικές μηχανές και γίνεται προσπάθεια εντοπισμού παρόμοιων δεδομένων με αυτών που εντοπίστηκαν προηγουμένως. Στη μία εικονική μηχανή η απεγκατάσταση γίνεται μέσω του λειτουργικού συστήματος των Windows, ενώ στην άλλη μέσω τρίτου προγράμματος και ειδικότερα με χρήση του CCleaner.

Έπειτα από την απεγκατάσταση της ανωτέρω εφαρμογής (μέσω του λειτουργικού συστήματος):

1. Διαγράφηκαν ορισμένοι από τους φακέλους και τα αρχεία που είχαν δημιουργηθεί κατά την εγκατάσταση του λογισμικού του Google Drive. Επισημαίνεται ότι με το λογισμικό Magnet Axiom δεν κατέστη εφικτή η ανάκτηση των διαγεγραμμένων αρχείων. Ωστόσο, χρησιμοποιώντας το λογισμικό Winhex και τη λειτουργία ανάκτησης δεδομένων που προσφέρει (Data Carving), ανακτήθηκε το αρχείο καταγραφής «sync_log.log».
2. Εντοπίστηκαν στοιχεία που καταδεικνύουν την απεγκατάσταση του λογισμικού του Google Drive. Τα στοιχεία αυτά σχετίζονται άμεσα με το λειτουργικό σύστημα Windows 10. Ειδικότερα, βρέθηκαν εγγραφές στα αρχεία καταγραφής συμβάντων των Windows (Windows Event Logs). Ενδεικτικά, παρουσιάζεται κάτωθι μία εξ αυτών (βλ. Εικόνα 59).
3. Όσον αφορά τις βάσεις δεδομένων που περιλάμβαναν τα επίμαχα δεδομένα, επισημαίνεται ότι διαγράφηκαν όλες, χωρίς να κατέστη εφικτό να ανακτηθούν ολόκληρες και ως εκ τούτου δεν μπορούσαν να προβληθούν τα δεδομένα τους.
4. Τέλος αναφέρεται ότι όλα τα αρχεία που είχαν συγχρονιστεί με το λογισμικό του Google Drive και βρίσκονταν στη διαδρομή C:\Users\<username>\Google Drive δεν διαγράφηκαν αλλά διατηρήθηκαν αναλλοίωτα ακόμα και έπειτα από τη διαγραφή του λογισμικού (κατά την απεγκατάσταση ο χρήστης ερωτάται αν προτιμά τη διαγραφή ή την παραμονή των αρχείων).



ARTIFACT INFORMATION

Event ID	**1034**
Security User ID	**S-1-5-21-167654484-677196580-2748798096-1001**
Created Date/Time	**06/04/19 17:32:48**
Event Description Summary	**Windows Installer removed a product.**
Level	**Information**
Keywords	**0x0080000000000000**
Provider Name	**MsiInstaller**
Task Category	**0**
Computer	**DESKTOP-M9TVKRB**
Event Data	**<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="MsiInstaller" /><EventID Qualifiers="0">1034</EventID><Level>4</Level><Task>0</Task><Keywords>0x0080000000000000</Keywords><TimeCreated SystemTime="2019-04-06T14:32:48.7611299Z" /><EventRecordID>651</EventRecordID><Channel>Application</Channel><Computer>DESKTOP-M9TVKRB</Computer><Security UserID="S-1-5-21-167654484-677196580-2748798096-1001" /></System><EventData><Data>Backup and Sync from Google3.43.2448.907110330Google, Inc.(NULL)</Data><Binary>7B36393343414442302D393632422D344143312D413933392D393532344232353843393937 7D3030303065383737666266376235663435363537306363366464353034356566306338353030303030393034</Binary></EventData></Event>**

Εικόνα 59

Αρχείο καταγραφής συμβάντων των Windows (Windows Event Logs)
Διαδρομή Αρχείου: C:\Windows\System32\winevt\Logs\Application.evtx

Έπειτα από την απεγκατάσταση της εφαρμογής Google Drive (μέσω του λογισμικού CCleaner) εντοπίστηκαν παρόμοια ευρήματα.

Στη συνέχεια εξετάζονται οι φυλλομετρητές Ιστού, και το πώς η χρήση τους επηρεάζει την ύπαρξη ή μη αποδεικτικών στοιχείων, σχετικών με τη χρήση της υπηρεσίας νέφους Google Drive.

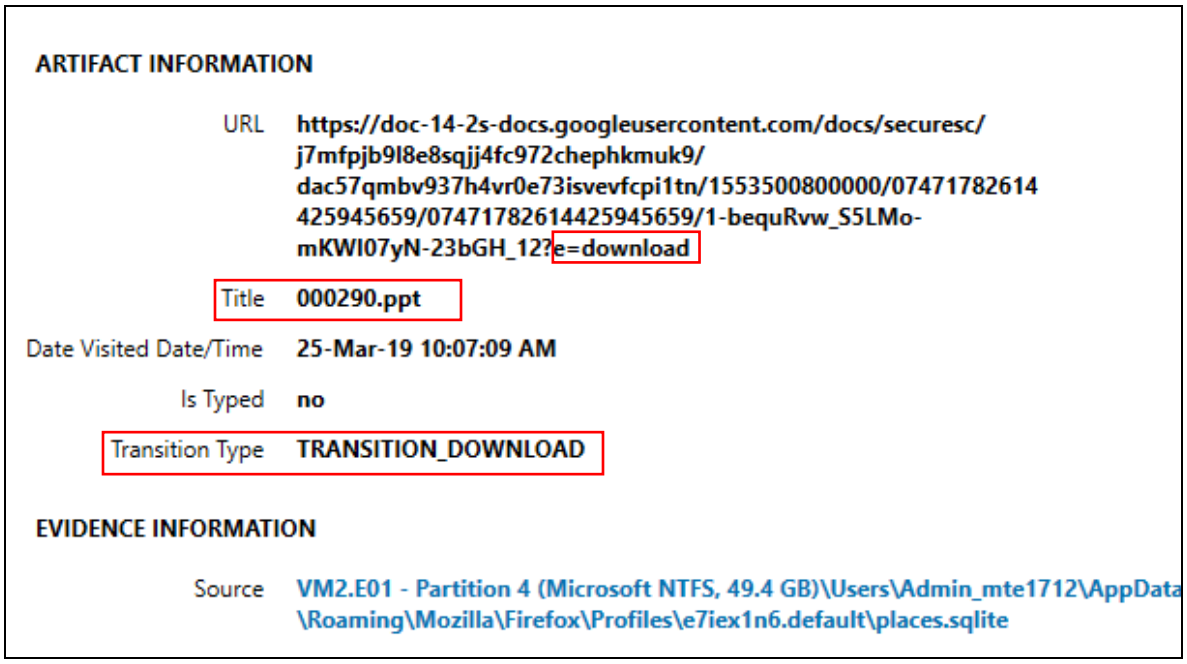
8.4. Χρήση των φυλλομετρητών Ιστού για πρόσβαση στην υπηρεσία Google Drive

8.4.1. Εξέταση του Mozilla Firefox

Όπως συνέβη και στην εξέταση της υπηρεσίας Dropbox, έτσι και εδώ, τα ευρήματα που προέκυψαν από την εξέταση των φυλλομετρητών Ιστού είναι σχετικά λιγότερα από αυτά που εντοπίστηκαν κατά την εξέταση της εφαρμογής του Google Drive.

Έπειτα από τις ενέργειες που περιγράφονται στο Κεφάλαιο 6, πραγματοποιήθηκε δικανική εξέταση στα εγκληματολογικά αντίγραφα των εικονικών μηχανών, των φυλλομετρητών Ιστού. Τα ευρήματα που εντοπίστηκαν, βοήθησαν στην εξακρίβωση ορισμένων ενεργειών που πραγματοποίησε ο χρήστης, χρησιμοποιώντας την υπηρεσία Google Drive. Στη συνέχεια παρουσιάζονται (βλ. Εικόνες 60-63) τα στοιχεία που εντοπίστηκαν και μπορούν να αποδοθούν σε μία συγκεκριμένη ενέργεια του χρήστη:

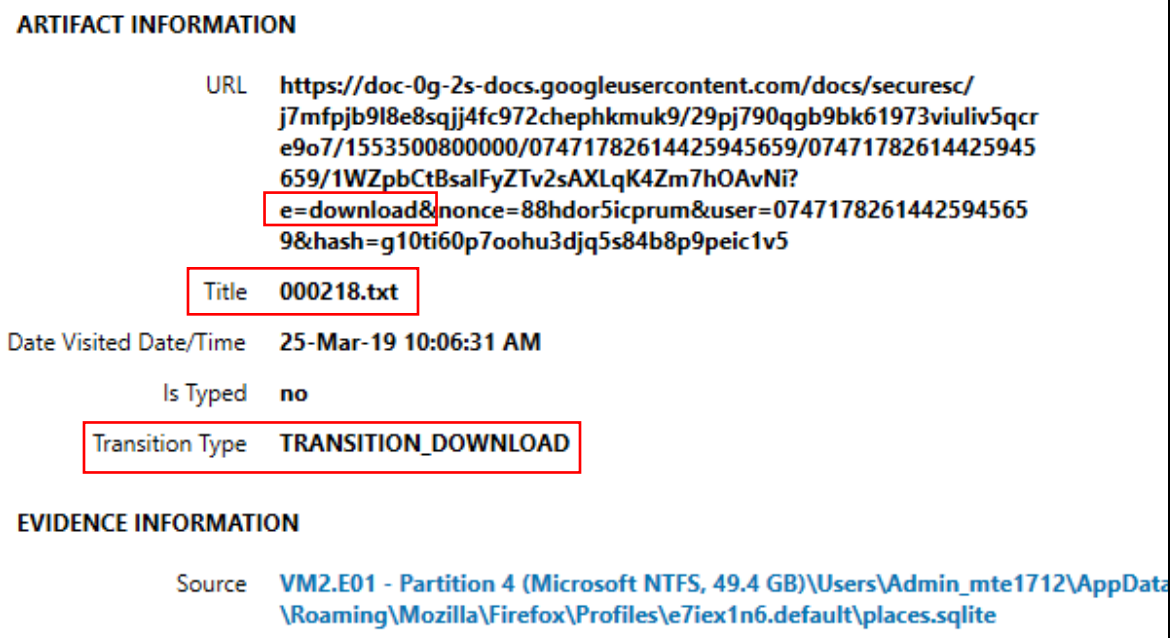
1. **Μεταφόρτωση (download) αρχείων μέσω του φυλλομετρητή Ιστού**
   - Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στη μεταφόρτωση (download) αρχείων από το νέφος του χρήστη (βλ. Εικόνες 60 και 61).



Εικόνα 60

Μεταφόρτωση αρχείου παρουσίασης μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite



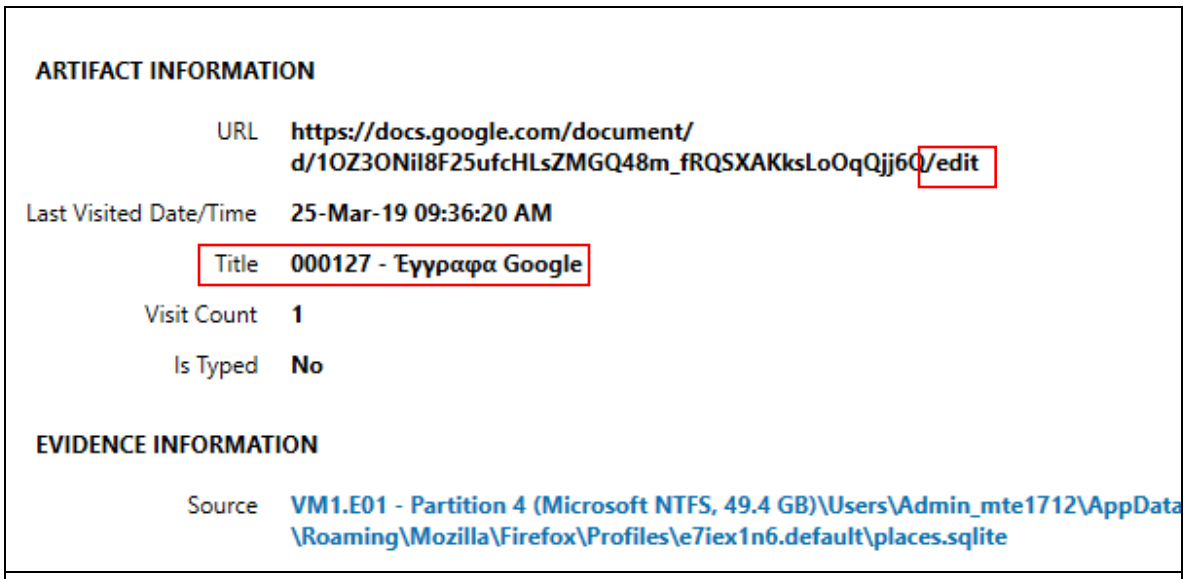
Εικόνα 61

Μεταφόρτωση αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite

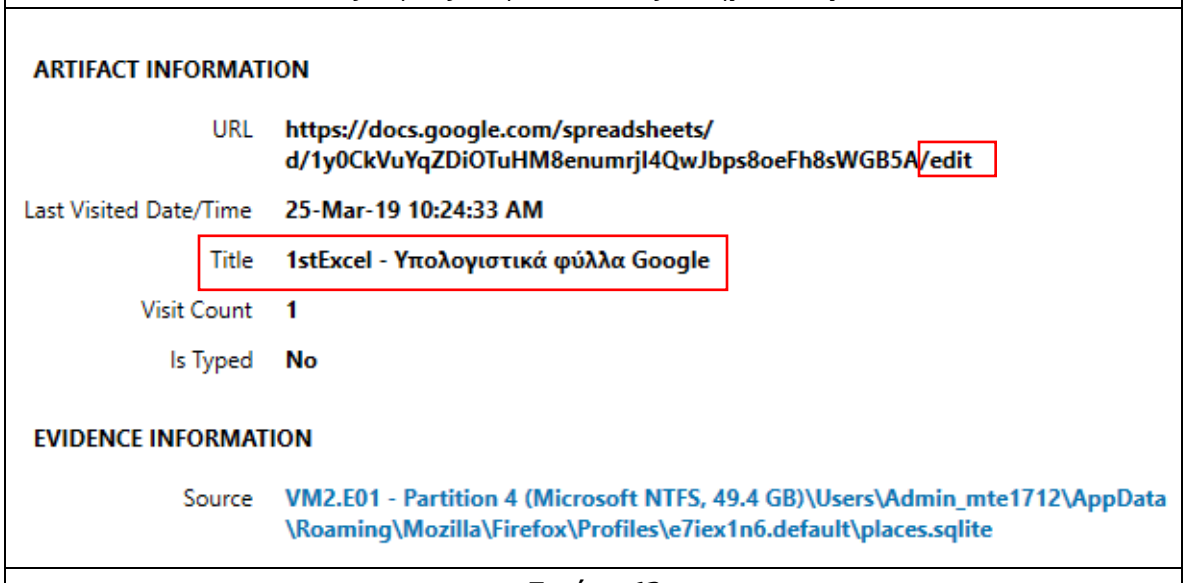
2. Επεξεργασία αρχείων μέσω του φυλλομετρητή Ιστού

- Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στην επεξεργασία αρχείων που υπάρχουν αποθηκευμένα στο νέφος του χρήστη (βλ. Εικόνες 62 και 63).



Εικόνα 62

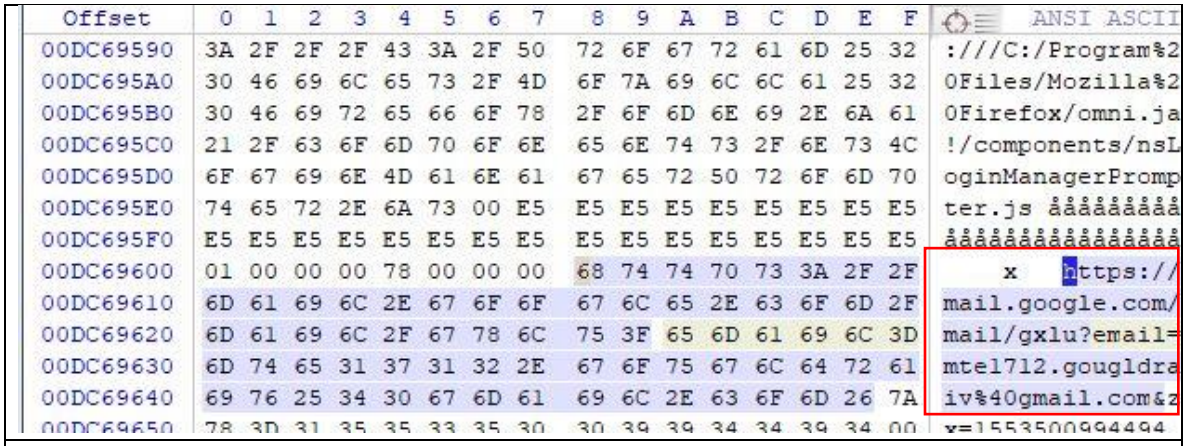
Επεξεργασία αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite



Εικόνα 63

Επεξεργασία αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\ AppData\Roaming\Mozilla\Firefox\Profiles\e7iex1n6.default\places.sqlite

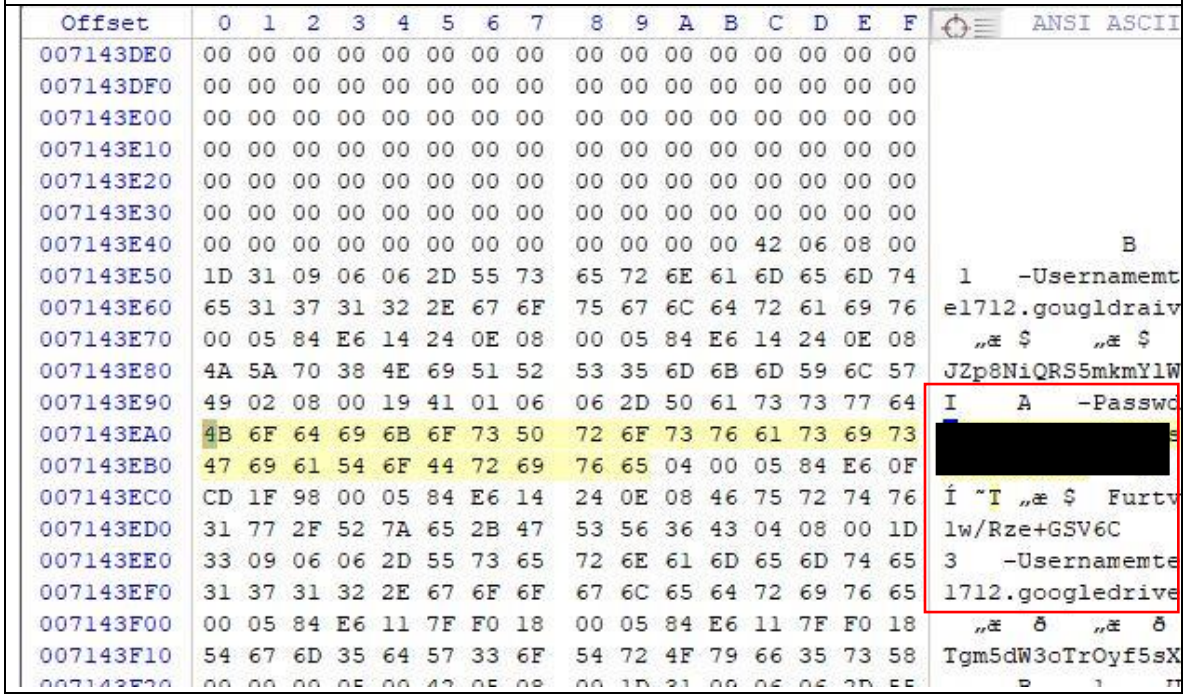
Έγινε αναζήτηση στο αντίγραφο της μνήμης RAM, σχετικά με τον λογαριασμό στον οποίο ανήκει η ανωτέρω δραστηριότητα. Κατά την αναζήτηση σε αυτή (χρησιμοποιώντας τη συμβολοσειρά «email=») εντοπίστηκε η σύνδεση ενός λογαριασμού στην υπηρεσία Google. Επιπρόσθετα, διερευνώντας περαιτέρω τη μνήμη RAM (χρησιμοποιώντας τη συμβολοσειρά «passwd») εντοπίστηκε ο κωδικός πρόσβασης του εν λόγω λογαριασμού (σε απλό κείμενο) και το όνομα χρήστη που χρησιμοποιεί. Στις εικόνες που ακολουθούν (βλ. Εικόνες 64 και 65), προβάλλονται τα εν λόγω ευρήματα της μνήμης RAM.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00DC69590	3A	2F	2F	2F	43	3A	2F	50	72	6F	67	72	61	6D	25	32	:///C:/Program%2
00DC695A0	30	46	69	6C	65	73	2F	4D	6F	7A	69	6C	6C	61	25	32	0Files/Mozilla%2
00DC695B0	30	46	69	72	65	66	6F	78	2F	6F	6D	6E	69	2E	6A	61	0Firefox/omni.ja
00DC695C0	21	2F	63	6F	6D	70	6F	6E	65	6E	74	73	2F	6E	73	4C	!/components/nsL
00DC695D0	6F	67	69	6E	4D	61	6E	61	67	65	72	50	72	6F	6D	70	oginManagerPromp
00DC695E0	74	65	72	2E	6A	73	00	E5	E5	E5	E5	E5	E5	E5	E5	E5	ter.js åååååååå
00DC695F0	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	åååååååååååååååå
00DC69600	01	00	00	00	78	00	00	00	68	74	74	70	73	3A	2F	2F	x https://
00DC69610	6D	61	69	6C	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	2F	mail.google.com/
00DC69620	6D	61	69	6C	2F	67	78	6C	75	3F	65	6D	61	69	6C	3D	mail/gxlu?email=
00DC69630	6D	74	65	31	37	31	32	2E	67	6F	75	67	6C	64	72	61	mte1712.gougldra
00DC69640	69	76	25	34	30	67	6D	61	69	6C	2E	63	6F	6D	26	7A	iv%40gmail.com&z
00DC69650	78	3D	31	35	35	33	35	30	30	39	39	34	34	39	34	00	x=1553500994494

Εικόνα 64

Διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη στο Google Drive



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
007143DE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
007143DF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
007143E00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
007143E10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
007143E20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
007143E30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
007143E40	00	00	00	00	00	00	00	00	00	00	00	00	42	06	08	00	B
007143E50	1D	31	09	06	06	2D	55	73	65	72	6E	61	6D	65	6D	74	1 -Usernamemt
007143E60	65	31	37	31	32	2E	67	6F	75	67	6C	64	72	61	69	76	e1712.gougldraiv
007143E70	00	05	84	E6	14	24	0E	08	00	05	84	E6	14	24	0E	08	„æ $ „æ $
007143E80	4A	5A	70	38	4E	69	51	52	53	35	6D	6B	6D	59	6C	57	JZp8NiQRS5mkmYlW
007143E90	49	02	08	00	19	41	01	06	06	2D	50	61	73	73	77	64	I A -Passwd
007143EA0	4B	6F	64	69	6B	6F	73	50	72	6F	73	76	61	73	69	73	[redacted]
007143EB0	47	69	61	54	6F	44	72	69	76	65	04	00	05	84	E6	0F	
007143EC0	CD	1F	98	00	05	84	E6	14	24	0E	08	46	75	72	74	76	Í ˜T „æ $ Furtv
007143ED0	31	77	2F	52	7A	65	2B	47	53	56	36	43	04	08	00	1D	1w/Rze+GSV6C
007143EE0	33	09	06	06	2D	55	73	65	72	6E	61	6D	65	6D	74	65	3 -Usernamemte
007143EF0	31	37	31	32	2E	67	6F	6F	67	6C	65	64	72	69	76	65	1712.googledrive
007143F00	00	05	84	E6	11	7F	F0	18	00	05	84	E6	11	7F	F0	18	„æ ð „æ ð
007143F10	54	67	6D	35	64	57	33	6F	54	72	4F	79	66	35	73	58	Tgm5dW3oTrOyf5sX
007143F20	00	00	00	05	00	42	05	08	00	1D	31	00	06	06	2D	55	B 1 -U

Εικόνα 65
Κωδικός πρόσβασης και όνομα του χρήστη στο Google Drive

Υπάρχει η πιθανότητα να βρεθούν αποθηκευμένα τα στοιχεία εισόδου του χρήστη και στις βάσεις δεδομένων του φυλλομετρητή Ιστού, ωστόσο σε αυτά τα σενάρια δεν επιλέχθηκε από τον χρήστη η αποθήκευση τους. Ακολουθεί η εξέταση του φυλλομετρητή Ιστού Google Chrome.

8.4.2. Εξέταση του Google Chrome

Η εξέταση του Google Chrome όσον αφορά τη χρήση της υπηρεσίας Google Drive, είχε ως αποτέλεσμα πολλά περισσότερα και πιο χρήσιμα ευρήματα από όσα έχουν παρουσιαστεί μέχρι τώρα, τόσο από την εξέταση των φυλλομετρητών Ιστού για την υπηρεσία Dropbox όσο και για την υπηρεσία Google Drive (μέσω του Mozilla Firefox).

Στην προκειμένη περίπτωση, κατά την εξέταση των δεδομένων του φυλλομετρητή Google Chrome, εντοπίστηκαν αποδεικτικά στοιχεία, τα οποία βοήθησαν στην εξακρίβωση διαφόρων ενεργειών που πραγματοποίησε ο χρήστης, χρησιμοποιώντας την υπηρεσία Google Drive. Στη συνέχεια αναλύονται (βλ. Εικόνες 66-74) τα δεδομένα που βρέθηκαν και μπορούν να αποδοθούν σε μία συγκεκριμένη ενέργεια του χρήστη:

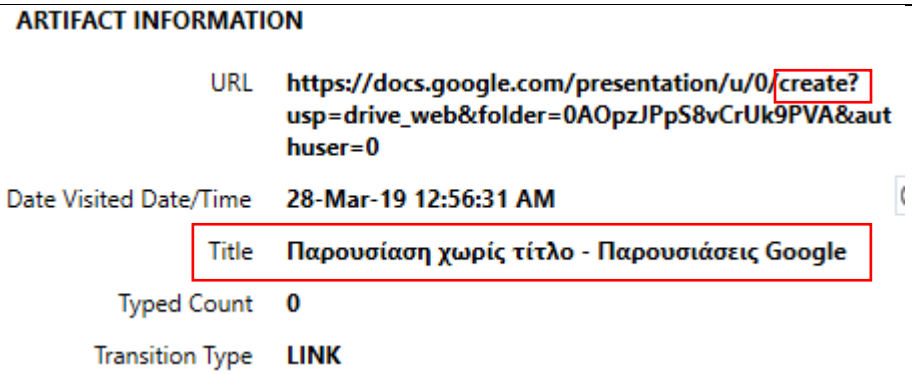
1. **Δημιουργία νέων αρχείων μέσω του φυλλομετρητή Ιστού**
   - Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στη δημιουργία νέων αρχείων στο νέφος του χρήστη (βλ. Εικόνες 66 και 67).

ARTIFACT INFORMATION

URL	**https://docs.google.com/document/create?usp=drive_web&ouid=113057060742050977240&folder=0AOpzJPpS8vCrUk9PVA&authuser=0**
Date Visited Date/Time	**28-Mar-19 12:48:50 AM**
Title	**Έγγραφο χωρίς τίτλο - Έγγραφα Google**
Typed Count	**0**
Transition Type	**LINK**

Εικόνα 66

Δημιουργία νέου αρχείου κειμένου μέσω φυλλομετρητή Ιστού, στην υπηρεσία Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

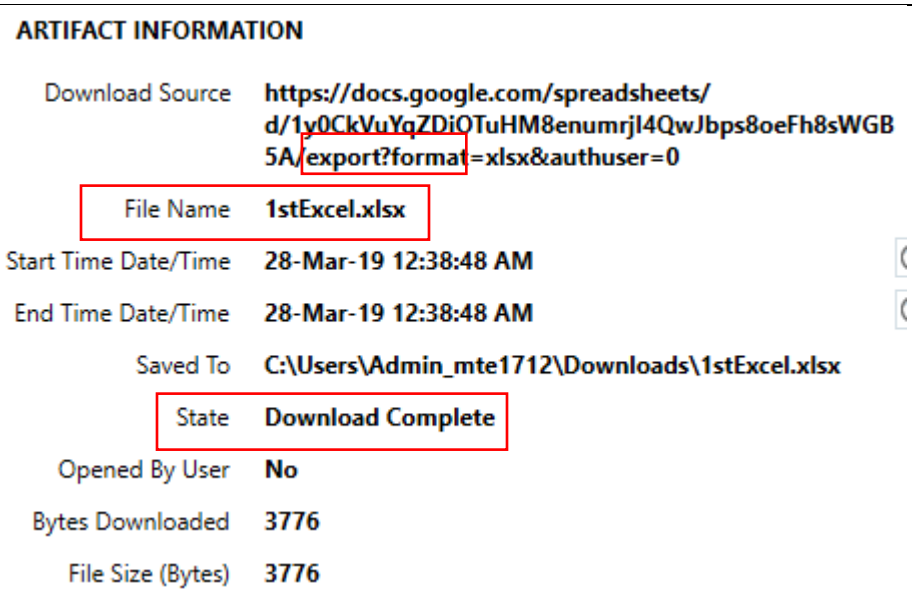


Εικόνα 67

Δημιουργία νέου αρχείου παρουσίασης μέσω φυλλομετρητή Ιστού, στην υπηρεσία Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

2. Μεταφόρτωση (download) αρχείων μέσω του φυλλομετρητή Ιστού

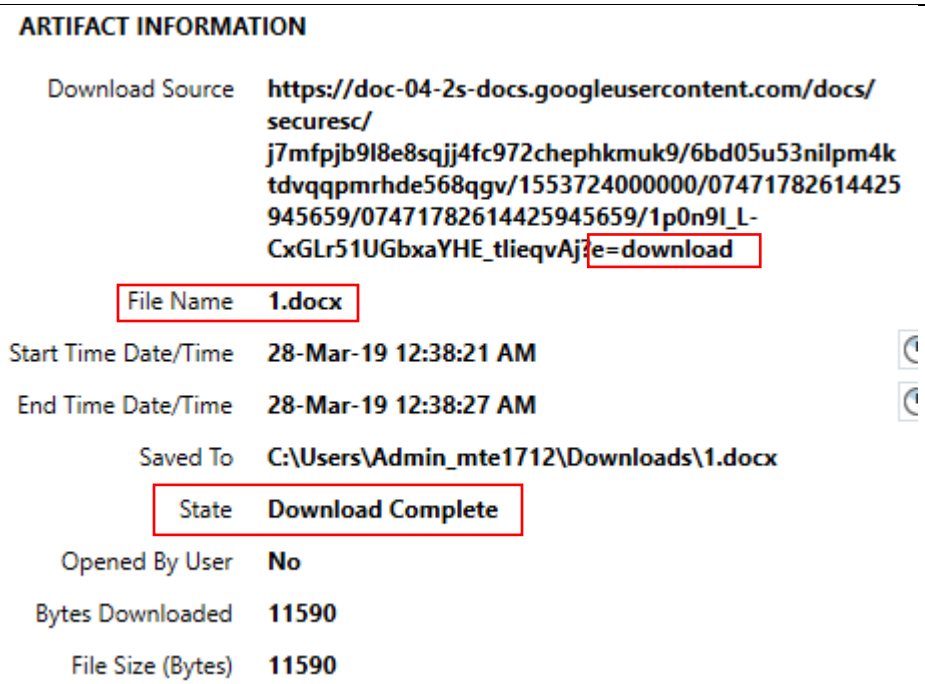
- Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στη μεταφόρτωση (download) αρχείων από το νέφος του χρήστη (βλ. Εικόνες 68 και 69).



Εικόνα 68

Μεταφόρτωση αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History



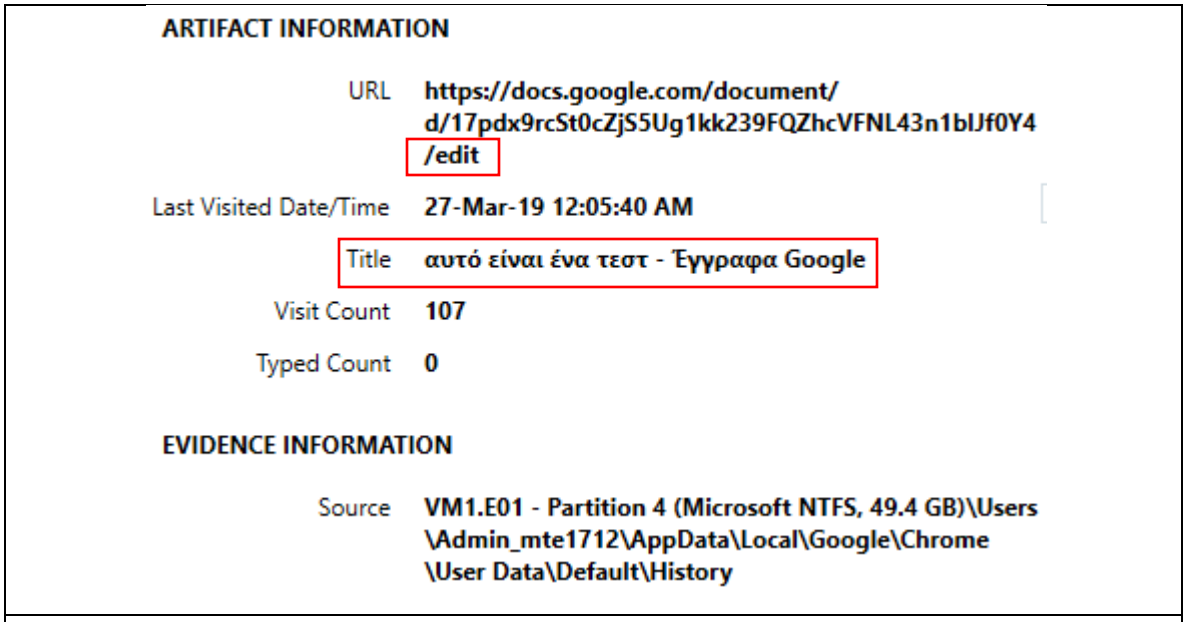
Εικόνα 69

Μεταφόρτωση αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive

Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

3. Επεξεργασία αρχείων μέσω του φυλλομετρητή Ιστού

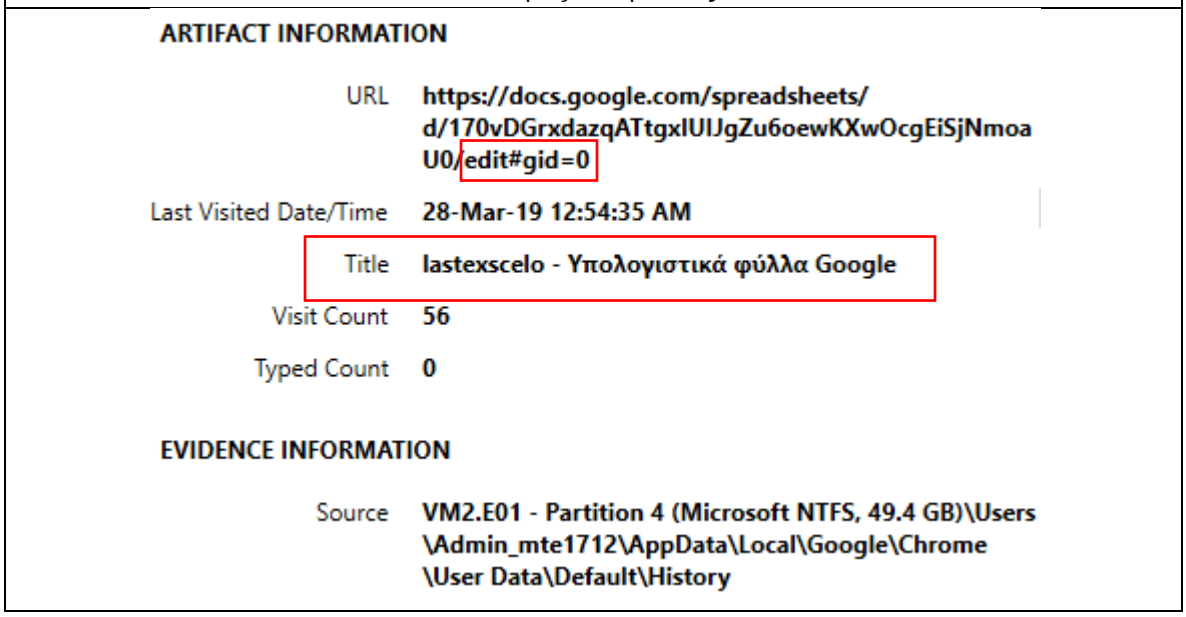
- Εντοπίστηκαν στις βάσεις δεδομένων του φυλλομετρητή Ιστού και ειδικότερα στο ιστορικό περιήγησης μέσω αυτού, εγγραφές οι οποίες μπορούν να αποδοθούν στην επεξεργασία αρχείων που υπάρχουν αποθηκευμένα στο νέφος του χρήστη (βλ. Εικόνες 70 και 71).



Εικόνα 70

Επεξεργασία αρχείου κειμένου μέσω φυλλομετρητή Ιστού, το οποίο είναι αποθηκευμένο στην υπηρεσία Google Drive

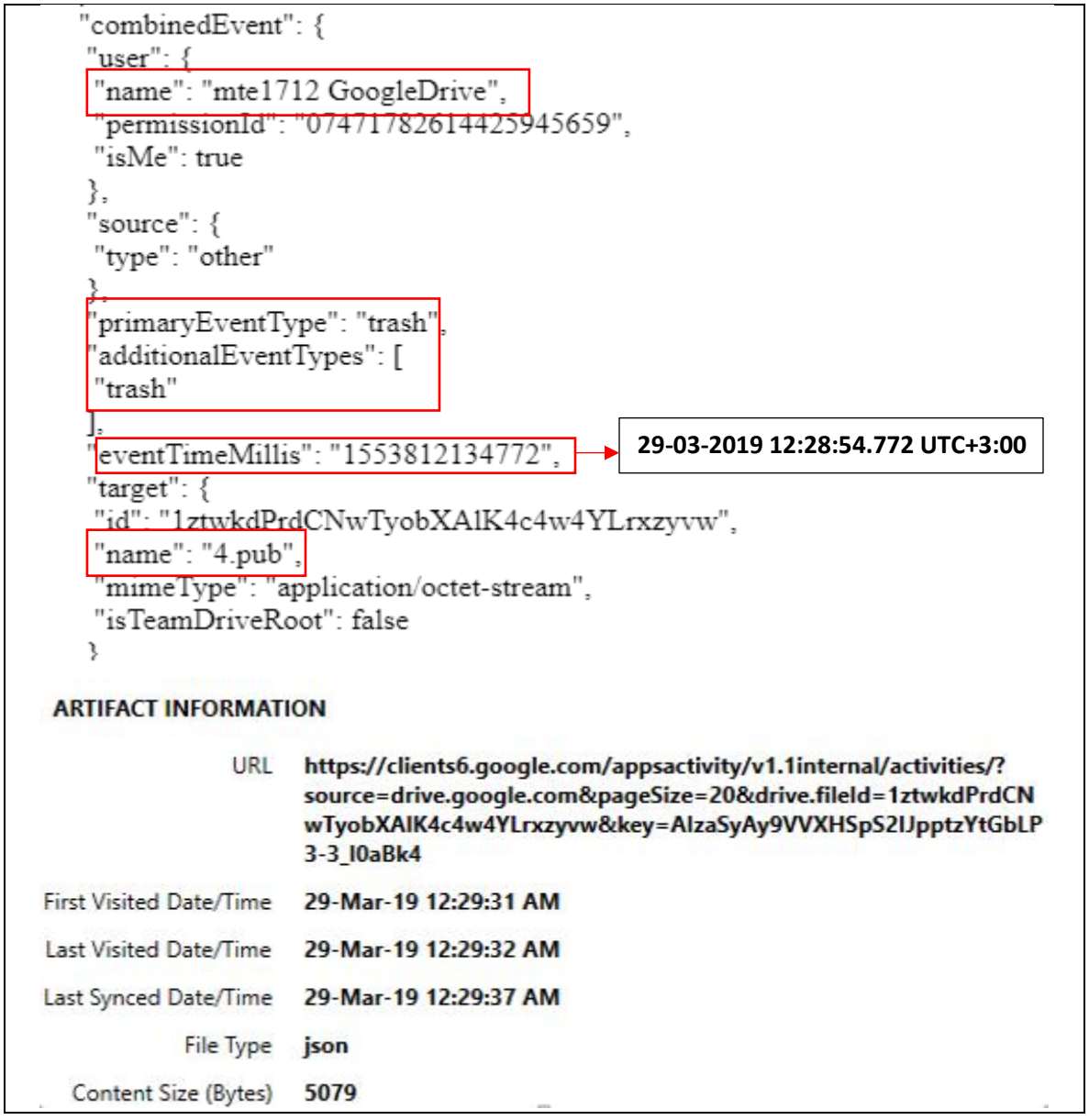
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History



Εικόνα 71
Επεξεργασία αρχείου λογιστικών φύλλων μέσω φυλλομετρητή Ιστού, το οποίο είναι αποθηκευμένο στην υπηρεσία Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

4. Διαγραφή αρχείων μέσω του φυλλομετρητή Ιστού

- Εντοπίστηκαν στη κρυφή μνήμη (cache) του φυλλομετρητή Ιστού, εγγραφές οι οποίες μπορούν να αποδοθούν στη διαγραφή αρχείων που βρίσκονταν αποθηκευμένα στο νέφος του χρήστη (βλ. Εικόνα 72).



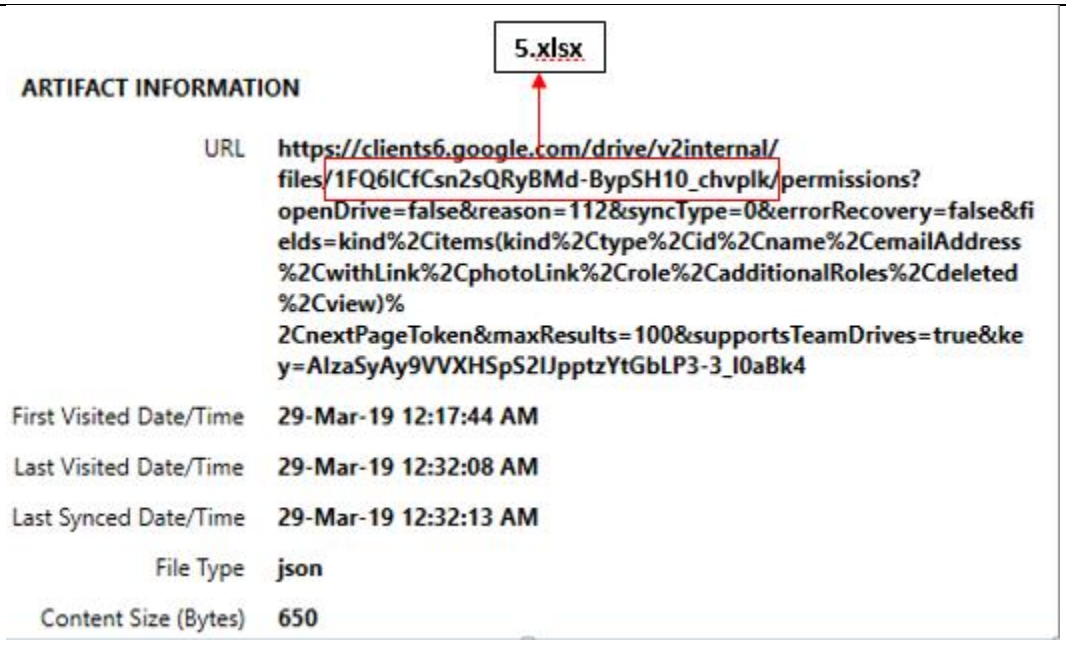
Εικόνα 72

Διαγραφή αρχείου κειμένου μέσω φυλλομετρητή Ιστού, από την υπηρεσία Google Drive
Διαδρομή Αρχείου: C:\Users\<username>\ AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

5. Διαμοιρασμός αρχείων μέσω του φυλλομετρητή Ιστού

- Εντοπίστηκαν στη κρυφή μνήμη (cache) του φυλλομετρητή Ιστού, εγγραφές οι οποίες μπορούν να αποδοθούν στο διαμοιρασμό αρχείων που βρίσκονταν αποθηκευμένα στο νέφος του χρήστη (βλ. Εικόνα 73).


```
"kind": "drive#permissionList",
"items": [
 {
 "kind": "drive#permission",
 "id": "01747070467446906007i",
 "emailAddress": "mte1712_ShareItWithMe@outlook.com.gr",
 "role": "writer",
 "type": "user",
 "deleted": false
 },
 {
 "kind": "drive#permission",
 "id": "07471782614425945659",
 "name": "mte1712 GoogleDrive",
 "emailAddress": "mte1712.gougldraiv@gmail.com",
 "role": "owner",
 "type": "user",
 "deleted": false
 },
 {
 "kind": "drive#permission",
 "id": "17650141624490290820i",
 "emailAddress": "mte1712_ShareItWithMe2@gmail.com",
 "role": "writer",
 "type": "user",
```

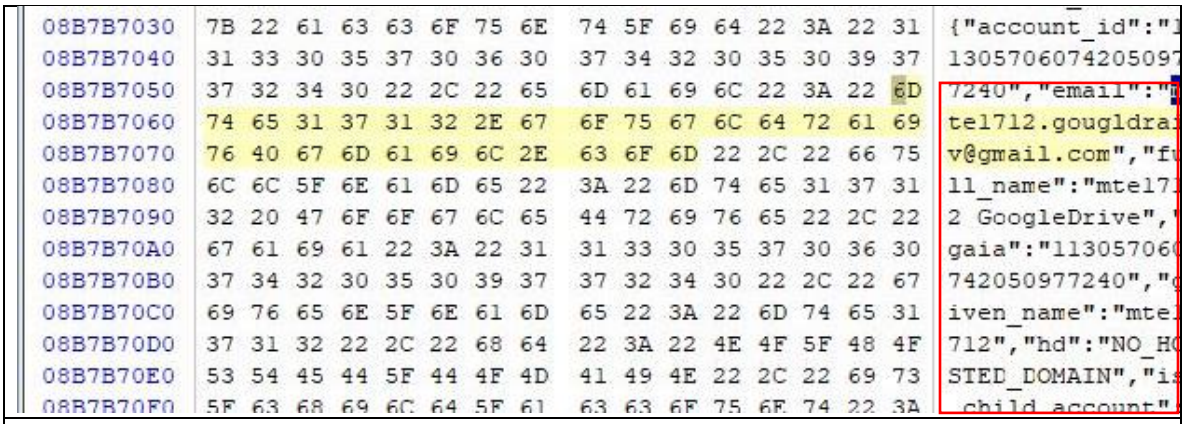


Εικόνα 73

Πληροφορίες αρχείου λογιστικών φύλλων που καταδεικνύει τον διαμοιρασμό του στην υπηρεσία Google Drive

Διαδρομή Αρχείου: C:\Users\<username>\ AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

Κατά την εξέταση της μνήμης RAM εντοπίστηκε η διεύθυνση ηλεκτρονικού ταχυδρομείου του λογαριασμού που ήταν συνδεδεμένος στο Google Drive (βλ. Εικόνα 74). Και εδώ υπάρχει η πιθανότητα να βρεθούν αποθηκευμένα διάφορα στοιχεία εισόδου του χρήστη, στις βάσεις δεδομένων του φυλλομετρητή Ιστού, ωστόσο σε αυτά τα σενάρια δεν επιλέχθηκε από τον χρήστη η αποθήκευση τους.



Εικόνα 74

Η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Google Drive

8.5. Εξέταση των μεταδεδομένων των αρχείων

Πριν τη μεταφόρτωση (upload) των αρχείων στο νέφος, καταγράφηκαν οι αλφαριθμητικές ταυτότητες μοναδικότητας (MD5) τους, προκειμένου να απαντηθεί η δεύτερη ερευνητική ερώτηση. Όπως επισημάνθηκε και στο Κεφάλαιο 6, το αντικείμενο μελέτης σε αυτό το υποκεφάλαιο αποτελούν όσα αρχεία δεν τέθηκαν υπό επεξεργασία (πάσης φύσεως επεξεργασία, π.χ. μετονομασία, περικοπή, διαγραφή, κ.ά.) από τον χρήστη, για το διάστημα που αυτά παρέμειναν στο νέφος. Τα αρχεία αυτά στη συνέχεια μεταφορτώθηκαν (download) από το νέφος και έγινε η σύγκριση των τεχνικών χαρακτηριστικών τους με αυτά των αρχικών αρχείων. Κάτωθι παρουσιάζονται σε 2 πίνακες τα τεχνικά χαρακτηριστικά των αρχείων πριν «ανέβουν» στο νέφος (βλ. Πίνακας 14) και αφότου «κατέβηκαν» από αυτό (βλ. Πίνακας 15).

Όνομα αρχείου	**Ημερομηνία Δημιουργίας (File Created)**	**Ημερομηνία Τελευταίας Προσπέλασης (Last Accessed)**	**Ημερομηνία Τελευταίας Τροποποίησης (Last Modified)**	**MD5**
000196.pdf	13-Mar-19 00:16:02	13-Mar-19 00:18:18	15-Apr-04 12:13:14	483ba74e1f2af97a245251f7cdee62a9
000382.xls	13-Mar-19 00:16:03	13-Mar-19 00:17:47	25-Jan-04 11:19:04	16eec263082ba76b6644a71d23a4b61a
000290.ppt	13-Mar-19 00:16:03	13-Mar-19 00:18:03	27-May-08 18:38:08	f15eca4ca12b880f879b6e556b773c2d
000218.txt	13-Mar-19 00:16:02	13-Mar-19 00:18:16	28-Mar-06 06:27:20	76e953c6b44b5e80a756bb1af286f190

Πίνακας 14

Τεχνικά χαρακτηριστικά των αρχείων πριν «ανέβουν» στο νέφος

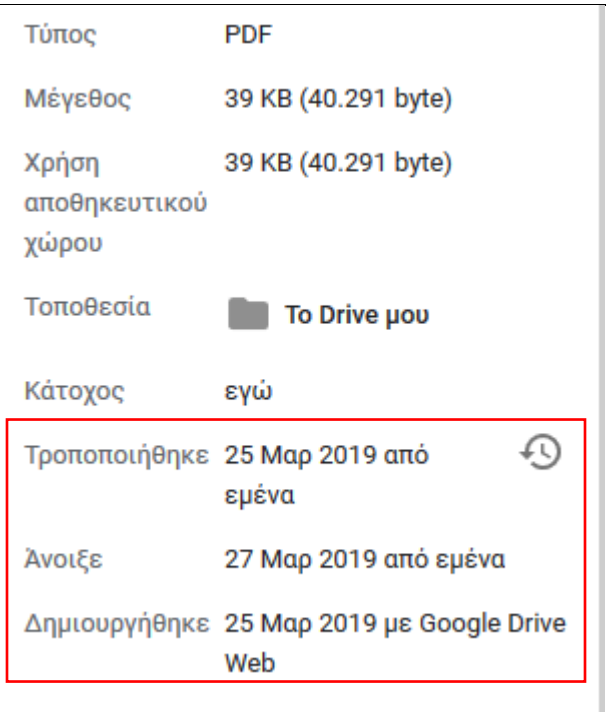
Όνομα αρχείου	**Ημερομηνία Δημιουργίας (File Created)**	**Ημερομηνία Τελευταίας Προσπέλασης (Last Accessed)**	**Ημερομηνία Τελευταίας Τροποποίησης (Last Modified)**	**MD5**
000196.pdf	28-Mar-19 00:40:08	28-Mar-19 00:40:08	28-Mar-19 00:40:10	483ba74e1f2af97a245251f7cdee62a9
000382.xls	25-Mar-19 10:07:36	25-Mar-19 10:07:36	25-Mar-19 10:07:42	16eec263082ba76b6644a71d23a4b61a
000290.ppt	25-Mar-19 10:07:06	25-Mar-19 10:07:06	25-Mar-19 10:07:09	f15eca4ca12b880f879b6e556b773c2d
000218.txt	25-Mar-19 10:06:26	25-Mar-19 10:06:26	25-Mar-19 10:06:31	76e953c6b44b5e80a756bb1af286f190

Πίνακας 15

Τεχνικά χαρακτηριστικά των αρχείων αφού «κατέβουν» από το νέφος

Συγκρίνοντας τους 2 πίνακες, παρατηρείται ότι συμβαίνει ότι συνέβη και με την υπηρεσία Dropbox, δηλ. οι αλφαριθμητικές ταυτότητες μοναδικότητας (MD5) των αρχείων παραμένουν ίδιες. Επομένως, μπορεί να εξαχθεί με ασφάλεια το συμπέρασμα ότι η μεταφόρτωση (download/upload) αρχείων στο νέφος, δεν τις επηρεάζει.

Από την άλλη μεριά, η μεταφόρτωση (download/upload) αρχείων από και προς το νέφος, επηρεάζει τις χρονοσφραγίδες των εν λόγω αρχείων. Ειδικότερα, οι χρονοσφραγίδες των αρχείων μεταβάλλονται δύο φορές. Η μία φορά είναι όταν από τη συσκευή του χρήστη «ανέβουν» και αποθηκευτούν στο νέφος, Και η άλλη φορά είναι όταν «κατέβουν» από το νέφος στη συσκευή του χρήστη. Για παράδειγμα, το αρχείο με ονομασία «000196.pdf» πριν «ανέβει» στο νέφος, φέρει τις χρονοσφραγίδες του Πίνακα 14. Όταν «ανέβηκε» στο νέφος, οι χρονοσφραγίδες τους μεταβλήθηκαν όπως φαίνονται στη κάτωθι εικόνα (βλ. Εικόνα 75). Και όταν το αρχείο αυτό, «κατέβηκε» από το νέφος, οι χρονοσφραγίδες τους μεταβλήθηκαν εκ νέου, όπως φαίνεται στον Πίνακα 15.



Εικόνα 75

Προβολή των χρονοσφραγίδων του αρχείου «000196.pdf», όσο βρίσκεται αποθηκευμένο στο νέφος της υπηρεσίας Google Drive

Τέλος αναφέρεται ότι το περιεχόμενο των εν λόγω αρχείων δεν αλλοιώθηκε κατά την μεταφόρτωση (download/upload) τους από και προς το νέφος. Στο επόμενο υποκεφάλαιο γίνεται μία συγκέντρωση των αποτελεσμάτων της δικανικής εξέτασης της υπηρεσίας νέφους Google Drive.

8.6. Σύνοψη δικανικής εξέτασης

Στο κεφάλαιο 8 πραγματοποιήθηκε εγκληματολογική εξέταση της υπηρεσίας νέφους Google Drive. Πιο συγκεκριμένα, εξετάστηκαν 18 εγκληματολογικά αντίγραφα, προερχόμενα από 9 εικονικές μηχανές που χρησιμοποιούσαν τις υπηρεσίες του Google Drive, είτε μέσω της εφαρμογής που προσφέρει στο λειτουργικό σύστημα Windows 10 (Backup and Sync from Google), είτε μέσω των δημοφιλέστερων φυλλομετρητών Ιστού για υπολογιστές (Google Chrome, Mozilla Firefox).

Ο σκοπός της εξέτασης ήταν ο εντοπισμός ευρημάτων που να αποδεικνύουν αφενός τη χρήση των υπηρεσιών νέφους και αφετέρου να προσδιορίζουν τη δραστηριότητα που πραγματοποίησε ο χρήστης μέσω αυτών. Επίσης, εξετάστηκε κατά πόσο επηρεάζει τα τεχνικά χαρακτηριστικά ενός αρχείου, η μεταφόρτωση του στο Google Drive.

Τα αποτελέσματα της δικανικής εξέτασης ήταν αρκετά ενθαρρυντικά. Εντοπίστηκαν αρκετά δεδομένα που να καταδεικνύουν τη χρήση του Google Drive αλλά και τις ενέργειες που πραγματοποίησε ο χρήστης μέσω αυτού. Συνολικά τα ευρήματα που προέκυψαν από τη δικανική εξέταση του Google Drive, παρουσιάζονται στο Παράρτημα Β. Στο επόμενο κεφάλαιο, θα γίνει επισκόπηση των ευρημάτων της πειραματικής διαδικασίας και θα εξεταστεί το αν αυτά επαρκούν για να απαντήσουν τις ερευνητικές ερωτήσεις της παρούσας διπλωματικής εργασίας.

Κεφάλαιο 9ο: Συμπεράσματα

9.1. Γενικά

Φτάνοντας στο τέλος της παρούσας διπλωματικής εργασίας και μελετώντας όλα όσα αναπτύχθηκαν ανωτέρω, κρίνεται απαραίτητο κάπου εδώ για αυτήν, να αξιολογηθεί ως προς την ικανοποίηση του σκοπού της. Υπενθυμίζεται ότι, απώτερος σκοπός της εργασίας είναι η ερευνητική συνεισφορά στην επιστήμη της ψηφιακής εγκληματολογίας. Προκειμένου να επιτευχθεί ο σκοπός αυτός, τέθηκαν ορισμένοι θεωρητικοί και ερευνητικοί στόχοι, οι οποίοι περιγράφονται στο κεφάλαιο 1. Στα υποκεφάλαια 9.2 και 9.3 που ακολουθούν, ελέγχεται το κατά πόσο αυτοί οι στόχοι εκπληρώθηκαν επιτυχώς.

Επιπρόσθετα, στα υπόλοιπα υποκεφάλαια αναφέρονται ορισμένα συμπεράσματα που εξήχθησαν από την παρούσα διπλωματική εργασία και σχετίζονται με το ευρύτερο αντικείμενο της ψηφιακής εγκληματολογίας στο νέφος.

9.2. Αξιολόγηση θεωρητικών στόχων διπλωματικής

Στο υποκεφάλαιο αυτό αξιολογούνται ξεχωριστά οι θεωρητικοί στόχοι της διπλωματικής. Κάτωθι παρατίθεται η αξιολόγηση για τον κάθε στόχο, ως εξής:
Θ.1. : *Ανάλυση των εννοιών της ψηφιακής εγκληματολογίας, του υπολογιστικού νέφους καθώς και της ψηφιακής εγκληματολογίας στο νέφος*.

Στο κεφάλαιο 2 επεξηγήθηκαν οι βασικές έννοιες και αρχές που διέπουν την ψηφιακή εγκληματολογία. Επιπρόσθετα, αποσαφηνίστηκε τι νοείται ψηφιακή εγκληματολογία στο νέφος. Στο κεφάλαιο 3 αναλύθηκαν τα χαρακτηριστικά του υπολογιστικού νέφους, τα μοντέλα υπηρεσίας με τα οποία διατίθεται, καθώς και τα μοντέλα ανάπτυξης του. Επομένως ο θεωρητικός στόχος Θ.1 εκπληρώθηκε επιτυχώς.

Θ.2. : *Επισκόπηση βασικών τεχνικών προκλήσεων και νομικών ζητημάτων που εμφανίζονται κατά την εγκληματολογική εξέταση στο νέφος*.

Στο κεφάλαιο 4 έγινε παρουσίαση των σημαντικότερων τεχνικών προκλήσεων που εμφανίζονται σε μία εγκληματολογική εξέταση στο νέφος. Επιπλέον, έγινε εκτενής αναφορά στα νομικά ζητήματα που εγείρει η εγκληματολογική εξέταση που λαμβάνει χώρα στο νέφος. Συνεπώς ο θεωρητικός στόχος Θ.2 κρίνεται εκπληρωμένος επιτυχώς.

Θ.3. : *Παρουσίαση των σημαντικότερων ευρημάτων που μπορούν να προκύψουν κατά τη δικανική εξέταση ψηφιακών δεδομένων, με έμφαση στα ευρήματα που σχετίζονται με τις υπηρεσίες νέφους.*

Στο κεφάλαιο 5 αναφέρθηκαν όλες οι ενδεχόμενες πηγές δεδομένων σε μία δικανική εξέταση στο νέφος. Συμπληρωματικά, αναπτύχθηκαν επαρκώς όλα τα διαφορετικά είδη ευρημάτων που μπορούν να προκύψουν από την εξέταση των εν λόγω πηγών. Ως εκ τούτου, ο θεωρητικός στόχος Θ.3 εκπληρώθηκε εξίσου επιτυχημένα.

Μετά από την επιτυχημένη ολοκλήρωση όλων των θεωρητικών στόχων της διπλωματικής εργασίας, γίνεται ακολούθως η αντίστοιχη εξέταση και στους ερευνητικούς στόχους αυτής.

9.3. Αξιολόγηση ερευνητικών στόχων διπλωματικής

Στο υποκεφάλαιο αυτό αξιολογούνται ξεχωριστά οι ερευνητικοί στόχοι της εργασίας. Υπενθυμίζεται ότι επίκεντρο της έρευνας της διπλωματικής εργασίας αποτελούσε, η διεξαγωγή εγκληματολογικής εξέτασης σε συσκευές που χρησιμοποιούν λειτουργικό σύστημα Windows 10 και δημοφιλείς υπηρεσίες υπολογιστικού νέφους, προς αναζήτηση ευρημάτων που σχετίζονται με τη χρήση των εν λόγω υπηρεσιών.

Στο Κεφάλαιο 6 επεξηγείται ακριβώς η μεθοδολογία της έρευνας, καθώς και οι συνθήκες διεξαγωγής της πειραματικής διαδικασίας της. Ακόμη, σχηματίστηκαν ερευνητικές ερωτήσεις προκειμένου η απάντηση τους να βοηθήσει στην ικανοποίηση των ερευνητικών στόχων του κεφαλαίου 1. Τέλος, επισημαίνονται οι περιορισμοί της έρευνας της παρούσας εργασίας. Σχετικά με τους ερευνητικούς στόχους αυτής, κάτωθι παρατίθεται η αξιολόγηση για τον κάθε στόχο, ως εξής:

Ε.1. : *Αναζήτηση δεδομένων που σχετίζονται με χρήση υπηρεσιών νέφους (μοντέλο SaaS), σε συσκευές που χρησιμοποιούν λειτουργικό σύστημα Windows 10 και δημοφιλείς εφαρμογές του μοντέλου αυτού (Dropbox και Google Drive)*.

Για τον ανωτέρω στόχο, σχηματίστηκε η ακόλουθη ερευνητική ερώτηση:

«*Υπάρχουν δεδομένα που να προκύπτουν από τη χρήση υπηρεσιών νέφους σε υπολογιστές που έχουν λειτουργικό σύστημα Windows 10 και τα οποία μπορούν να αποδείξουν τη χρήση των υπηρεσιών αυτών;*»

Η ανωτέρω ερώτηση οδηγεί με τη σειρά της σε δύο υποθέσεις:

- **Υπόθεση 1**: Δεν υπάρχουν εναπομείναντα ίχνη δεδομένων που να αποδεικνύουν τη χρήση υπηρεσιών νέφους και κατ' επέκταση να επιτρέπουν τον εντοπισμό περαιτέρω ευρημάτων σχετικών με αυτές (π.χ. εντοπισμός του παρόχου της υπηρεσίας νέφους, όνομα χρήστη, κ.τ.λ.).
- **Υπόθεση 2**: Υπάρχουν εναπομείναντα ίχνη δεδομένων που να αποδεικνύουν τη χρήση υπηρεσιών νέφους και τα οποία επιτρέπουν κατ' επέκταση τον εντοπισμό περαιτέρω ευρημάτων σχετικών με αυτές (π.χ. εντοπισμός του παρόχου της υπηρεσίας νέφους, όνομα χρήστη, κ.τ.λ.).

Στα κεφάλαια 7 και 8 έγινε δικανική εξέταση των υπηρεσιών νέφους Google Drive και Dropbox σε περιβάλλον Windows 10. Τα ίχνη δεδομένων που εντοπίστηκαν σε αυτή, αποδεικνύουν τη χρήση των υπηρεσιών νέφους. Επομένως, από τις υποθέσεις που έγιναν πριν από τη διεξαγωγή της εγκληματολογικής εξέτασης, η «Υπόθεση 2» επιβεβαιώνεται, ενώ η «Υπόθεση 1» απορρίπτεται. Αφού η «Υπόθεση 2» επιβεβαιώνεται, προκύπτουν οι κάτωθι υποερωτήσεις:

- *Τι δεδομένα παραμένουν στον υπολογιστή του χρήστη μετά την εγκατάσταση του λογισμικού της υπηρεσίας νέφους και έπειτα από τη χρήση του, για μεταφόρτωση (download/upload) αρχείων ή και άλλου είδους δραστηριότητα (προσπέλαση αρχείων, διαγραφή αρχείων, διαμοιρασμός με άλλους χρήστες, κ.τ.λ.); Επίσης, τι δεδομένα παραμένουν στον υπολογιστή του χρήστη μετά την απεγκατάσταση του λογισμικού της υπηρεσίας νέφους;*

Στα ευρήματα που παρουσιάστηκαν στα κεφάλαια 7 και 8, διαπιστώθηκε ότι τα δεδομένα που αποδεικνύουν τη χρήση της υπηρεσίας νέφους, βρίσκονται κατά κύριο λόγο στις βάσεις δεδομένων που χρησιμοποιεί το εν λόγω λογισμικό. Οι βάσεις δεδομένων δύνανται σε ορισμένες περιπτώσεις να ανακτηθούν, ακόμη και έπειτα από την απεγκατάσταση της εφαρμογής της υπηρεσίας νέφους. Τέλος, δεδομένα χρήσης των υπηρεσιών νέφους μπορούν να εντοπιστούν και σε αρχεία του λειτουργικού συστήματος των Windows 10. Αναλυτικά τα ευρήματα που προέκυψαν παρατίθενται στα Παραρτήματα Α και Β.

- *Τι δεδομένα παραμένουν στον υπολογιστή του χρήστη μετά τη χρήση υπηρεσιών νέφους μέσω ενός φυλλομετρητή Ιστού, για μεταφόρτωση (download/ upload) αρχείων ή και άλλου είδους δραστηριότητα (προσπέλαση αρχείων, διαγραφή αρχείων, διαμοιρασμός με άλλους χρήστες, κ.τ.λ.);*

Αντίστοιχα, τα δεδομένα που παραμένουν έπειτα από τη χρήση των υπηρεσιών νέφους, μέσω κάποιου φυλλομετρητή Ιστού, βρίσκονται κυρίως στις βάσεις δεδομέ-

νων του φυλλομετρητή Ιστού. Συμπληρωματικά όμως, ευρήματα μπορούν να εντοπιστούν και σε αρχεία του λειτουργικού συστήματος των Windows 10. Αναλυτικά τα ευρήματα που προέκυψαν παρατίθενται στα Παραρτήματα Α και Β.

- *Τι δεδομένα παραμένουν στην πτητική μνήμη του υπολογιστή του χρήστη, όταν χρησιμοποιείται το λογισμικό της εφαρμογής και τι δεδομένα όταν χρησιμοποιείται ένας φυλλομετρητή Ιστού;*

Τα ευρήματα που προέκυψαν από την εξέταση των μνημών RAM, σχετίζονται κυρίως με τα στοιχεία εισόδου του συνδεδεμένου λογαριασμού, στην υπηρεσία νέφους. Ειδικότερα, εντοπίστηκαν η διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιούσε, το όνομα χρήστη του και σε ορισμένες περιπτώσεις, ο κωδικός πρόσβασης του στην υπηρεσία νέφους. Πλέον έχουν απαντηθεί όλες οι επί μέρους υποερωτήσεις της «Υπόθεσης 2». Αυτό οδηγεί στην απάντηση της ερευνητικής ερώτησης 1 και κατ' επέκταση, στην ικανοποίηση του ερευνητικού στόχου [**Ε.1**].

Ε.2. : *Μελέτη των αλλαγών που επιφέρει η διακίνηση αρχείων μέσω των εφαρμογών αυτών, στα τεχνικά χαρακτηριστικά ενός αρχείου (metadata, hash, κ.τ.λ.).*

Για τον ανωτέρω στόχο, σχηματίστηκε η ακόλουθη ερευνητική ερώτηση:

«*Επηρεάζονται τα τεχνικά χαρακτηριστικά (περιεχόμενο, μεταδεδομένα, hash, κ.τ.λ.) ενός αρχείου κατά τη μεταφόρτωση (download/ upload) του μέσω μίας υπηρεσίας νέφους;*»

Η ανωτέρω ερώτηση οδηγεί με τη σειρά της σε δύο υποθέσεις:

- **Υπόθεση 1**: Τα τεχνικά χαρακτηριστικά ενός αρχείου δεν επηρεάζονται κατά τη μεταφόρτωση (download/ upload) του μέσω μίας υπηρεσίας νέφους.
- **Υπόθεση 2**: Τα τεχνικά χαρακτηριστικά ενός αρχείου επηρεάζονται κατά τη μεταφόρτωση (download/ upload) του μέσω μίας υπηρεσίας νέφους.

Στα κεφάλαια 7 και 8 έγινε δικανική εξέταση των υπηρεσιών νέφους Google Drive και Dropbox σε περιβάλλον Windows 10. Τα ίχνη δεδομένων που εντοπίστηκαν σε αυτή, αποδεικνύουν ότι μερικά από τα τεχνικά χαρακτηριστικά ενός αρχείου, επηρεάζονται από τη μεταφόρτωση του μέσω μίας υπηρεσίας νέφους. Συνεπώς, από τις υποθέσεις που έγιναν πριν από τη διεξαγωγή της εγκληματολογικής εξέτασης, η «Υπόθεση 2» επιβεβαιώνεται, ενώ η «Υπόθεση 1» απορρίπτεται. Αφού η «Υπόθεση 2» επιβεβαιώνεται, προκύπτει η κάτωθι υποερώτηση:

- Πώς επηρεάζονται οι χρονοσφραγίδες (timestamps) του αρχείου, το περιεχόμενο του και η αλφαριθμητική ταυτότητα μοναδικότητας (MD5) του, κατά τη διακίνηση του μέσω μίας υπηρεσίας νέφους;

Κατά τη διακίνηση των αρχείων μέσω μίας υπηρεσίας νέφους, δεν μεταβάλλεται το περιεχόμενο των αρχείων. Επίσης, δεν μεταβάλλεται η αλφαριθμητική ταυτότητα μοναδικότητας (MD5) τους. Αντίθετα, επισημαίνεται ότι μεταβάλλονται οι κάτωθι χρονοσφραγίδες των αρχείων:

- Ημερομηνία δημιουργίας στο σύστημα (File Created),
- Ημερομηνία τελευταίας προσπέλασης στο σύστημα (Last Accessed) και
- Ημερομηνία τελευταίας τροποποίησης στο σύστημα (Last Modified).

Αναλυτικά τα ευρήματα που προέκυψαν παρατίθενται στα Παραρτήματα Α και Β.

9.4. Σχολιασμός των αποτελεσμάτων της έρευνας της διπλωματικής εργασίας

Όπως παρατηρείται από όσα αναλύθηκαν στα προηγούμενα υποκεφάλαια, στην παρούσα εγκληματολογική εξέταση στο νέφος, προέκυψαν ευρήματα πολύ χρήσιμα για έναν ερευνητή. Τα δεδομένα που εντοπίστηκαν, αποδεικνύουν αρχικά τη χρήση υπηρεσιών νέφους. Επιπλέον, μπορούν να μαρτυρήσουν τη δραστηριότητα που πραγματοποίησε ο χρήστης μέσω αυτών, καθώς και να οδηγήσουν τον ερευνητή στην εξαγωγή ασφαλών συμπερασμάτων, όσον αφορά τις ενέργειες του χρήστη. Επομένως, χρησιμοποιώντας τα ευρήματα της παρούσας διπλωματικής εργασίας, ένας ερευνητής μπορεί με ευκολία να εντοπίσει αποδεικτικά δεδομένα που σχετίζονται με τις υπηρεσίες Google Drive και Dropbox, σε περιβάλλον Windows 10.

Ωστόσο, όπως έχει ήδη αναφερθεί άλλωστε, τα ευρήματα σε μία εγκληματολογική εξέταση στο νέφος διαφοροποιούνται σημαντικά ανάλογα με τις περιστάσεις (μοντέλο υπηρεσίας, νομικές προϋποθέσεις, τεχνικές δυσκολίες, κ.τ.λ.). Αυτό σημαίνει ότι, μία δικανική εξέταση που θα λάβει χώρα σε διαφορετικό μοντέλο υπηρεσίας του νέφους (π.χ. IaaS model), θα έχει διαφορετικά ευρήματα, διαφορετικές τεχνικές προκλήσεις και ενδεχομένως μπορεί να οδηγήσει σε εντελώς διαφορετικά συμπεράσματα. Επομένως, το γεγονός ότι σε αυτή την εξέταση εντοπίστηκαν αυτά ευρήματα, δεν συνεπάγεται απαραίτητα ότι σε κάθε εγκληματολογική εξέταση στο νέφος θα συμβαίνει κάτι τέτοιο.

Ένα ακόμη συμπέρασμα που προκύπτει από την έως τώρα ενασχόληση με την ψηφιακή εγκληματολογία στο νέφος, είναι ότι τα περισσότερα από τα νομικά ζητήματα και τις τεχνικές προκλήσεις του Κεφαλαίου 4, εξακολουθούν έως και σήμερα να

μην έχουν επιλυθεί. Η επίλυση τους θεωρείται αναγκαία και θα οδηγήσει σε πιο πλήρεις εγκληματολογικές εξετάσεις των αξιοποίνων πράξεων που λαμβάνουν χώρα στο νέφος. Ενδεικτικά στο επόμενο υποκεφάλαιο, αναφέρονται δύο από τα πιο δισεπίλυτα προβλήματα.

9.5. Ζητήματα που παραμένουν προς διερεύνηση

Το σημαντικότερο νομικό ζήτημα που μέχρι και σήμερα δεν έχει επιλυθεί, είναι αυτό των πολλαπλών ενοικιαστών στο νέφος. Όπως αναλύθηκε στο κεφάλαιο 4.2., ακόμα και να εντοπιστούν τα επίμαχα ψηφιακά πειστήρια που εμπλέκονται στην αξιόποινη πράξη που εξετάζεται, η κατάσχεση τους δεν είναι εύκολο να πραγματοποιηθεί. Αυτό συμβαίνει γιατί το συγκεκριμένο ψηφιακό πειστήριο εξυπηρετεί αναμφίβολα και άλλους χρήστες εκτός από τον ύποπτο χρήστη και επομένως με την κατάσχεση του, παραβιάζονται τα δικαιώματα αλλά και η ιδιωτικότητα των υπόλοιπων χρηστών. Η επίλυση του εν λόγω νομικού ζητήματος, θα βοηθήσει τα μέγιστα τις Διωκτικές Αρχές.

Από την άλλη μεριά, όσον αφορά τις τεχνικές προκλήσεις για τις οποίες δεν έχει βρεθεί ακόμα λύση, τότε αυτή που ξεχωρίζει από τις υπόλοιπες είναι τα πτητικά δεδομένα που υπάρχουν στο νέφος. Όπως επεξηγήθηκε και στο κεφάλαιο 4.3., η φύση αυτή των δεδομένων που υπάρχουν στο νέφος αποτελεί πολλές φορές πρόβλημα για τον ερευνητή, αφού πολύτιμα αποδεικτικά δεδομένα δύναται να εξαφανιστούν με το που τερματιστεί η λειτουργία της εικονικής μηχανής που τα περιέχει. Είναι πολύ ενδιαφέρον να βρεθεί ένας τρόπος ο οποίος θα επιτρέπει την συλλογή των πτητικών δεδομένων στο νέφος, αλλά παράλληλα δεν θα παραβιάζει τα δικαιώματα των χρηστών του.

9.6. Μελλοντική ενασχόληση

Συνοψίζοντας, αναφέρεται ότι η παρούσα διπλωματική εργασία, δύναται να αποτελέσει σύμμαχο για κάθε ερευνητή που επιθυμεί να ασχοληθεί με την εγκληματολογική εξέταση στο νέφος. Για όποιον επιθυμεί να ερευνήσει περαιτέρω τη συγκεκριμένη θεματική περιοχή, προτείνεται η εξέταση παρόμοιων υπηρεσιών νέφους σε περιβάλλον MacOS, Android ή/και iOS.

Βιβλιογραφία

A. Amirullah, I. Riadi and A. Luthfi, 2016, Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System, 1-7, [Journal Article], 10.5120/ijca2016907696, http://www.ijcaonline.org/archives/volume143/number1/amirullah-2016-ijca-907696.pdf, (Accessed 2019-05-23)

A. Antwi-Boasiako and H. Venter, G. Peterson and S. Shenoi, 2017, A Model for Digital Evidence Admissibility Assessment, 23-38, [Conference Proceedings], DOI: 10.1007/978-3-319-67208-3_2, http://link.springer.com/10.1007/978-3-319-67208-3_2, (Accessed 2018-11-15)

M. Arafat, B. Mondal and S. Rani, 2017, Technical Challenges of Cloud Forensics and Suggested Solutions, 1142-1149, [Journal Article], 10.14299/ijser.2017.08.004, https://www.ijser.org/onlineResearchPaperViewer.aspx?Technical-Challenges-of-Cloud-Forensics-and-Suggested-Solutions.pdf, (Accessed 2018-12-12)

CapitalNetworkSolutions, n.d., What exactly is volatile data, [Web Page], http://www.computerforensicsspecialists.co.uk/blog/what-is-volatile-datahttp://www.computerforensicsspecialists.co.uk/blog/what-is-volatile-data, (Accessed 2019-01-08)

B. Carrier, 2003, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, 12, [Journal Article], (Accessed 2019-06-01)

CCleaner, n.d., CCleaner Professional | Try the world's most trusted PC cleaner, free!, [Web Page], https://www.ccleaner.com/ccleanerhttps://www.ccleaner.com/ccleaner, (Accessed 2019-05-17)

M. S. Chang, 2016, Forensic Analysis of Google Drive on Windows, 8, [Journal Article], http://ijiset.com/vol3/v3s8/IJISET_V3_I8_44.pdfhttp://ijiset.com/vol3/v3s8/IJISET_V3_I8_44.pdf, (Accessed 2019-27-05)

H. Chung, J. Park, S. Lee and C. Kang, 2012, Digital Forensic Investigation of Cloud Storage Services, 81–95, [Journal Article], 10.1016/j.diin.2012.05.015, https://linkinghub.elsevier.com/retrieve/pii/S1742287612000400, (Accessed 2019-05-23)

CRU-INC, n.d., Logical Imaging, [Blog], https://www.cru-inc.com/data-protection-topics/logical-imaging/https://www.cru-inc.com/data-protection-topics/logical-imaging/, (Accessed 2019-05-31)

R. Dave, N. Mistry and M. Dahiya, 2014, Volatile Memory Based Forensic Artifacts & Analysis, [Journal Article], https://www.researchgate.net/publication/286321859_Volatile_Memory_Based_Forensic_Artifacts_Analysishttps://www.researchgate.net/publication/286321859_Volatile_Memory_Based_Forensic_Artifacts_Analysis, (Accessed 2019-05-15)

M. Destefani Neto, 2014, A brief history of cloud computing, [Web Page], https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/, (Accessed 2018-12-03)

DigitalCorpora, n.d., Digital Corpora, computer forensics education research, [Blog], https://digitalcorpora.org/https://digitalcorpora.org/, (Accessed 2019-05-19)

Dropbox, 2019, Dropbox, [Web Page], https://www.dropbox.com/https://www.dropbox.com/, (Accessed 2019-05-23)

X. Du, N.-A. Le-Khac and M. Scanlon, 2017, Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, [Conference Proceedings], https://www.researchgate.net/profile/Mark_Scanlon/publication/316788671_Evaluation_of_Digital_Forensic_Process_Models_with_Respect_to_Digital_Forensics_as_a_Service/links/5911a9e40f7e9b70f4803d54/Evaluation-of-Digital-Forensic-Process-Models-with-Respect-to-Digital-Forensics-as-a-Service.pdfhttps://www.researchgate.net/profile/Mark_Scanlon/publication/316788671_Evaluation_of_Digital_Forensic_Process_Models_with_Respect_to_Digital_Forensics_as_a_Service/links/5911a9e40f7e9b70f4803d54/Evaluation-of-Digital-Forensic-Process-Models-with-Respect-to-Digital-Forensics-as-a-Service.pdf, (Accessed 2019-15-05)

M. Epifani, 2013, Cloud Storage Forensics, 81, [Journal Article], https://digital-forensics.sans.org/summit-archives/Prague_Summit/Cloud_Storage_Forensics_Mattia_Eppifani.pdfhttps://digital-forensics.sans.org/summit-archives/Prague_Summit/Cloud_Storage_Forensics_Mattia_Eppifani.pdf, (Accessed 2019-19-05)

C. Federici, 2014, Cloud Data Imager: A unified answer to remote acquisition of cloud storage areas, 30-42, [Journal Article], 10.1016/j.diin.2014.02.002, https://linkinghub.elsevier.com/retrieve/pii/S174228761400005X, (Accessed 2019-05-23)

ForensicsWiki, 2015, Dropbox - ForensicsWiki, [Web Page], https://forensicswiki.org/wiki/Dropboxhttps://forensicswiki.org/wiki/Dropbox, (Accessed 2019-05-19)

Gartner, 2018, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018, [Web Page],

https://www.gartner.com/newsroom/id/3871416https://www.gartner.com/newsroom/id/3871416, (Accessed 2018-11-11)

GoogleDrive, 2019, Google Drive - Cloud Storage και αντίγραφα ασφαλείας για το Photos, τα Έγγραφα και πολλά άλλα, [Web Page], www.google.com/intl/el_ALL/drive/www.google.com/intl/el_ALL/drive/, (Accessed 2019-05-23)

T. Grance, S. Chevalier, K. K. Scarfone and H. Dang, 2006, Guide to Integrating Forensic Techniques into Incident Response | NIST, [Journal Article], https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-responsehttps://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response, (Accessed 2019-05-15)

O. A. a. Y. Gubanov, 2013, Catching the Ghost: How to Discover Ephemeral Evidence through Live RAM Analysis, [Magazine Article], https://www.forensicmag.com/article/2013/05/catching-ghost-how-discover-ephemeral-evidence-through-live-ram-analysishttps://www.forensicmag.com/article/2013/05/catching-ghost-how-discover-ephemeral-evidence-through-live-ram-analysis, (Accessed 2019-05-15)

imageforensicexpert, n.d., Digital Image Authentication, Edit Detection, [Blog], (Accessed 2019-05-31)

E.-E. ISO/IEC, 2016, EVS-EN ISO/IEC 27037:2016 - Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012), [Report], https://www.evs.ee/products/evs-en-iso-iec-27037-2016https://www.evs.ee/products/evs-en-iso-iec-27037-2016, (Accessed 2019-05-15)

M. James and P. Szewczyk, 2017, Jurisdictional issues in cloud forensics, [Conference Proceedings], https://ro.ecu.edu.au/ecuworkspost2013/3792https://ro.ecu.edu.au/ecuworkspost2013/3792, (Accessed 2019-15-05)

H. Kaur and G. Singh, 2016, Volatile Memory Forensics: A Legal Perspective, 11-15, [Journal Article], 10.5120/ijca2016912276, http://www.ijcaonline.org/archives/volume155/number3/mann-2016-ijca-912276.pdf, (Accessed 2019-05-15)

O. Leroux, 2004, Legal admissibility of electronic evidence, 193-220, [Journal Article], 10.1080/1360086042000223508, https://doi.org/10.1080/1360086042000223508, (Accessed 2019-05-15)

J. Lewis, 2018, Economic Impact of Cybercrime, [Report], https://www.csis.org/analysis/economic-impact-cybercrimehttps://www.csis.org/analysis/economic-impact-cybercrime, (Accessed 2019-05-15)

S. Liles, M. Rogers and M. Hoebich, 2009, A Survey of the Legal Issues Facing Digital Forensic Experts, 267-276, [Conference Proceedings], 10.1007/978-3-642-04155-6_20, https://www.researchgate.net/publication/221352825_A_Survey_of_the_Legal_Issues_Facing_Digital_Forensic_Experts, (Accessed 2019-05-15)

MagnetForensics, n.d., Magnet AXIOM - Digital Investigation Platform, [Web Page], https://www.magnetforensics.com/products/magnet-axiom/https://www.magnetforensics.com/products/magnet-axiom/, (Accessed 2019-05-17)

R. Malik, N. Shashidhar and L. Chen, 2015, Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform, 6, [Journal Article], https://pdfs.semanticscholar.org/2729/7bf3d53097d95d465203069b8231c20e5c77.pdfhttps://pdfs.semanticscholar.org/2729/7bf3d53097d95d465203069b8231c20e5c77.pdf, (Accessed 2019-05-15)

B. Martini and K.-K. R. Choo, 2012, An integrated conceptual digital forensic framework for cloud computing, 71–80, [Journal Article], 10.1016/j.diin.2012.07.001, http://linkinghub.elsevier.com/retrieve/pii/S174228761200059X, (Accessed 2018-11-21)

F. Marturana, G. Me and S. Tacconi, 2012, A Case Study on Digital Forensics in the Cloud, 111-116, [Conference Proceedings], 10.1109/CyberC.2012.26, http://ieeexplore.ieee.org/document/6384952/, (Accessed 2019-05-23)

R. McKemmish, 1999, What Is Forensic Computing?, 6, [Conference Proceedings], https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=179200https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=179200, (Accessed 2019-05-15)

S. Mehreen and B. Aslam, 2015, Windows 8 cloud storage analysis: Dropbox forensics, 312-317, [Conference Proceedings], 10.1109/IBCAST.2015.7058522, http://ieeexplore.ieee.org/document/7058522/, (Accessed 2019-05-23)

P. M. Mell and T. Grance, 2011, The NIST Definition of Cloud Computing, [Journal Article], https://www.nist.gov/publications/nist-definition-cloud-computinghttps://www.nist.gov/publications/nist-definition-cloud-computing, (Accessed 2019-05-15)

J. Milagre and M. Caiado, 2013, Cloud Computing Forensics. Best Practice and Challenges for Process Efficiency of Investigations and Digital Forensics, 18-26,

[Conference Proceedings], 10.5769/C2013003, http://www.icofcs.org/2013/papers-published-003.html, (Accessed 2018-11-22)

L. Mitrou and M. Karyda, 2007, Internet Forensics: Legal and Technical Issues, 3-12, [Conference Proceedings], 10.1109/WDFIA.2007.4299368, https://www.researchgate.net/profile/Lilian_Mitrou/publication/4273820_Internet_Forensics_Legal_and_Technical_Issues/links/55ac70f608ae815a042b0db8/Internet-Forensics-Legal-and-Technical-Issues.pdf, (Accessed 2019-05-01)

L. Mitrou, N. Marangos and P. Rizomiliotis, 2012, Digital forensics in the Cloud Computing Era, 775-780, [Conference Proceedings], 10.1109/GLOCOMW.2012.6477673, http://ieeexplore.ieee.org/document/6477673/, (Accessed 2018-11-21)

J. Norman, n.d., Probably the First U. S. Legislation against Computer Crimes : HistoryofInformation.com, [Web Page], http://www.historyofinformation.com/detail.php?entryid=3888http://www.historyofinformation.com/detail.php?entryid=3888, (Accessed 2018-11-07)

F. Picasso, 2017, A sort of a toolkit to decrypt Dropbox Windows DBX files: dfirfpi/decwindbx, [Computer Program], (Accessed 2019-05-17 16:36:11)

D. Quick and K.-K. R. Choo, 2013, Dropbox analysis: Data remnants on user machines, 3-18, [Journal Article], 10.1016/j.diin.2013.02.003, https://linkinghub.elsevier.com/retrieve/pii/S174228761300011X, (Accessed 2019-05-23)

D. Quick and K.-K. R. Choo, 2014, Google Drive: Forensic analysis of data remnants, 179-193, [Journal Article], 10.1016/j.jnca.2013.09.016,

https://linkinghub.elsevier.com/retrieve/pii/S1084804513002051, (Accessed 2019-05-27)

D. Rathod, 2017, Google Drive Forensics, 136, [Journal Article], https://www.researchgate.net/profile/Digvijaysinh_Rathod6/publication/321534818_Google_Drive_Forensics/links/5a26cbb20f7e9b71dd0c7e52/Google-Drive-Forensics.pdfhttps://www.researchgate.net/profile/Digvijaysinh_Rathod6/publication/321534818_Google_Drive_Forensics/links/5a26cbb20f7e9b71dd0c7e52/Google-Drive-Forensics.pdf, (Accessed 2019-05-25)

D. Reilly, C. Wren and T. Berry, 2010, Cloud computing: Forensic challenges for law enforcement, 1-7, [Conference Proceedings], https://www.researchgate.net/publication/224208711_Cloud_computing_Forensic_challenges_for_law_enforcementhttps://www.researchgate.net/publication/224208711_Cloud_computing_Forensic_challenges_for_law_enforcement, (Accessed 2019-05-05)

M. Reith, C. Carr and G. Gunsch, 2002, The digital age can be characterized as the application of computer technology as a tool that enhances traditional methodologi, 12, [Journal Article], https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdfhttps://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf, (Accessed 2019-05-25)

K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, 2011a, Cloud Forensics, 35-46, [Conference Proceedings], 10.1007/978-3-642-24212-0_3, https://www.researchgate.net/profile/Tahar_Kechadi/publication/221352743_Cloud_Forensics/links/5a1fd8fd0f7e9b9d5e02e04c/Cloud-Forensics.pdf, (Accessed 2019-05-15)

K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, 2011b, Cloud forensics: An overview, [Journal Article], https://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000/Cloud-forensics-An-overview.pdfhttps://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000/Cloud-forensics-An-overview.pdf, (Accessed 2019-05-15)

N. Santos, 2015, Course Overview. Welcome! CSF: Forensics Cyber-Security. Fall 2015 Nuno Santos - PDF, [Web Page], https://docplayer.net/51218134-Course-overview-welcome-csf-forensics-cyber-security-fall-2015-nuno-santos.htmlhttps://docplayer.net/51218134-Course-overview-welcome-csf-forensics-cyber-security-fall-2015-nuno-santos.html, (Accessed 2019-05-31)

Simon, AcquireForensics, 2015, Google Chrome Browser Forensics – Analyze Chrome Data, [Blog], https://www.acquireforensics.com/blog/google-chrome-browser-forensics.htmlhttps://www.acquireforensics.com/blog/google-chrome-browser-forensics.html, (Accessed 2019-05-19)

S. Simou, C. Kalloniatis, H. Mouratidis and S. Gritzalis, 2015, A Meta-model for Assisting a Cloud Forensics Process, [Conference Proceedings], 10.1007/978-3-319-31811-0_11, https://www.researchgate.net/publication/305475214_A_Meta-model_for_Assisting_a_Cloud_Forensics_Process, (Accessed 2019-05-15)

O. Skulkin and I. Mikhaylov, 2018, Cloud Forensics: Google Drive – Cyber Forensicator, [Blog], https://cyberforensicator.com/2018/10/19/cloud-forensics-google-drive/https://cyberforensicator.com/2018/10/19/cloud-forensics-google-drive/, (Accessed 2019-05-27)

D. Spiekermann, T. Eggendorfer and J. Keller, 2015, Using network data to improve digital investigation in cloud computing environments, 98-105, [Conference Proceedings], 10.1109/HPCSim.2015.7237027, http://ieeexplore.ieee.org/document/7237027/, (Accessed 2019-02-20)

SQLiteBrowser, n.d., DB Browser for SQLite, [Web Page], https://sqlitebrowser.org/https://sqlitebrowser.org/, (Accessed 2019-05-17)

StatCounter, 2019, Desktop Browser Market Share Worldwide, [Web Page], http://gs.statcounter.com/browser-market-share/desktop/worldwidehttp://gs.statcounter.com/browser-market-share/desktop/worldwide, (Accessed 2019-05-15)

StatCounter, n.d., Operating System Market Share Worldwide, [Web Page], http://gs.statcounter.com/os-market-share/all/worldwide/2018http://gs.statcounter.com/os-market-share/all/worldwide/2018, (Accessed 2018-11-11)

M. Tenhunen, S. Jajodia, W. List, G. McGregor and L. Strous, 1997, The Integrity of Electronic Evidence, 153-186, [Book Section], 10.1007/978-0-387-35317-3_8, https://link.springer.com/content/pdf/10.1007%2F978-0-387-35317-3_8.pdf, (Accessed 2019-05-31)

TheTOC, 2018, Τα ψηφιακά πειστήρια στην υπηρεσία εξιχνίασης εγκλημάτων |thetoc.gr, [Web Page], https://www.thetoc.gr/koinwnia/article/ta-psifiaka-peistiria-stin-upiresia-eksixniasis-egklimatwnhttps://www.thetoc.gr/koinwnia/article/ta-psifiaka-peistiria-stin-upiresia-eksixniasis-egklimatwn, (Accessed 2019-05-31)

VMware, n.d., Windows VM | VMware Workstation Pro, [Web Page], https://www.vmware.com/products/workstation-

pro.htmlhttps://www.vmware.com/products/workstation-pro.html, (Accessed 2019-05-17)

C. Wilson, 2014, ACPO Good Practice Guide for Digital Evidence, [Web Page], https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/, (Accessed 2019-05-31)

S. Zawoad and R. Hasan, 2013, Digital Forensics in the Cloud, [Journal Article], https://www.researchgate.net/publication/260364240_Digital_Forensics_in_the_Cloudhttps://www.researchgate.net/publication/260364240_Digital_Forensics_in_the_Cloud, (Accessed 2019-05-15)

Α. Μανιτάκης, 2011, Η διάκριση των εξουσιών ως οργανωτική βάση του κράτους ή ως πολιτική αρχή, [Web Page], https://www.constitutionalism.gr/2002-i-diakrisi-twn-exoysiwn-ws-organwtiki-basi-toy-kra/https://www.constitutionalism.gr/2002-i-diakrisi-twn-exoysiwn-ws-organwtiki-basi-toy-kra/, (Accessed 2019-05-31)

Γ. Μπαμπινιώτης, 2012, ΛΕΞΙΚΟ ΤΗΣ ΝΕΑΣ ΕΛΛΗΝΙΚΗΣ ΓΛΩΣΣΑΣ / ΜΠΑΜΠΙΝΙΩΤΗΣ ΓΕΩΡΓΙΟΣ, 2210, [Book], https://www.politeianet.gr/books/9789608975156-mpampiniotis-georgios-kentro-lexikologias-lexiko-tis-neas-ellinikis-glossas-199857https://www.politeianet.gr/books/9789608975156-mpampiniotis-georgios-kentro-lexikologias-lexiko-tis-neas-ellinikis-glossas-199857, (Accessed 2019-05-15)

Νόμος 4267/2014 - ΦΕΚ 137/Α/12-6-2014, [Generic], https://www.e-nomothesia.gr/kat-anilikoi/n-4267-2014.htmlhttps://www.e-nomothesia.gr/kat-anilikoi/n-4267-2014.html, (Accessed 2019-05-15)

Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679 | Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, [Web Page], (Accessed 2019-01-28)

Σ.-Α. Πριλή, 2018, Η παράνομη πρόσβαση σε πληροφοριακό σύστημα κατ' αρ. 370 Γ § 2 Ποινικού Κώδικα- «Hacking», 82, [Thesis], https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/2694400/theFile https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/2694400/theFile, (Accessed 2019-05-15)

Παράρτημα Α

Ευρήματα που προέκυψαν κατά την εξέταση της υπηρεσίας νέφους Dropbox		
Τρόπος Χρήσης	**Είδος Αρχείου/ Αρχείο**	**Περιγραφή**
Windows Application	Windows Event logs, .LNK files, Windows Registry, Prefetch Files	-Πότε εγκαταστάθηκε η εφαρμογή του νέφους -Πότε έτρεξε τελευταία φορά το λογισμικό και πόσες φορές συνολικά
	Web History (Edge)	Από τα URLs προέκυψαν εγγραφές σχετικές με: -Δημιουργία νέων αρχείων - Προβολή συγκεκριμένων αρχείων
	Recycle Bin	-Διαγραφή αρχείων
	Log	-Στο αρχείο καταγραφής με ονομασία «info.son», στη διαδρομή *C:\Users\<username>\AppData\Local\Dropbox, βρέθηκε το αναγνωριστικό της εγκατάστασης*
	Βάση δεδομένων Config.dbx	Περιλαμβάνει δεδομένα όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στην εφαρμογή Dropbox
	Βάση δεδομένων Filecache.dbx	Περιέχει πληροφορίες για τα αρχεία που έχουν συγχρονιστεί, με το λογαριασμό του συνδεδεμένου χρήστη
	RAM memory	-Βρέθηκαν το email και το username του χρήστη
	Απεγκατάσταση με Windows Uninstall	-Βρέθηκε το Filecache.dbx και διάφορες εγγραφές στα Amcache,Windows Registry, κ.ά.
	Απεγκατάσταση με CCleaner	-Βρέθηκαν παρόμοιες εγγραφές στα Amcache,Windows Registry, κ.ά. όχι όμως και τα αρχεία των βάσεων δεδομένων
Mozilla Firefox	Βάσεις δεδομένων	Από τα URLs προέκυψαν εγγραφές σχετικές με: -Δημιουργία νέων αρχείων

	(Web history, cache κ.ά.)	-Προβολή αρχείων -«Κατέβασμα» αρχείων -Διαγραφή αρχείων
	RAM memory	-Βρέθηκαν τα στοιχεία εισόδου του χρήστη (email και το password)
Google Chrome	Βάσεις δεδομένων (Web history, cache κ.ά.)	Από τα URLs προέκυψαν εγγραφές σχετικές με: -Δημιουργία νέων αρχείων -Προβολή αρχείων -«Κατέβασμα» αρχείων -Διαγραφή αρχείων
	RAM memory	-Βρέθηκαν τα στοιχεία εισόδου του χρήστη (email και το password)
Μεταδεδομένα Αρχείων	Metadata	-Αλλάζουν οι χρονοσφραγίδες (σε επίπεδο file system και όχι του περιεχομένου των αρχείων) των αρχείων κατά τη μεταφόρτωση (download/upload) τους από και προς το νέφος -Η αλφαριθμητική ταυτότητα μοναδικότητας (MD5) του αρχείου παραμένει η ίδια πριν και μετά τη μεταφόρτωση (upload)

Παράρτημα Β

Ευρήματα που προέκυψαν κατά την εξέταση της υπηρεσίας νέφους Google Drive		
Τρόπος Χρήσης	**Είδος Αρχείου/ Αρχείο**	**Περιγραφή**
Windows Application	Windows Event logs, .LNK files, Windows Registry, Prefetch Files	-Πότε εγκαταστάθηκε η εφαρμογή του νέφους -Πότε έτρεξε τελευταία φορά το λογισμικό και πόσες φορές συνολικά
	Log	-Στο αρχείο καταγραφής με ονομασία «sync_log.log», στη διαδρομή *C:\Users\<username>\AppData\Local\Google \Drive, βρέθηκε το email που χρησιμοποιούσε ο χρήστης καθώς όλες οι ενέργειες στις οποίες προέβη μέσω της εφαρμογής*
	Recycle Bin	-Διαγραφή αρχείων
	Βάση δεδομένων snapshot.db	-Περιέχει πληροφορίες για τα αρχεία που έχουν συγχρονιστεί, με το λογαριασμό του συνδεδεμένου χρήστη. Περιλαμβάνει εντός του και τα δεδομένα που περιέχει η βάση δεδομένων cloud_graph.db

	Βάση δεδομένων cloud_graph.db	-Περιέχει πληροφορίες για τα αρχεία που έχουν συγχρονιστεί, με το λογαριασμό του συνδεδεμένου χρήστη. Τα δεδομένα του περιέχονται και στη βάση δεδομένων snapshot.db
	Βάση δεδομένων sync_config.db	-Περιλαμβάνει δεδομένα όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Google Drive
	Βάση δεδομένων global.db	-Περιλαμβάνει δεδομένα όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδεδεμένου λογαριασμού στο Google Drive
	RAM memory	-Βρέθηκαν τα στοιχεία εισόδου του χρήστη (email και το password)
	Απεγκατάσταση με Windows Uninstall	-Δεν βρέθηκαν οι βάσεις δεδομένων αλλά εντοπίστηκαν διάφορες εγγραφές στα Windows Registry, κ.ά.
	Απεγκατάσταση με CCleaner	-Βρέθηκαν παρόμοιες εγγραφές στα Amcache,Windows Registry, κ.ά.
Mozilla Firefox	Βάσεις δεδομένων (Web history, cache κ.ά.)	Από τα URLs προέκυψαν εγγραφές σχετικές με: -Επεξεργασία αρχείων -«Κατέβασμα» αρχείων
	RAM memory	-Βρέθηκαν τα στοιχεία εισόδου του χρήστη (email και το password)
Google Chrome	Βάσεις δεδομένων (Web history, cache κ.ά.)	Από τα URLs προέκυψαν εγγραφές σχετικές με: -Δημιουργία νέων αρχείων -Επεξεργασία αρχείων -Διαμοιρασμός αρχείων -Προβολή αρχείων -«Κατέβασμα» αρχείων
	Recycle Bin	-Διαγραφή αρχείων
	RAM memory	-Βρέθηκαν το email και το username του χρήστη
Μεταδεδομένα Αρχείων	Metadata	-Αλλάζουν οι χρονοσφραγίδες (σε επίπεδο file system και όχι του περιεχομένου των αρχείων) των αρχείων κατά τη μεταφόρτωση (download/ upload) τους από και προς το νέφος -Η αλφαριθμητική ταυτότητα μοναδικότητας (MD5) του αρχείου παραμένει η ίδια πριν και μετά τη μεταφόρτωση (upload)