ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΤΕΧΝΙΚΕΣ ANTI-FORENSICS»

Της φοιτήτριας
Μανούση Ηλέκτρα
Αρ. Μητρώου: 154487

Επιβλέπων
Ηλιούδης Χρήστος
Βαθμίδα: Καθηγητής

Ημερομηνία 31-05-2021

Τίτλος Δ.Ε.: Τεχνικές Anti-Forensics

Κωδικός Δ.Ε.: 20228

Ονοματεπώνυμο φοιτητή/των: Μανούση Ηλέκτρα

Ονοματεπώνυμο εισηγητή: Ηλιούδης Χρήστος

Ημερομηνία ανάληψης Δ.Ε.: 03-11-2020

Ημερομηνία περάτωσης Δ.Ε.: 31-05-2021

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η παρούσα διπλωματική εργασία έχει ως αντικείμενο τη μελέτη τεχνικών anti-forensics που είναι πιθανό να συναντήσει ένας ερευνητής κατά τη διεξαγωγή μιας εγκληματολογικής έρευνας ψηφιακών δεδομένων. Ο λόγος για τον οποίο επιλέχθηκε το συγκεκριμένο θέμα είναι το γεγονός ότι οι τεχνικές anti-forensics αποτελούν μία από τις σημαντικότερες προκλήσεις κατά τη διεξαγωγή ερευνών για τη διερεύνηση περιστατικών ασφάλειας ή άλλων ποινικών υποθέσεων. Παρόλο που υπάρχει σχετική βιβλιογραφία για την ανάλυση των τεχνικών anti-forensics πολλές φορές γίνεται ελάχιστη ή καμία αναφορά στους τρόπους αντιμετώπισής τους. Ζητούμενο της διπλωματικής εργασίας είναι η μελέτη του προβλήματος των τεχνικών anti-forensics, καθώς και τρόπων προσέγγισης και αντιμετώπισης αυτών.

Περίληψη

Μία από τις μεγαλύτερες προκλήσεις που καλούνται να αντιμετωπίσουν οι ερευνητές της ψηφιακής εγκληματολογίας είναι οι τεχνικές anti-forensics, δηλαδή τεχνικές που επηρεάζουν και συχνά παρεμποδίζουν την ερευνητική διαδικασία. Σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη αυτών των τεχνικών και η αναζήτηση τρόπων αντιμετώπισής τους. Η μελέτη των τεχνικών πραγματοποιείται, αρχικά, μέσα από την προσέγγισή τους σε θεωρητικό και, στη συνέχεια, σε πρακτικό επίπεδο με την παρουσίαση εργαλείων και πειραμάτων. Έπειτα, εξετάζονται μέθοδοι για την αντιμετώπισή τους, εστιάζοντας σε λειτουργίες του λειτουργικού συστήματος Windows που μπορούν να αξιοποιηθούν, καθώς και σε μη-τεχνικά μέσα, όπως η εκμετάλλευση πληροφοριών OSINT και η μελέτη του ανθρώπινου παράγοντα. Τέλος, εφαρμόζονται ορισμένοι από τους προτεινόμενους τρόπους αντιμετώπισης στη μελέτη περίπτωσης ενός σεναρίου υποκλοπής εμπιστευτικών δεδομένων. Τα βασικά συμπεράσματα τα οποία εξάγουμε μέσα από την έρευνά μας είναι η σημασία της ανάλυσης των συστημάτων σε λειτουργία και η εκμετάλλευση των λειτουργιών τους, καθώς και η ανάγκη επέκτασης της ερευνητικής διαδικασίας πέρα από τα προς ανάλυση ψηφιακά μέσα.

Abstract

«ANTI-FORENSICS TECHNIQUES»

«Electra Manousi»

One of the biggest challenges that digital forensic researchers face is anti-forensics techniques, that is, techniques that affect and often hinder the research process. The purpose of this thesis is to study these techniques and search for ways to overcome them. The study of the anti-forensics techniques is carried out, first, through approaching them on a theoretical and then on a practical level with the presentation of tools and experiments. Methods for dealing with them are then examined, focusing on features of the Windows operating system that can be utilized, as well as non-technical means, such as exploiting OSINT information and studying the human factor. Finally, some of the suggested countermeasures are applied in the case study of a confidential data breach scenario. The main conclusions we draw from our research are the importance of live analysis of computer systems and the exploitation of their functions, as well as the need to extend the research process beyond the digital media to be analyzed.

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, τον κύριο Χρήστο Ηλιούδη, για την εμπιστοσύνη που έδειξε στην επιλογή του θέματος και για τις χρήσιμες συμβουλές του στο κομμάτι της συγγραφής. Θα ήθελα, όμως, να τον ευχαριστήσω ιδιαίτερα για το εκπαιδευτικό του έργο, καθώς μέσα από τις εκδηλώσεις που διοργανώνει στα πλαίσια του μαθήματος 'Ασφάλεια Πληροφοριακών Συστημάτων', δίνει την ευκαιρία στους φοιτητές να γνωρίσουν κλάδους της επιστήμης της Κυβερνοασφάλειας. Έτσι, είχα την ευκαιρία και εγώ να γνωρίσω και να αγαπήσω την Ψηφιακή Εγκληματολογία. Επίσης θα ήθελα να ευχαριστήσω τη φίλη μου Γεωργία Χρυσοβαλάντα Κασσάρα για τις συμβουλές της σχετικά με τα νομικά ζητήματα που αναφέρονται στην εργασία. Πάνω απ' όλα, όμως, θα ήθελα να ευχαριστήσω τους γονείς μου οι οποίοι κάνουν τα πάντα για να στηρίξουν τα όνειρά μου.

Περιεχόμενα

Ευρετήριο σχημάτων

Ευρετήριο πινάκων

Εισαγωγή

Η ερευνητική περιοχή την οποία προσεγγίζει η παρούσα εργασία είναι η επιστήμη της Ψηφιακής Εγκληματολογίας (Digital Forensics), η οποία αποτελεί συνεχώς αναπτυσσόμενο κλάδο της Εγκληματολογικής Έρευνας (Forensics Science). Η Ψηφιακή Εγκληματολογία ασχολείται με τη διερεύνηση περιστατικών ασφάλειας, όπως οι επιθέσεις σε ψηφιακά συστήματα εταιρειών και οργανισμών, ώστε να αποδοθούν ευθύνες και να βελτιστοποιηθούν οι αμυντικοί μηχανισμοί για αποφυγή παρόμοιων περιστατικών στο μέλλον. Ωστόσο, η σημασία της ψηφιακής εγκληματολογίας δεν περιορίζεται μόνο στη διερεύνηση περιστατικών ασφάλειας. Με τη χρήση της τεχνολογίας πολλά "παραδοσιακά" εγκλήματα έχουν μεταφερθεί στον κυβερνοχώρο, όπως η τρομοκρατία, η παρενόχληση, η εμπορία ναρκωτικών, κ.α. Επιπλέον, από τη στιγμή που η τεχνολογία έχει κατακλύσει σχεδόν κάθε πτυχή της καθημερινότητάς μας, είναι δύσκολο να φανταστούμε ένα έγκλημα το οποίο να μην μπορεί να συσχετιστεί με ψηφιακά δεδομένα. Από την επικοινωνία του εγκληματία μέχρι και την τοποθεσία ή τη δραστηριότητά του, όλα αφήνουν ψηφιακά ίχνη.

Ένας παράγοντας που διαφοροποιεί την ψηφιακή εγκληματολογία από τους υπόλοιπους κλάδους της Εγκληματολογίας είναι η πτητικότητα των δεδομένων, καθώς και η ευαισθησία τους σε άμεσες μεταβολές. Η ευκολία τροποποίησης των ψηφιακών δεδομένων συχνά τα καθιστά αμφίβολα ως πειστήρια, επομένως είναι απαραίτητο να ακολουθούνται διαδικασίες για τη σωστή διαχείριση των ψηφιακών δεδομένων από τη συλλογή τους μέχρι και την παρουσίασή τους ως πειστήρια. Όμως, αυτή η ευαισθησία των ψηφιακών δεδομένων είναι και ο λόγος που οι τεχνικές anti-forensics αποτελούν ένα σημαντικό ζήτημα κατά τη διεξαγωγή ερευνών.

Η διάρθρωση της εργασίας ακολουθεί τα τρία βασικά στάδια επίλυσης ενός προβλήματος: τον προσδιορισμό και την κατανόηση του προβλήματος, την ανάλυση και την αναζήτηση κατάλληλων λύσεων. Έτσι, αρχικό στόχο της παρούσας διπλωματικής εργασίας αποτελεί ο προσδιορισμός των τεχνικών anti-forensics και οι επιπτώσεις που επιφέρουν στη διεξαγωγή ερευνών. Επόμενο στόχο αποτελεί η ανάλυση των τεχνικών anti-forensics, αρχικά, μέσα από μία θεωρητική προσέγγιση και στη συνέχεια μέσω της πρακτικής εφαρμογής ορισμένων τεχνικών, η οποία με τη σειρά της αποσκοπεί στον εντοπισμό των τεχνικών αυτών αλλά και στην τεχνική αντιμετώπισή τους, όταν αυτό είναι δυνατό. Ως τελικός στόχος την εργασίας τίθεται η μελέτη γενικότερων τρόπων αντιμετώπισης των μεθόδων anti-forensics.

Μέσα από την παρούσα εργασία καταφέραμε να προσδιορίσουμε με σαφήνεια τις τεχνικές anti-forensics και τον τρόπο με τον οποίο επηρεάζουν την εγκληματολογική ανάλυση ψηφιακών δεδομένων. Επιπλέον, με την πρακτική εφαρμογή ορισμένων κοινών τεχνικών, είδαμε ορισμένα χαρακτηριστικά τους, τα οποία θα πρέπει να λαμβάνονται υπόψη από τον ερευνητή, ώστε να είναι σε θέση να εντοπίσει τις τεχνικές ή να αποφύγει τυχόν παραλείψεις. Τέλος, αναδείξαμε τη χρησιμότητα ορισμένων λειτουργιών των Windows για την αντιμετώπιση των τεχνικών anti-forensics, καθώς και τη σημασία του ανθρώπινου παράγοντα, τόσο από τη μεριά του ερευνητή όσο και από τη μεριά του εγκληματία, ο οποίος σε πολλές περιπτώσεις παίζει καθοριστικό ρόλο στην έκβαση της ερευνητικής διαδικασίας.

Όσον αφορά την δομή της εργασίας, στο πρώτο κεφάλαιο γίνεται μία σύντομη εισαγωγή στην επιστήμη της ψηφιακής εγκληματολογίας. Ορίζεται η έννοια των anti-forensics και παρουσιάζονται μερικές από τις βασικότερες προκλήσεις στη διεξαγωγή διερεύνησης περιστατικών, καθώς πάνω σε

αυτές βασίζεται η αποτελεσματικότητα των τεχνικών anti-forensics. Στο δεύτερο κεφάλαιο περιγράφονται οι πιο κοινές τεχνικές anti-forensics ταξινομημένες σε τέσσερις ευρύτερες κατηγορίες που είναι η καταστροφή πειστηρίων, η απόκρυψη πειστηρίων, η απόκρυψη ιχνών και η επίθεση σε εργαλεία και διαδικασίες της έρευνας. Το τρίτο κεφάλαιο περιλαμβάνει την πρακτική εφαρμογή ορισμένων τεχνικών από κάθε κατηγορία, μέσα από την παρουσίαση παραδειγμάτων με χρήση εργαλείων και πειραμάτων. Θέμα του τέταρτου κεφαλαίου αποτελεί η παρουσίαση τρόπων αντιμετώπισης των τεχνικών anti-forensics, με τεχνικές αλλά και μη-τεχνικές προσεγγίσεις. Στο πέμπτο κεφάλαιο παρουσιάζεται μία μελέτη περίπτωσης όπου εφαρμόζονται ορισμένοι από τους τεχνικούς τρόπους αντιμετώπισης που παρουσιάστηκαν στο τέταρτο κεφάλαιο, ενώ, στο έκτο κεφάλαιο παρουσιάζονται τα συμπεράσματα τα οποία προέκυψαν μέσα από την εκπόνηση της παρούσας διπλωματικής εργασίας.

Κεφάλαιο 1 Ψηφιακή Εγκληματολογία και Anti-forensics

Εισαγωγή

Για να γίνει σαφής ο λόγος για τον οποίο οι τεχνικές anti-forensics επηρεάζουν την ψηφιακή εγκληματολογία είναι σημαντικό να οριστούν αρχικά οι έννοιες και οι στόχοι της ψηφιακής εγκληματολογίας και των anti-forensics. Έτσι, σε αυτό το κεφάλαιο παρουσιάζονται τα στάδια της ερευνητικής διαδικασίας και οι τρόποι με τους οποίους οι τεχνικές αυτές επηρεάζουν κάθε ένα από αυτά τα στάδια. Βέβαια, η επιτυχία των τεχνικών anti-forensics βασίζεται και σε ορισμένες προκλήσεις που αντιμετωπίζει γενικότερα η ψηφιακή εγκληματολογία.

1.1 Ψηφιακή εγκληματολογία

Ή ψηφιακή εγκληματολογία αποτελεί κλάδο της επιστήμης της Εγκληματολογίας. Ως Εγκληματολογία ορίζεται η "Εφαρμογή μεθόδων των φυσικών και θετικών επιστημών σε θέματα ποινικού και αστικού δικαίου". Ένας ορισμός της ψηφιακής εγκληματολογίας δόθηκε από τον Ken Zatyko το 2008 ως εξής:

«*Η εφαρμογή της επιστήμης των υπολογιστών και ερευνητικών διαδικασιών για έναν νομικό σκοπό που περιλαμβάνει την ανάλυση ψηφιακών στοιχείων ύστερα από κατάλληλη αναζήτηση, διαδικασία καταγραφής (chain of custody), έλεγχο εγκυρότητας με μαθηματικούς υπολογισμούς, χρήση επικυρωμένων εργαλείων, επαναληψιμότητα, αναφορά και πιθανή έκθεση εμπειρογνώμονα*» [1].

Ο παραπάνω ορισμός συνοψίζει επαρκώς την έννοια της ψηφιακής εγκληματολογίας, καθώς περιλαμβάνει τα βασικά στάδια και τις διαδικασίες που πρέπει να ακολουθούνται κατά τη διεξαγωγή της έρευνας. Επιπλέον, διακρίνεται ο βασικός στόχος της ο οποίος αποτελεί την εύρεση ψηφιακών δεδομένων που στη συνέχεια θα αξιοποιηθούν ως πειστήρια σε ποινικές έρευνες μέσα από την εφαρμογή μιας νομικά αποδεκτής επιστημονικής μεθοδολογίας. Η εξέταση ψηφιακών πειστηρίων δεν περιορίζεται μόνο στην εξιχνίαση ηλεκτρονικών εγκλημάτων, αλλά και σε ποινικές και αστικές υποθέσεις όπου τα ψηφιακά δεδομένα κατέχουν συμπληρωματικό (και πολλές φορές μείζονα) ρόλο [2]. Σε αστικές και ποινικές υποθέσεις τα ψηφιακά δεδομένα ενδιαφέροντος είναι κατά κύριο λόγο συνομιλίες, ηλεκτρονική αλληλογραφία, μηνύματα SMS, δεδομένα γεωγραφικού εντοπισμού και πληροφορίες ελεύθερα διαθέσιμες στο Διαδίκτυο και ειδικότερα σε μέσα κοινωνικής δικτύωσης. Παρακάτω παρουσιάζονται οι βασικοί τύποι ηλεκτρονικού εγκλήματος:

- Γνήσια ηλεκτρονικά εγκλήματα (σχετίζονται άμεσα με τον Κυβερνοχώρο) [3]
  - Άνευ δικαιώματος πρόσβαση σε υπολογιστικά συστήματα με στόχο τη διαχείριση του συστήματος, την παρεμπόδιση της λειτουργίας του ή την πρόσβαση σε δεδομένα για την υποκλοπή, τροποποίηση ή καταστροφή αυτών.
  - Επιθέσεις άρνησης εξυπηρέτησης, δηλαδή, αναστολή της δυνατότητας ενός εξυπηρετητή να απαντήσει σε αιτήματα πελατών. Αυτό επιτυγχάνεται με την

εξάντληση των διαθέσιμων πόρων του εξυπηρετητή υπερφορτώνοντάς τον με περισσότερα αιτήματα από αυτά που μπορεί να διαχειριστεί.

- ➢ Εισαγωγή κακόβουλου λογισμικού σε κάποιο υπολογιστικό σύστημα με σκοπό τη παρεμβολή στη λειτουργικότητα του συστήματος ή στα δεδομένα που βρίσκονται σε αυτό. Οι βασικοί τύποι κακόβουλου λογισμικού, βάσει του τρόπου με τον οποίο διασπείρονται είναι οι ιοί, οι οποίοι πρέπει να εκτελεστούν από τον χρήστη ή το σύστημα για να μολύνουν αρχεία και συστήματα, τα σκουλήκια, τα οποία αναπαράγονται ανεξάρτητα, και οι δούρειοι ίπποι, οι οποίοι εγκαθίστανται από τον χρήστη καθώς αποτελούν φαινομενικά μη-κακόβουλα προγράμματα.
- ➢ Spamming, δηλαδή μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας, εμπορικού ή ενημερωτικού χαρακτήρα, σε μεγάλο αριθμό χρηστών χωρίς την άδειά τους.
- ➢ Επιθέσεις σε δικτυακούς τόπους με στόχο την αλλοίωση του περιεχομένου τους. Οι επιθέσεις αυτές αποσκοπούν στην προβολή ενός πολιτικού, θρησκευτικού ή κοινωνικού μηνύματος, ή την προσβολή του κατόχου της ιστοσελίδας.
- ➢ Εξαπάτηση χρηστών μέσω φαινομενικά αξιόπιστων οντοτήτων (π.χ. τράπεζες, ασφαλιστικές εταιρείες) με στόχο την υποκλοπή προσωπικών ή οικονομικών δεδομένων. Αυτού του είδους η απάτη ονομάζεται phishing (ηλεκτρονικό ψάρεμα).
- ➢ Πειρατεία λογισμικού, δηλαδή η άνευ δικαιώματος παραγωγή, πώληση, διανομή ή διάθεση προγραμμάτων υπολογιστή.
- ➢ Υποκλοπή μη-δημόσιων ψηφιακών δεδομένων από ένα υπολογιστικό σύστημα με φυσική πρόσβαση σε αυτό, απομακρυσμένα ή με εγκατάσταση κακόβουλου λογισμικού.

❖ Εγκλήματα με χρήση Ηλεκτρονικού Υπολογιστή [4]

- ➢ Απάτη στο διαδίκτυο με υποσχόμενες χρηματικές αμοιβές μετά από καταβολή χρηματικού ποσού ή οικονομικών δεδομένων.
- ➢ Κλοπή ταυτότητας μέσα από τη συλλογή προσωπικών ή/και οικονομικών δεδομένων ενός ατόμου (συνήθως με υποκλοπή αυτών) με σκοπό την προσποίηση του ατόμου για πρόσβαση σε υπηρεσίες ή πρόκληση οικονομικής ή προσωπική βλάβης στο θύμα.
- ➢ Πλαστογραφία, δηλαδή άνευ δικαιώματος εισαγωγή, αλλοίωση ή διαγραφή ψηφιακών δεδομένων που έχουν ως αποτέλεσμα την παραγωγή μη αυθεντικών πληροφοριών με σκοπό να αξιοποιηθούν ως αυθεντικές για νόμιμους σκοπούς.
- ➢ Ξέπλυμα χρήματος, δηλαδή απόκρυψη παράνομου ή αδήλωτου εισοδήματος, το οποίο επωφελείται από την ανωνυμία που παρέχει το διαδίκτυο και το κρυπτονόμισμα.
- ➢ Διακίνηση ναρκωτικών, οργάνων ακόμα και ανθρώπων.

- ➢ Παραγωγή, διανομή, διάθεση, προμήθεια και κατοχή παιδικής πορνογραφίας μέσω ενός υπολογιστικού συστήματος.
- ➢ Διαδικτυακή τρομοκρατία η οποία έχει πολιτικά ή ιδεολογικά κίνητρα, και στοχοποιεί υπηρεσίες, οργανισμούς και βιομηχανίες, προκαλώντας βλάβη σε υπολογιστικά συστήματα ή καταστρέφοντας και υποκλέπτοντας ψηφιακά δεδομένα.
- ➢ Παρενόχληση ατόμων μέσω της προσβολής, της απειλής ή του εκβιασμού αυτών.

Ο όρος «υπόθεση» καθ'όλη τη διάρκεια της εργασίας θα καλύπτει τόσο τη διερεύνηση ηλεκτρονικών εγκλημάτων όσο και αστικών και ποινικών υποθέσεων.

1.1.1 Στάδια ερευνητικής διαδικασίας

Παρόλο που έχουν προταθεί διάφορες μεθοδολογίες για τη διεξαγωγή της ερευνητικής διαδικασίας η πλειοψηφία αυτών συμπεριλαμβάνει τέσσερα βασικά στάδια, τα οποία είναι η συλλογή ψηφιακών δεδομένων, η εξέτασή τους, η ανάλυσή τους και η σύνταξη αναφοράς [5].

Στο πρώτο στάδιο της έρευνας τα δεδομένα συλλέγονται από ψηφιακές συσκευές και μέσα αποθήκευσης ακολουθώντας πρακτικές που εξασφαλίζουν την ποιότητα των δεδομένων - δηλαδή τη συλλογή δεδομένων που σχετίζονται με την έρευνα - και την ακεραιότητά τους, η οποία πρέπει να ελέγχεται καθ'όλη τη διάρκεια της έρευνας. Σε υπολογιστικές συσκευές (προσωπικοί υπολογιστές, κινητά τηλέφωνα, tablets) η συλλογή δεδομένων μπορεί να γίνει από τη συσκευή ενώ βρίσκεται σε λειτουργία για συλλογή πτητικών δεδομένων (δεδομένα που χάνονται όταν απενεργοποιηθεί το σύστημα) από καταχωρητές και τη μνήμη RAM, από απενεργοποιημένη συσκευή για συλλογή μη πτητικών δεδομένων από μέσα μόνιμης αποθήκευσης, ή απομακρυσμένα όταν η συσκευή είναι συνδεδεμένη στο διαδίκτυο [6].

Το δεύτερο στάδιο αποτελεί η εξέταση των δεδομένων που έχουν συλλεχθεί. Σε αυτό το στάδιο γίνεται η αναζήτηση και ανάκτηση δεδομένων που σχετίζονται με το υπό διερεύνηση περιστατικό ασφάλειας ή την υπόθεση [7]. Τα σχετικά δεδομένα στη συνέχεια αναλύονται στο στάδιο της ανάλυσης, ώστε μέσα από μεταξύ τους συσχετίσεις και τη δημιουργία χρονοδιαγραμμάτων να εξαχθούν συμπεράσματα τα οποία θα χρησιμοποιηθούν ως πειστήρια για την επιβεβαίωση ή την απόρριψη μιας αρχικής εικασίας [7].

Το τελευταίο, και κρισιμότερο στάδιο κατά τη διεξαγωγή μιας έρευνας, περιλαμβάνει τη σύνταξη αναφοράς στην οποία συνοψίζονται και επεξηγούνται τα συμπεράσματα της έρευνας [8]. Στην αναφορά πρέπει να εξηγούνται με σαφήνεια τα ευρήματα της έρευνας ώστε να είναι κατανοητά και από άτομα που δεν διαθέτουν τις απαραίτητες τεχνικές γνώσεις (π.χ. δικαστικοί υπάλληλοι, δικηγόροι, διευθυντές εταιρειών), και να αποδεικνύεται η εγκυρότητα των συμπερασμάτων, καθώς σε αντίθετη περίπτωση είναι πιθανόν να αμφισβητηθούν και να απορριφθούν, ιδίως αν παρουσιαστούν ως πειστήρια στο δικαστήριο [9].

1.1.2 Κλάδοι Ψηφιακής Εγκληματολογίας

Η ψηφιακή εγκληματολογία αναγνωρίστηκε ως επιστήμη στις αρχές του 2000, καθώς πλέον υπήρχαν καθιερωμένες διαδικασίες για τη διεξαγωγή ερευνών και κατάλληλη εκπαίδευση για τους ερευνητές [10]. Αρχικά, ο όρος *ψηφιακή εγκληματολογία* (digital forensics) ήταν συνώνυμος του όρου *εγκληματολογία υπολογιστών* (computer forensics) αφού οι ηλεκτρονικοί υπολογιστές ήταν η κύρια πηγή άντλησης ψηφιακών πειστηρίων αλλά και το κύριο μέσο τέλεσης ψηφιακών εγκλημάτων [10]. Στη συνέχεια, όμως, με την ανάπτυξη της τεχνολογίας τα ψηφιακά δεδομένα ήταν πλέον διασκορπισμένα και σε άλλες τεχνολογίες όπως κινητά τηλέφωνα, συσκευές του Διαδικτύου και έξυπνες συσκευές, με αποτέλεσμα ο όρος *εγκληματολογία υπολογιστών* να αποτελεί κλάδο της ευρύτερης επιστήμης ανάλυσης ψηφιακών πειστηρίων, της ψηφιακής εγκληματολογίας. Έτσι, ανάλογα με το μέσο ή το αντικείμενο που αναλύεται και εξειδικεύεται η έρευνα έχουν προκύψει οι παρακάτω βασικοί κλάδοι ψηφιακής εγκληματολογίας [11]:

- **Εγκληματολογία Υπολογιστών (Computer Forensics)** : Αντικείμενο της εγκληματολογίας υπολογιστών είναι η εξαγωγή και ανάλυση πειστηρίων από υπολογιστές και αποθηκευτικά μέσα.

- **Εγκληματολογία Κινητών Συσκευών (Mobile Forensics)** : Η εγκληματολογία κινητών συσκευών ασχολείται με την εξαγωγή ψηφιακών δεδομένων από κινητά τηλέφωνα, συσκευές tablet, συσκευές GPS και συσκευές PDA. Αποτελεί έναν πολύ σημαντικό κλάδο της ψηφιακής εγκληματολογίας, καθώς η χρήση κινητών τηλεφώνων έχει πλέον ξεπεράσει τη χρήση ηλεκτρονικών υπολογιστών [12] με αποτέλεσμα δεδομένα ερευνητικού ενδιαφέροντος, όπως συνομιλίες ή η διαδικτυακή δραστηριότητα των χρηστών, να συσσωρεύονται σε κινητές συσκευές.

- **Εγκληματολογία Δικτύων (Network Forensics)** : Η εγκληματολογία δικτύων ασχολείται με την ανάλυση της διαδικτυακής κίνησης και έχει ως στόχο τον εντοπισμό της πηγής κυβερνοεπιθέσεων ή την άντληση δεδομένων από δίκτυα που σχετίζονται με κάποιο κυβερνοέγκλημα.

- **Εγκληματολογία Βάσεων Δεδομένων** : Αντικείμενο της Εγκληματολογίας Βάσεων Δεδομένων είναι η εξέταση των δεδομένων που βρίσκονται σε βάσεις δεδομένων καθώς και των μεταδεδομένων τους.

- **Εγκληματολογία IoT** : Η εγκληματολογία IoT (Internet of Things) αποτελεί ένα σχετικά νέο κλάδο της ψηφιακής εγκληματολογίας ο οποίος περιλαμβάνει την ανάλυση ψηφιακών δεδομένων από συσκευές IoT και αισθητήρες, καθώς και από το δίκτυο στο οποίο συνδέονται [13].

- **Εγκληματολογία Νέφους (Cloud Forensics)** : Η Εγκληματολογία Νέφους είναι η εφαρμογή της ψηφιακής εγκληματολογίας σε περιβάλλοντα νέφους, και μπορεί να θεωρηθεί υποκλάδος της Εγκληματολογίας Δικτύων.

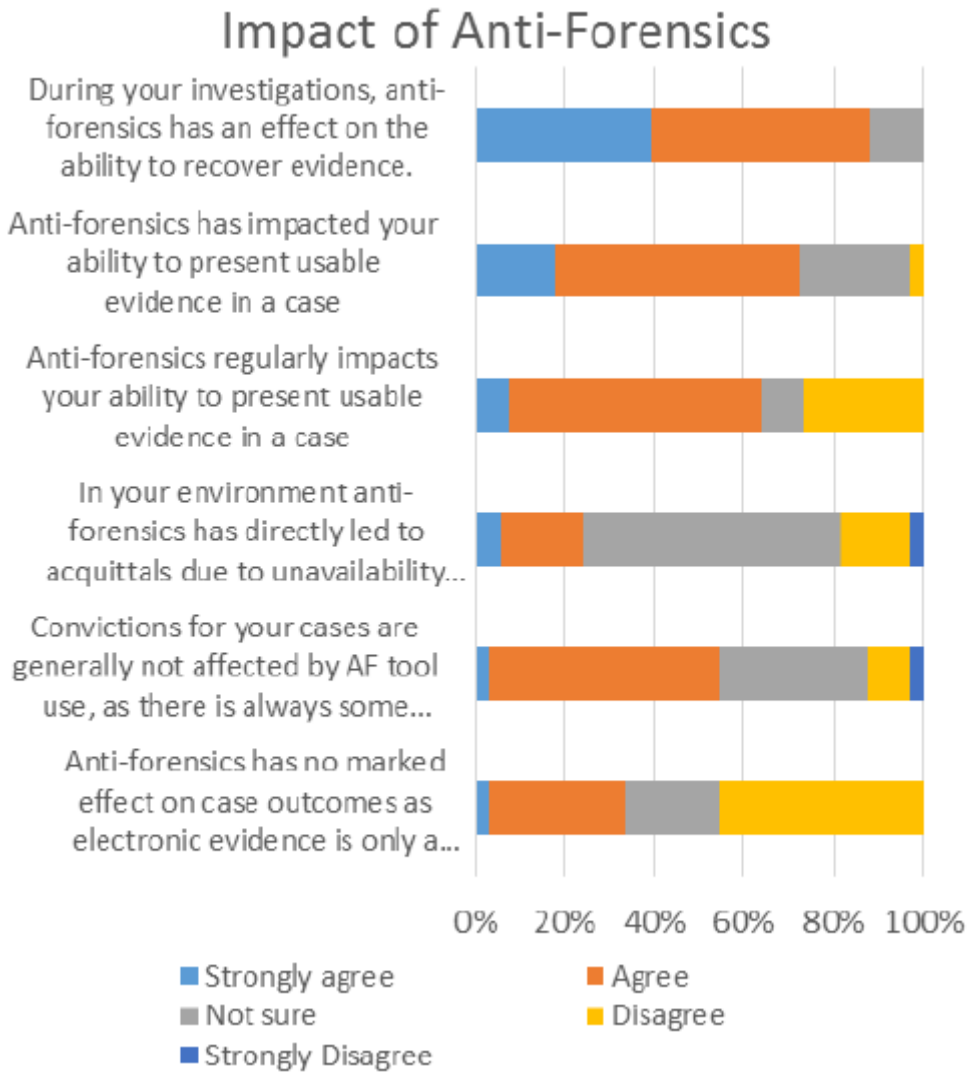
1.2 Anti-Forensics – Ορισμός

Όπως αναφέρθηκε παραπάνω, η Ψηφιακή Εγκληματολογία (Digital Forensics) περιλαμβάνει τη χρήση εργαλείων και μεθοδολογιών για τη συλλογή, ανάλυση, εξέταση και παρουσίαση των ψηφιακών πειστηρίων. Από την άλλη πλευρά, η έννοια Anti-Forensics (Αντι-Δικανική) περιλαμβάνει τη χρήση εργαλείων και τεχνικών ως αντίμετρο στην ομαλή διεξαγωγή μιας έρευνας. Έχουν γίνει πολλές προσπάθειες ορισμού της έννοιας «anti-forensics» [14], ωστόσο ο Rogers δίνει έναν περιεκτικό ορισμό ως εξής:

«Απόπειρες να επηρεαστεί αρνητικά η ύπαρξη, η ποσότητα και/ή η ποιότητα των πειστηρίων από τον τόπο του εγκλήματος, ή να καταστήσουν την ανάλυση και την εξέταση των πειστηρίων δύσκολη ή αδύνατη να πραγματοποιηθεί» [15].

Από τον παραπάνω ορισμό προκύπτει πως οι τεχνικές anti-forensics έχουν ως στόχο να επηρεάσουν κάποιο/α από τα βασικά στάδια της ερευνητικής διαδικασίας (συλλογή, εξέταση και ανάλυση των ψηφιακών δεδομένων). Για παράδειγμα, η καταστροφή των μέσων από τα οποία πραγματοποιείται η συλλογή των ψηφιακών δεδομένων μπορεί να καταστήσει το στάδιο της συλλογής αδύνατο ή ασύμφορο χρονικά ή/και οικονομικά. Επίσης, κατά τη συλλογή δεδομένων από ένα σύστημα σε λειτουργία είναι πιθανό να ενεργοποιηθεί κάποια διαδικασία καταστροφής δεδομένων αν δεν ικανοποιούνται ορισμένες συνθήκες, όπως για παράδειγμα το πάτημα ενός συγκεκριμένου συνδυασμού πλήκτρων σε περιορισμένο χρονικό διάστημα [16]. Υπάρχουν ορισμένα εργαλεία που έχουν ως στόχο να αποτρέψουν πρόσβαση σε δεδομένα του συστήματος όπως το εργαλείο USBKill το οποίο τερματίζει τη λειτουργία τους συστήματος αν ανιχνευτεί κάποια άγνωστη συσκευή USB [17].

Στο στάδιο στης εξέτασης πραγματοποιείται η αναζήτηση δεδομένων που θα αποτελέσουν πειστήρια για την υπό διερεύνηση υπόθεση. Η απόκρυψη δεδομένων με χρήση τεχνικών όπως η κρυπτογραφία και η στεγανογραφία μπορούν να δυσχεράνουν τον εντοπισμό σημαντικών στοιχείων ή να οδηγήσουν σε μία χρονικά δαπανηρή διαδικασία. Τέλος, στο στάδιο της ανάλυσης τα δεδομένα που έχουν συλλεχθεί ως πειστήρια συσχετίζονται και ερμηνεύονται ώστε να οδηγήσουν σε μια χρονική σειρά γεγονότων. Οι χρονοσημάνσεις (timestamps), που βρίσκονται στα μεταδεδομένα αρχείων και σε αρχεία καταγραφής, υποδηλώνουν τη χρονική στιγμή την οποία πραγματοποιήθηκε κάποια ενέργεια και αξιοποιούνται για τη δημιουργία χρονοδιαγραμμάτων. Επομένως, η τροποποίηση των χρονοσημάνσεων θα οδηγήσει σε εσφαλμένα συμπεράσματα [18]. Η επίδραση των τεχνικών anti-forensics φαίνεται και σχηματικά στο σχήμα 1.1 το οποίο συνοψίζει τα ευρήματα της έρευνας του J. Van Belle σχετικά με την εξοικείωση των ερευνητών όσον αφορά τις τεχνικές anti-forensics [19].



Σχήμα 1.1 Επιπτώσεις των τεχνικών anti-forensics, όπως απεικονίζεται στο [19, Σχήμα 7]

1.3 Anti-Forensics – Εφαρμογές

1.3.1 Προστασία δεδομένων

Παρότι θα μπορούσε να σχηματιστεί η άποψη ότι οι τεχνικές και τα εργαλεία anti-forensics αξιοποιούνται αποκλειστικά για κακόβουλες ενέργειες, είναι σημαντικό να σημειωθεί ότι πολλές από αυτές τις τεχνικές χρησιμοποιούνται για την προστασία ψηφιακών δεδομένων, καθώς και την ανωνυμία των χρηστών στο διαδίκτυο. Παράδειγμα αποτελεί η κρυπτογράφηση, η οποία ενώ, όπως θα αναφερθεί παρακάτω, αποτελεί μία τεχνική anti-forensics, χρησιμοποιείται κατά κόρων για την ασφαλή μετάδοση των δεδομένων των χρηστών στο διαδίκτυο μέσω του πρωτοκόλλου TLS (Transport Layer Security). Η οριστική διαγραφή δεδομένων από το σκληρό δίσκο αποτελεί επίσης μία τεχνική anti-forensics. Ωστόσο, είναι μία απαραίτητη διαδικασία για την καταστροφή ευαίσθητων πληροφοριών τόσο απλών χρηστών, όσο και εταιρειών, ενώ χρησιμοποιείται και από τους ερευνητές της ψηφιακής εγκληματολογίας για τον καθαρισμό αποθηκευτικών μέσων ώστε να

επαναχρησιμοποιηθούν. Για την ασφαλή καταστροφή ψηφιακών δεδομένων υπάρχουν πρότυπα που ακολουθούνται από οργανισμούς, υπηρεσίες και εταιρείες [20],[21].

1.3.2 Ανωνυμία

Επιπλέον, τα εργαλεία που παρέχουν ανωνυμία στο διαδίκτυο όσον αφορά το κομμάτι της έρευνας δυσχεραίνουν τον εντοπισμό εγκληματιών, ωστόσο, δεν χρησιμοποιούνται αποκλειστικά για κακόβουλες ενέργειες. Χαρακτηριστικό παράδειγμα αποτελεί ο δρομολογητής Tor ο οποίος χρησιμοποιείται από χρήστες που θέλουν να προστατεύσουν την ταυτότητά τους στο διαδίκτυο (δημοσιογράφοι, πληροφοριοδότες, ακτιβιστές, απλοί χρήστες) ή να έχουν ελεύθερη πρόσβαση σε πηγές και ιστοσελίδες που έχουν αποκλειστεί είτε λόγω λογοκρισίας είτε λόγω γεωγραφικού αποκλεισμού [22]. Συνεπώς, πολλά εργαλεία και τεχνικές που χρησιμοποιούνται ως μέθοδοι anti-forensics θα μπορούσαμε να τα θεωρήσουμε δυνητικά κακόβουλα, αφού ο τρόπος με τον οποίο χρησιμοποιούνται εξαρτάται από τις προθέσεις του χρήστη.

1.4 Προκλήσεις Ψηφιακής Εγκληματολογίας

Οι τεχνικές anti-forensics μπορεί να προκαλέσουν σοβαρές επιπτώσεις στην διεξαγωγή και στην έκβαση μιας έρευνας κατά τη διερεύνηση περιστατικών ασφάλειας και άλλων υποθέσεων. Ωστόσο, υπάρχουν και άλλοι παράγοντες οι οποίοι μπορούν να διακινδυνεύσουν την ομαλή διεξαγωγή μιας έρευνας και, συνεπώς, είναι σημαντικό να λαμβάνονται υπόψη από τους ερευνητές. Ένας ακόμα λόγος που αξίζει να αναφερθούν, είναι το γεγονός ότι η αποτελεσματικότητα των τεχνικών anti-forensics έγκειται στην εκμετάλλευση αυτών των παραγόντων.

1.4.1 Ανθρώπινος Παράγοντας

Ο ανθρώπινος παράγοντας περιλαμβάνει παραλείψεις και σφάλματα που οφείλονται στη φύση του ανθρώπου και στις δυνατότητές του. Οι Sunde και Dror στην ερευνητική εργασία τους με θέμα "Cognitive and human factors in digital forensics: Problems, challenges, and the way forward", αναλύουν τις επιπτώσεις που έχει η γνωστική προκατάληψη[1] και άλλοι ανθρώπινοι παράγοντες σε μία έρευνα, καθώς οδηγούν σε εσφαλμένα αποτελέσματα και πιθανώς σε λανθασμένες δικαστικές αποφάσεις [23]. Πιο συγκεκριμένα, τα συμπεράσματα στα οποία καταλήγει ένας ερευνητής και η διαδικασία σκέψης που θα ακολουθήσει για να καταλήξει σε αυτά, είναι πιθανό να επηρεάζονται από πηγές γνωστικής προκατάληψης οι οποίες παρουσιάζονται συνοπτικά παρακάτω [23]:

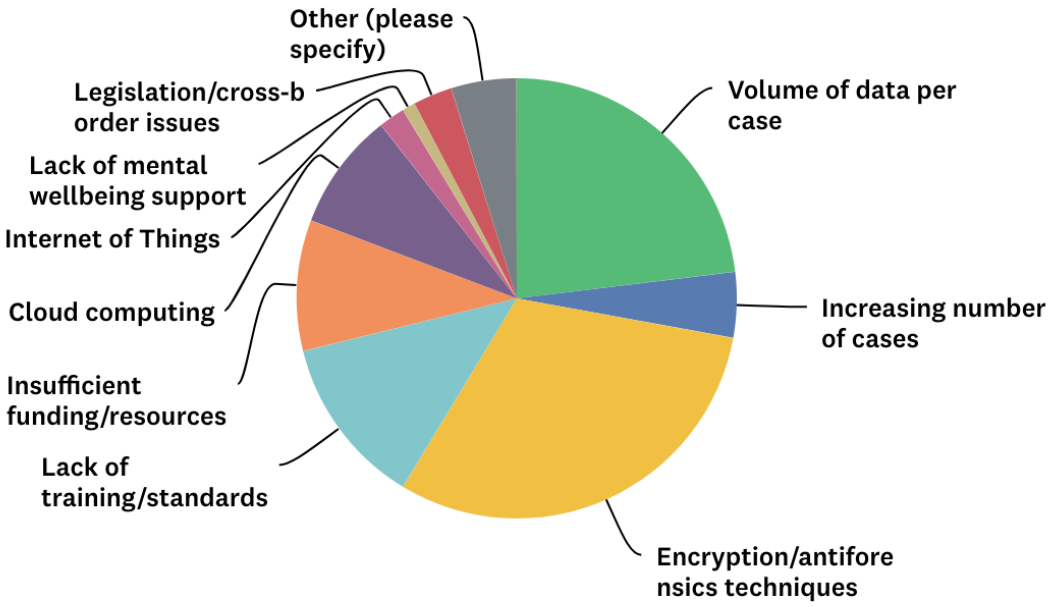
1. **Γνωσιακή αρχιτεκτονική και εγκέφαλος** - Κατά τη διεξαγωγή μιας έρευνας ο ερευνητής είναι πιθανό να εστιάσει και να να δώσει μεγαλύτερη αξία σε αρχικές πληροφορίες (anchoring bias), να αναμένει παρόμοια αποτελέσματα με αυτά από παρόμοια περιστατικά (availability bias), και να καταλήξει σε μία υπόθεση προσπαθώντας να την υποστηρίξει, αγνοώντας τις

[1] Γνωστική προκατάληψη είναι ο λανθασμένος τρόπος σκέψης ενός ατόμου που βασίζεται στις προσωπικές εμπειρίες και πεποιθήσεις του. Πολλές φορές η γνωστική προκατάληψη είναι αποτέλεσμα της τάσης του εγκεφάλου να απλοποιεί την επεξεργασία πληροφοριών [24].

πληροφορίες που αντιτίθενται στην υπόθεση και δίνοντας αξία σε αυτές που την υποστηρίζουν (confirmation bias) [23]. Οι παραπάνω προκαταλήψεις είναι αποτέλεσμα του τρόπου με τον οποίο ο εγκέφαλος προσπαθεί να επεξεργαστεί πληροφορίες ώστε να επιτευχθεί η πιο αποτελεσματική δράση και η ταχύτερη λήψη αποφάσεων [24].

2. **Εκπαίδευση και κίνητρο** - Τα προγράμματα σπουδών που ακολουθούν οι υποψήφιοι ερευνητές της ψηφιακής εγκληματολογίας δεν δίνουν την απαραίτητη έμφαση ή συχνά παραλείπουν εντελώς την επίδραση του ανθρώπινου παράγοντα και των γνωστικών προκαταλήψεων στη διεξαγωγή μιας έρευνας εστιάζοντας σε τεχνικά θέματα, με αποτέλεσμα να μην λαμβάνονται υπόψη από τους ερευνητές. Επιπλέον, το κίνητρο για υπεράσπιση του θύματος ή για απόδοση δικαιοσύνης μπορεί να οδηγήσει τον ερευνητή στην αναζήτηση πειστηρίων που θα ενοχοποιούν τον θύτη.
3. **Οργανωτικοί παράγοντες** - Το εργασιακό περιβάλλον, ο τρόπος λειτουργίας του και τα συμφέροντα που εξυπηρετεί είναι ένας παράγοντας που μπορεί να επηρεάσει τον τρόπο με τον οποίο ο ερευνητής προσεγγίζει την έρευνα. Ο όρος adversarial allegiance χρησιμοποιείται για να περιγράψει την προκατάληψη ενός εμπειρογνώμονα ανάλογα με την πλευρά που εξυπηρετεί, αυτή της υπεράσπισης ή της κατηγορίας ενός κατηγορούμενου [23].
4. **Base rate expectations** - Οι προσδοκίες που έχει ένας ερευνητής από μία υπόθεση βασίζονται στην εμπειρία του με προηγούμενες υποθέσεις, με αποτέλεσμα να την προσεγγίζει με παρόμοιο τρόπο αναμένοντας παρόμοια αποτελέσματα.
5. **Πληροφορίες μη σχετικές με την υπόθεση** - Η υποκειμενική άποψη του ερευνητή για τα πιθανά αποτελέσματα μιας έρευνας και η γνώμη που σχηματίζει για τον ύποπτο λόγω της εθνικότητάς του, του ποινικού του μητρώου, τις μαρτυρίες ή τα Μέσα Μαζικής Ενημέρωσης [25], αποτελούν πληροφορίες που δεν σχετίζονται με την υπόθεση και διακινδυνεύουν την αντικειμενική προσέγγιση της υπόθεσης από τον ερευνητή.
6. **Υλικό αναφοράς** - Όταν υπάρχει υλικό αναφοράς στο οποίο βασίζεται η έρευνα για την αναζήτηση πειστηρίων σχετικά με αυτό, τότε η έρευνα μπορεί να επηρεαστεί όταν το ίδιο το σημείο αναφοράς περιλαμβάνει πληροφορίες που θα μπορούσαν να οδηγήσουν σε προκατάληψη.
7. **Πειστήρια** - Τα ίδια τα πειστήρια μπορούν να προσανατολίσουν την έρευνα. Ένα παράδειγμα είναι οι αναζητήσεις στο διαδίκτυο τις οποίες ο ερευνητής μπορεί να συσχετίσει με την έρευνα, όπως συνέβη στην υπόθεση της Casey Anthony στην οποία οι ερευνητές βασιζόμενοι στις διαδικτυακές αναζητήσεις της κατηγορούμενης παρέλειψαν σημαντικές πληροφορίες και κατέληξαν σε εσφαλμένα συμπεράσματα [26].

Σε έρευνα που πραγματοποιήθηκε το 2018 από την ιστοσελίδα *Forensic Focus* τα αποτελέσματα έδειξαν ότι η έλλειψη εκπαίδευσης και προτύπων ήταν ανάμεσα στις 3 πρώτες προκλήσεις που καλείται να αντιμετωπίσει η ψηφιακή εγκληματολογία με ποσοστό 12,50% ακολουθώντας τον όγκο δεδομένων ανά υπόθεση με 23,08% και τις τεχνικές anti-forensics με ποσοστό 30,77% [27]. Η σωστή και συνεχής εκπαίδευση παίζει πολύ σημαντικό ρόλο στη διεξαγωγή ερευνών. Με σωστή εκπαίδευση ο ερευνητής θα είναι σε θέση να αντεπεξέρχεται κατάλληλα στις απαιτήσεις κάθε υπόθεσης ακολουθώντας προτυποποιημένες διαδικασίες και χρησιμοποιώντας επικυρωμένα εργαλεία, αποφεύγοντας σφάλματα που μπορούν να προκληθούν από μη ορθή διαχείριση των ψηφιακών δεδομένων. Με τη συνεχή εκπαίδευση ο ερευνητής θα έχει την δυνατότητα να διαχειριστεί τις προκλήσεις που επιφέρει η εμφάνιση νέων τεχνολογιών (όπως οι έξυπνες συσκευές, η τεχνολογία blockchain, το Διαδίκτυο των Πραγμάτων (Internet of Things)), οι οποίες πιθανόν να αποτελέσουν αντικείμενο έρευνας για τη διερεύνηση υποθέσεων και περιστατικών ασφάλειας.



Σχήμα 1.2 Αποτελέσματα της έρευνας για τις προκλήσεις της ψηφιακής εγκληματολογίας, όπως απεικονίζεται στο [27]

1.4.2 Εργαλεία

Οι περισσότερες διαδικασίες στη διερεύνηση περιστατικών ασφάλειας έχουν αυτοματοποιηθεί με τη χρήση εργαλείων. Σύμφωνα με τον David Kovar η χρήση εργαλείων που αυτοματοποιούν διαδικασίες με το πάτημα μερικών πλήκτρων («push button forensics») δεν απαιτεί από τον ερευνητή να έχει ιδιαίτερες γνώσεις, πέραν από αυτές που αφορούν τη χρήση του εργαλείου [28]. Έτσι, οι ειδικοί μπορούν να αντικατασταθούν από τεχνικούς σε μία προσπάθεια μείωσης του κόστους της έρευνας. Όταν η αυτοματοποίηση γίνεται σε πιο πολύπλοκες διαδικασίες, όπως η ανάλυση των ψηφιακών πειστηρίων όπου πρέπει τα δεδομένα να ερμηνευτούν και να οδηγήσουν στη διεξαγωγή συμπερασμάτων, μπορεί να εξοικονομεί σημαντικό χρόνο στον ερευνητή. Ωστόσο, όταν τα αποτελέσματα που παράγουν τα εργαλεία δεν υφίστανται κατάλληλη επεξεργασία που βασίζεται στις γνώσεις και τις εμπειρίες του ερευνητή, η ποιότητα των αποτελεσμάτων τα οποία θα παρουσιαστούν ως πειστήρια είναι αμφίβολη [29].

Επιπλέον, δεν πρέπει να παραλείψουμε πως τα εργαλεία που χρησιμοποιούνται κατά τη διεξαγωγή μιας έρευνας είναι προγράμματα τα οποία πιθανόν να είναι επιρρεπή σε σφάλματα. Για παράδειγμα, η επεξεργασία τροποποιημένων (malformed) αρχείων από το πρόγραμμα, είναι δυνατόν να οδηγήσει σε απρόσμενη συμπεριφορά του προγράμματος, όπως την εμφάνιση σφαλμάτων και κατάρρευση του προγράμματος, ή και στην παραγωγή εσφαλμένων αποτελεσμάτων [30]. Έτσι, καθίσταται αναγκαίος ο έλεγχος εγκυρότητας και η επαλήθευση των εργαλείων που χρησιμοποιούνται, αφού από αυτά εξαρτάται και η αξιοπιστία των αποτελεσμάτων της έρευνας [31]. Πολλές αγωγές έχουν απορριφθεί λόγω των εργαλείων που είτε προσπέλασαν προσωπικά αρχεία των κατηγορούμενων με ακατάλληλο τρόπο είτε δεν ήταν δυνατή η επικύρωση της ορθής λειτουργίας τους στους δικηγόρους υπεράσπισης [32].

1.4.3 Κόστος

Ένας πολύ σημαντικός περιορισμός στη διεξαγωγή μιας έρευνας είναι το κόστος της, τόσο το χρονικό όσο και το οικονομικό, και αποτελεί κριτήριο για την επιλογή και τη διάρκεια διερεύνησης των υποθέσεων [33]. Το κόστος της έρευνας εξαρτάται και από τις τεχνολογίες από τις οποίες εξάγονται τα δεδομένα προς ανάλυση. Σε έρευνα που πραγματοποίησε ο Tyler Moore στη εργασία του «The Economics of Digital Forensics» συγκρίνεται το κόστος της έρευνας σε τεχνολογίες που χρησιμοποιούν ανοιχτά πρότυπα σε σύγκριση με αυτά που χρησιμοποιούν ιδιωτικά πρότυπα [34]. Μέσα από αυτή τη σύγκριση προκύπτει το συμπέρασμα πως η έρευνα που πραγματοποιείται σε ηλεκτρονικούς υπολογιστές έχει σαφώς μικρότερο κόστος από μία έρευνα που πραγματοποιείται σε κινητά τηλέφωνα. Αυτό οφείλεται στο γεγονός ότι οι ηλεκτρονικοί υπολογιστές χρησιμοποιούν κάποια κοινά πρότυπα, με αποτέλεσμα να υπάρχουν διαθέσιμα εργαλεία και επικυρωμένες μεθοδολογίες για την πραγματοποίηση της έρευνας [34]. Αντίθετα, η χρήση διαφορετικών προτύπων ανάλογα με τον κατασκευαστή αυξάνουν το κόστος και το χρόνο που απαιτείται για την έρευνα από τη στιγμή που τα διαθέσιμα εργαλεία είναι περιορισμένα και πιθανόν να απαιτείται συνεργασία με τον εκάστοτε κατασκευαστή [35]. Τέλος, ένας ακόμα παράγοντας που αυξάνει το κόστος της έρευνας είναι ο όγκος των δεδομένων ο οποίος, όπως προκύπτει από έρευνα σχετικά με τις προκλήσεις της ψηφιακής εγκληματολογίας, αποτελεί τη δεύτερη μεγαλύτερη πρόκληση που αντιμετωπίζουν οι ερευνητές [27]. Το 2012 αποσύρθηκαν οι κατηγορίες σε βάρος ενός γιατρού για παράνομη πώληση φαρμάκων σε ασθενείς, λόγω του υψηλού κόστους διατήρησης του πολύ μεγάλου όγκου δεδομένων που είχε συσσωρευτεί σχετικά με την υπόθεση [36].

1.4.4 Νομικοί περιορισμοί

Θα μπορούσε κανείς να αναρωτηθεί γιατί δεν αξιοποιούνται οι τεχνικές που χρησιμοποιούν οι εγκληματίες (π.χ. υποκλοπή ηλεκτρονικών δεδομένων και επικοινωνιών) ώστε να εντοπίσουν τους ίδιους τους εγκληματίες; Ένας πολύ σημαντικός παράγοντας που πρέπει να λαμβάνεται υπόψη καθ'όλη τη διάρκεια διεξαγωγής της εγκληματολογικής έρευνας είναι η ισχύουσα νομοθεσία. Οι νομοθεσίες που σχετίζονται με την προάσπιση της ιδιωτικής ζωής[2] περιορίζουν την έρευνα, έτσι, για παράδειγμα η παρακολούθηση της διαδικτυακής κίνησης ή η υποκλοπή προσωπικών δεδομένων ενός ατόμου με σκοπό τη συλλογή αποδεικτικών στοιχείων που θα οδηγήσουν στην ενοχοποίησή του, να μην είναι δυνατή ή να είναι περιορισμένη από τη στιγμή που αυτή παραβιάζει με τον οποιονδήποτε τρόπο την ιδιωτικότητά του [39]. Επιπλέον, το άρθρο 265 του Κώδικα Ποινικής Δικονομίας (ΚΠΔ) ορίζει τον τρόπο με τον οποίο πρέπει να γίνεται η κατάσχεση και η διαχείριση των ψηφιακών πειστηρίων, έτσι ώστε αυτά να είναι αποδεκτά από το δικαστήριο [40]. Αν η συλλογή και η διαχείριση των ψηφιακών δεδομένων δεν πραγματοποιηθεί βάσει των νόμων που ορίζονται από τη νομοθεσία, τότε τα πειστήρια ενδέχεται να αμφισβητηθούν ή ακόμα και να απορριφθούν από το αρμόδιο δικαστήριο.

Η ασάφεια των γεωγραφικών ορίων του Διαδικτύου αποτελεί επίσης πρόκληση για τους ερευνητές. Μέσω του Διαδικτύου καθίσταται δυνατή η τέλεση ενός εγκλήματος από μία χώρα σε οποιαδήποτε άλλη χώρα (ή χώρες) με αποτέλεσμα τα πειστήρια να είναι διασκορπισμένα σε μία πολύ ευρεία γεωγραφική έκταση. Αυτό αποτελεί συχνή πρόκληση κατά τη διερεύνηση περιστατικών ασφάλειας σε

[2] Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου [37], Electronic Communications Privacy Act of 1986 (ECPA) [38].

υπηρεσίες cloud όπου τα δεδομένα είναι πιθανό να διαμοιράζονται σε εξυπηρετητές που βρίσκονται σε διαφορετικές χώρες [41]. Έτσι, τίθεται το θέμα της δικαιοδοσίας σχετικά με τη διαχείριση των δεδομένων που αφορούν την έρευνα αλλά και των νόμων που ισχύουν σε κάθε χώρα. Για παράδειγμα, είναι δυνατόν μία αξιόποινη πράξη να διαπραχθεί σε αλλοδαπή χώρα στην οποία αυτή δεν θεωρείται αξιόποινη ή δεν υπάρχουν σχετικοί νόμοι και διαδικασίες για τη διεξαγωγή εγκληματολογικής έρευνας, όπως στην περίπτωση του δημιουργού του ιού "I Love You". Οι Αρχές στις Φιλιππίνες (όπου και διέμενε) απέσυραν τις κατηγορίες σε βάρος του, επειδή δεν υπήρχαν νόμοι σχετικοί με αυτόν τον τύπο ηλεκτρονικού εγκλήματος [42]. Επομένως, η νομοθεσία μιας χώρας είναι κάτι το οποίο ένας εγκληματίας μπορεί να εκμεταλλευτεί, καθώς ορισμένες υπηρεσίες cloud παρέχουν τη δυνατότητα στους χρήστες να επιλέξουν την τοποθεσία στην οποία θα είναι αποθηκευμένα τα δεδομένα τους [43-44]. Ωστόσο, ο Ποινικός Κώδικας στο άρθρο 8 ορίζει τα «Εγκλήματα στην αλλοδαπή που τιμωρούνται πάντοτε κατά τους ελληνικούς νόμους» και στα οποία συγκαταλέγονται εγκλήματα όπως η εμπορία ναρκωτικών και η πειρατεία που τελούνται και με τη χρήση υπολογιστή [45].

Επίλογος

Σε αυτό το κεφάλαιο ορίστηκαν αρχικά οι έννοιες της ψηφιακής εγκληματολογίας και των τεχνικών anti-forensics, και στης συνέχεια παρουσιάστηκαν τα βασικότερα στάδια της ερευνητικής διαδικασίας και ο τρόπος με τον οποίο οι τεχνικές anti-forensics επηρεάζουν κάθε ένα από αυτά. Τέλος, έγινε αναφορά στις προκλήσεις της διεξαγωγής ερευνών ψηφιακής εγκληματολογίας.

Κεφάλαιο 2 Τεχνικές Anti-Forensics

Εισαγωγή

Αφού έχει γίνει μία αναφορά στις διαδικασίες που πλαισιώνουν την ψηφιακή εγκληματολογία και στους στόχους των τεχνικών anti-forensics, σε αυτό το κεφάλαιο οι τεχνικές κατηγοριοποιούνται και γίνεται αναφορά στα στάδια της ερευνητικής διαδικασίας που έχουν ως στόχο να επηρεάσουν. Η κατηγοριοποίησή τους βαζίζεται στην ταξινόμηση που προτάθηκε από τον Rogers, σύμφωνα με την οποία οι τεχνικές εντάσσονται στις εξής τέσσερις κατηγορίες: καταστροφή πειστηρίων, απόκρυψη δεδομένων, απόκρυψη ιχνών και επίθεση σε εργαλεία και διαδικασίες [46]. Η κατηγοριοποίηση αυτή επιλέχθηκε, καθώς είναι η επικρατέστερη στη διαθέσιμη βιβλιογραφία και καλύπτει επαρκώς τις υπάρχουσες τεχνικές anti-forensics. Ωστόσο, ανάλογα με τον τρόπο προσέγγισης ορισμένων τεχνικών είναι δυνατή η κατάταξή τους και σε περισσότερες από μία κατηγορίες.

2.1 Καταστροφή Πειστηρίων

Η καταστροφή πειστηρίων περιλαμβάνει τεχνικές με τις οποίες τα ψηφιακά δεδομένα σε ένα σύστημα ή αποθηκευτικό μέσο αχρηστεύουν και καθίσταται αδύνατη η επαναφορά τους. Υπάρχουν τρεις βασικές κατηγορίες καταστροφής πειστηρίων: η φυσική καταστροφή του μέσου, η διαδικασία Degaussing, και η λογική καταστροφή των ψηφιακών δεδομένων [47]. Οι τεχνικές καταστροφής πειστηρίων έχουν επιπτώσεις στη διαδικασία συλλογής, όταν καταστρέφεται το μέσο αποθήκευσης, και τη διαδικασία εξέτασης πειστηρίων, όταν πραγματοποιείται λογική καταστροφή των δεδομένων.

2.1.1 Φυσική καταστροφή

Η φυσική καταστροφή επιτυγχάνεται με οποιαδήποτε μέθοδο προκαλεί ανεπανόρθωτη βλάβη στη λειτουργικότητά ενός μέσου αποθήκευσης πληροφοριών, με αποτέλεσμα να είναι αδύνατη η εξαγωγή δεδομένων από αυτό. Στα μέσα αποθήκευσης περιλαμβάνονται μεταξύ άλλων σκληροί δίσκοι, USB sticks, CD, μνήμες SD και κάρτες SIM. Για την καταστροφή των μέσων αποθήκευσης χρησιμοποιούνται ειδικές μηχανές τεμαχισμού (Shredders) και θραυστήρες (Crushers), ωστόσο, πιο συχνά χρησιμοποιούνται κοινά εργαλεία όπως σφυριά και τρυπάνια [48] ως μία πιο προσιτή και άμεση διαδικασία.

2.1.2 Degaussing

Degaussing είναι μια διαδικασία μείωσης ή εξολόθρευσης ενός μαγνητικού πεδίου και χρησιμοποιείται για την οριστική διαγραφή δεδομένων από μαγνητικά μέσα αποθήκευσης. Στα μαγνητικά μέσα η πληροφορία αποθηκεύεται μαγνητίζοντας την αγώγιμη επιφάνεια στην οποία θα αποθηκευτεί η πληροφορία (π.χ. μαγνητική ταινία στις κασέτες ή μαγνητικοί δίσκοι στους σκληρούς δίσκους) με τη χρήση ενός ηλεκτρομαγνήτη που περνάει πάνω από διαδοχικά σημεία της αγώγιμης επιφάνειας. Ανάλογα με τη κατεύθυνση του ρεύματος που διέρχεται από τον ηλεκτρομαγνήτη, το σημείο πάνω από το οποίο περνάει ο ηλεκτρομαγνήτης μαγνητίζεται με διαφορετική πολικότητα, η

οποία κατά τη διαδικασία της ανάγνωσης θα «μεταφραστεί» σε τιμές 0 και 1 [49]. Μία συσκευή Degausser δημιουργεί μαγνητικό πεδίο ισχυρής έντασης που διαταράσσει τη μαγνητική δομή που έχει δημιουργηθεί στην επιφάνεια του μαγνητικού μέσου αποθήκευσης, τυχαιοποιώντας την πολικότητα τον σημείων που είχαν μαγνητιστεί [50]. Αυτή η διαδικασία καθιστά αδύνατη την επαναφορά των δεδομένων αλλά και την επαναχρησιμοποίησή του σκληρού δίσκου αν καταστραφούν τα δεδομένα servo (embedded servo) τα οποία ρυθμίζουν την ορθή λειτουργία του σκληρού δίσκου [51].

2.1.3 Λογική καταστροφή

Σε αντίθεση με τις παραπάνω μεθόδους οι οποίες επηρεάζουν το μέσο αποθήκευσης, υπάρχει και η δυνατότητα καταστροφής των αρχείων χωρίς να καταστρέφεται το μέσο. Αυτός ο τύπος καταστροφής ψηφιακών δεδομένων ονομάζεται λογική καταστροφή και πραγματοποιείται με τη χρήση εργαλείων software. Στους ηλεκτρονικούς υπολογιστές η απλή διαγραφή των αρχείων μέσω του λειτουργικού συστήματος δεν είναι οριστική. Όταν ένας χρήστης διαγράφει ένα αρχείο, ουσιαστικά διαγράφονται οι αναφορές προς τη θέση στην οποία βρίσκεται το διαγραμμένο αρχείο στο μέσο αποθήκευσης. Για να διαγραφεί το αρχείο οριστικά πρέπει να καταστραφεί. Οι τεχνικές με τις οποίες πραγματοποιείται η καταστροφή των δεδομένων είναι η επεγγραφή (overwriting) δεδομένων, η κρυπτογραφική διαγραφή και η διαγραφή μεταδεδομένων. Η διαγραφή μεταδεδομένων αφορά μόνο τα μεταδεδομένα ενός αρχείου ωστόσο είναι μόνιμη και αφορά τις περιπτώσεις στις οποίες τα ίδια τα μεταδεδομένα αποτελούν πειστήρια.

2.1.3.1 Επεγγραφή δεδομένων

Στο λειτουργικό σύστημα Windows το σύστημα αρχείων NTFS διατηρεί έναν κατάλογο με πληροφορίες των αρχείων του συστήματος στο αρχείο MFT (Master File Table). Όταν ένα αρχείο διαγράφεται η καταχώρηση που σχετίζεται με το αρχείο στο MFT μαρκάρεται ως ελεύθερη και μπορεί να επαναχρησιμοποιηθεί, ωστόσο το αρχείο παραμένει στο σκληρό δίσκο μέχρι τη στιγμή που θα επεγγραφεί με νέα δεδομένα [52]. Παρομοίως, στο λειτουργικό σύστημα Linux το οποίο χρησιμοποιεί το σύστημα αρχείων EXT, η δομή δεδομένων inode διατηρεί μεταδεδομένα για κάθε αρχείο και κατάλογο του συστήματος μεταξύ των οποίων περιλαμβάνεται και η θέση των δεδομένων του αρχείου στο δίσκο [53]. Όταν ένα αρχείο διαγράφεται αποδεσμεύεται το inode και είναι ελεύθερο να επαναχρησιμοποιηθεί.

Σε κάθε περίπτωση τα αρχεία παραμένουν στον σκληρό δίσκο μετά τη διαγραφή τους. Επομένως, ένας τρόπος καταστροφής των ψηφιακών δεδομένων είναι η επεγγραφή τους με τυχαία ή και καθορισμένα μοτίβα πληροφορίας (0 και 1). Η επεγγραφή των δεδομένων μπορεί να γίνει στην περιοχή του δίσκου που καταλαμβάνουν συγκεκριμένα αρχεία ώστε να καταστραφούν μόνο αυτά, σε περιοχές του δίσκου που είναι ελεύθερες (στις οποίες μπορεί να βρίσκονται προηγουμένως διαγραμμένα αρχεία) ή σε ολόκληρο το σκληρό δίσκο για την καταστροφή όλων των δεδομένων που βρίσκονται σε αυτόν. Ωστόσο, πρέπει να επισημανθεί πως σε αντίθεση με τους σκληρούς δίσκους (HDD) όπου τα διαγραμμένα δεδομένα πιθανόν να διατηρηθούν και για χρόνια μέχρι να επεγγραφούν, οι δίσκοι στερεάς κατάστασης (SSD) “καθαρίζουν τις περιοχές στις οποίες υπάρχουν διαγραμμένα αρχεία για την αποδοτικότερη λειτουργία του δίσκου [54]. Επιπλέον, η επεγγραφή δεδομένων είναι

μία αναποτελεσματική μέθοδος διαγραφής δεδομένων στους δίσκους SSD, και για αυτόν τον λόγο οι κατασκευαστές δίσκων SSD παρέχουν αποκλειστικά προγράμματα ασφαλούς καταστροφής δεδομένων.

Υπάρχουν ποικίλοι μέθοδοι επεγγραφής οι οποίοι διαφοροποιούνται μεταξύ τους βάσει των δεδομένων που γράφουν στο δίσκο και στα περάσματα (passes), δηλαδή στο πόσες φορές επαναλαμβάνεται η επεγγραφή. Για παράδειγμα, η μέθοδος DoD 5220.22-M, η οποία δημοσιεύθηκε από το Υπουργείο Άμυνας των ΗΠΑ, εφαρμόζει τρία περάσματα: στο πρώτο πέρασμα εγγράφονται όλες οι διευθυνσιοδοτούμενες περιοχές του δίσκου με μηδενικά, στο δεύτερο πέρασμα εγγράφονται με άσους και στο τρίτο πέρασμα με τυχαίο μοτίβο από bits [55]. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) δημοσίευσε το πρότυπο NIST 800-88 για την καταστροφή δεδομένων από διάφορα μέσα, σύμφωνα με το οποίο για τη λογική καταστροφή των δεδομένων αρκεί ένα πέρασμα επεγγραφής του δίσκου με μηδενικά [20]. Τα προγράμματα καταστροφής δεδομένων υποστηρίζουν διάφορες μεθόδους επεγγραφής όπως οι παραπάνω.

2.1.3.2 Κρυπτογραφική διαγραφή

Η κρυπτογραφική διαγραφή είναι η διαδικασία διαγραφής δεδομένων κατά την οποία διαγράφεται το κλειδί με το οποίο έχουν κρυπτογραφηθεί τα δεδομένα. Η τεχνική αυτή εφαρμόζεται σε δίσκους SED (Self-Encrypting Drive) που παρέχουν τη δυνατότητα κρυπτογράφησης των δεδομένων τους [20]. Στην ουσία τα δεδομένα δεν καταστρέφονται, ωστόσο, το κλειδί κρυπτογράφησης των δεδομένων επεγγράφεται με ένα καινούργιο κλειδί με αποτέλεσμα να είναι αδύνατη η αποκρυπτογράφηση και, κατά συνέπεια, η επαναφορά των κρυπτογραφημένων δεδομένων. Η κρυπτογραφική διαγραφή είναι μια διαδικασία ταχύτερη από την επεγγραφή ολόκληρου του δίσκου, αφού επεγγράφεται μόνο το κλειδί κρυπτογράφησης. Κατά μία έννοια αυτή η τεχνική χρησιμοποιείται από κρυπτογραφικά ransomware, όπως το CryptoLocker [56] και το SamSam [57], τα οποία κρυπτογραφούν τα αρχεία του χρήστη και σε περίπτωση που δεν πληρωθούν τα λίτρα το κλειδί αποκρυπτογράφησης δεν αποστέλλεται ποτέ στο θύμα, με αποτέλεσμα να μην είναι δυνατή η αποκρυπτογράφησή τους, άρα και η πρόσβαση σε αυτά.

2.1.3.3 Καταστροφή μεταδεδομένων

Τα μεταδεδομένα ορίζονται ως δεδομένα για τα δεδομένα και αποτελούν πληροφορίες που περιγράφουν ένα αρχείο, όπως η ημερομηνία τροποποίησης, πρόσβασης και δημιουργίας - οι οποίες συνοπτικά θα αναφέρονται ως πληροφορίες MAC (Modification, Access, Creation) -, το όνομα χρήστη, το μέγεθος ενός αρχείο κ.λπ..

Οι πληροφορίες MAC έχουν σημαντικό ρόλο σε μια έρευνα, αφού μπορεί να γίνει φιλτράρισμα των δεδομένων με βάση μια χρονική περίοδο που σχετίζεται με την υπόθεση, μειώνοντας τον όγκο των στοιχείων προς ανάλυση, αλλά και τον απαιτούμενο χρόνο ανάλυσής τους. Οι πληροφορίες MAC χρησιμοποιούνται επίσης για τη χρονική αναπαράσταση γεγονότων με τη χρήση εργαλείων τα οποία αξιοποιούν αυτές τις πληροφορίες για τη δημιουργία χρονοδιαγραμμάτων [58]. Επομένως, αν οι χρονοσημάνσεις MAC τροποποιηθούν, κάποια χρήσιμα στοιχεία πιθανόν να παραλειφθούν αν λόγω των (τροποποιημένων) χρόνων δημιουργίας ή πρόσβασής τους θεωρηθεί πως δεν σχετίζονται με το υπό διερεύνηση περιστατικό. Επιπλέον, αν οι χρονικές αυτές πληροφορίες τροποποιηθούν ή

διαγραφούν από ένα αρχείο που θεωρείται πως σχετίζεται με ένα περιστατικό, πιθανόν να είναι δύσκολο να αποδειχθεί η αξιοπιστία του ως πειστήριο. Η ευκολία τροποποίησης τον χρονοσφραγίδων με ελεύθερο λογισμικό αποτελεί έναν ακόμα λόγο για τον οποίο συχνά αμφισβητείται η αξιοπιστία τους.

Τα μεταδεδομένα αρχείων εικόνας αποτελούν άλλη μία σπουδαία πηγή πειστηρίων, όμως η καταστροφή τους είναι μία εύκολη διαδικασία. Στα μεταδεδομένα αρχείων εικόνας συγκαταλέγονται, μεταξύ άλλων, πληροφορίες όπως ο κατασκευαστής και το μοντέλο της συσκευής, ρυθμίσεις της συσκευής, ώρα και ημερομηνία λήψης, ακόμα και γεωγραφικές συντεταγμένες του σημείου στο οποίο έγινε η λήψη της εικόνας [59]. Μπορεί κανείς να βρει μια πληθώρα ελεύθερων εργαλείων για τη διαγραφή μεταδεδομένων από αρχεία, πολλά από τα οποία είναι διαδικτυακά και δεν απαιτούν λήψη ή/και εγκατάσταση (δεν αφήνουν ίχνη στο σύστημα), ενώ και το λειτουργικό σύστημα Windows παρέχει αυτή τη δυνατότητα χωρίς να απαιτείται εγκατάσταση κάποιας εφαρμογής. Επιπλέον, η διαγραφή μεταδεδομένων είναι κάτι που πολλά μέσα κοινωνικής δικτύωσης πραγματοποιούν πριν την ανάρτηση εικόνων από τους χρήστες.

2.2 Απόκρυψη Πειστηρίων

Οι διάφορες τεχνικές απόκρυψης πειστηρίων αποσκοπούν στα να καταστήσουν τα πειστήρια όσο το δυνατόν πιο δυσπρόσιτα και εκμεταλλεύονται τον περιορισμένο χρόνο που έχουν στη διάθεσή τους οι ερευνητές, καθώς και τον μεγάλο όγκο δεδομένων προς ανάλυση [60]. Ακόμα και η πιο απλή και εύκολα ανιχνεύσιμη τεχνική θα έχει κάποια επίπτωση στο χρόνο που απαιτείται για την ανάλυση των πειστηρίων, άρα και στο κόστος της έρευνας. Η απόκρυψη πειστηρίων επηρεάζει τη φάση της εξέτασης των δεδομένων, αλλά και τη φάση της συλλογής σε ενεργά συστήματα.

2.2.1 Τροποποίηση αρχείων

Μία πολύ απλή τεχνική για την απόκρυψη πειστηρίων αποτελεί η αλλαγή της επέκτασης των αρχείων. Πλέον η τροποποίηση των επεκτάσεων εντοπίζεται από πολλά εργαλεία forensics που ελέγχουν αν η επέκταση του αρχείου, που δηλώνει το είδος του αρχείου, συμπίπτει με τον τύπο αρχείου που δηλώνει η υπογραφή του (file signature)[3]. Ωστόσο, η απλή αυτή τεχνική μπορεί να είναι αποτελεσματική σε περίπτωση που η έρευνα περιορίζεται σε συγκεκριμένου τύπου αρχεία (π.χ. εγγράφων κειμένου, εκτελέσιμων αρχείων, εικόνων κ.λπ.) και χρησιμοποιούνται εργαλεία που δεν πραγματοποιούν τον παραπάνω έλεγχο. Βέβαια, είναι δυνατή και η τροποποίηση της ίδιας της υπογραφής του αρχείου αποκρύπτοντας το αρχείο ακόμα πιο αποτελεσματικά και από εργαλεία που πραγματοποιούν έλεγχο ασυμβατότητας μεταξύ του τύπου ενός αρχείου και της υπογραφής του, όπως παρουσιάζεται στο 3ο κεφάλαιο. Με αυτόν τον τρόπο θα μπορούσε κάποιος, για παράδειγμα, να τροποποιήσει αρχεία ώστε να φαίνονται ως αρχεία του συστήματος τα οποία πιθανόν να αγνοούνται κατά τη διάρκεια μιας έρευνας στην οποία αναζητούνται αρχεία όπως έγγραφα, εικόνες ή βίντεο.

[3] Η υπογραφή ενός αρχείου είναι μία ακολουθία από bytes, συνήθως στην αρχή του αρχείου, που δηλώνουν τον τύπο του αρχείου.

2.2.2 Κρυπτογραφία

Η κρυπτογραφία θεωρείται μία από τις ταχύτερες και αποτελεσματικότερες τεχνικές απόκρυψης δεδομένων [10], και η ευκολία τόσο στην πρόσβαση όσο και στη χρήση εργαλείων κρυπτογράφησης την καθιστά μία τεχνική ευρέως χρησιμοποιούμενη. Ανάλογα με το πόσο ισχυρός είναι ο αλγόριθμος κρυπτογράφησης και τη δυνατότητα ή μη πρόσβασης στο κλειδί κρυπτογράφησης η έρευνα μπορεί να γίνει δύσκολη ή ακόμα και αδύνατη. Το 2016 το FBI έδωσε κοντά στο 1 εκατομμύριο δολάρια για να ξεκλειδώσουν το iPhone ενός από τους δράστες της ένοπλης επίθεσης στο *Σαν* Μπερναντίνο της Καλιφόρνια το 2015 [61]. Είναι, βέβαια, προφανές πως αυτό δεν μπορεί να συμβεί για κάθε κινητό τηλέφωνο που είναι κρυπτογραφημένο ή για κάθε άλλη περίπτωση κρυπτογραφημένων δεδομένων, καθώς αποτελεί μία ασύμφορη διαδικασία, με αποτέλεσμα να χάνονται πολύτιμα δεδομένα που θα μπορούσαν να αποτελέσουν πειστήρια.

2.2.2.1 Τύποι κρυπτογραφίας

Η κρυπτογράφηση μπορεί να εφαρμοστεί σε μεμονωμένα αρχεία και καταλόγους με χρήση εργαλείων software ή από το σύστημα αρχείων το οποίο είναι είτε γενικού σκοπού με δυνατότητα κρυπτογράφησης είτε κρυπτογραφικό. Επιπλέον, υπάρχει και η δυνατότητα κρυπτογράφησης του μέσου αποθήκευσης των δεδομένων με χρήση λογισμικού κρυπτογράφησης, ενώ πολλοί κατασκευαστές σκληρών δίσκων παρέχουν λειτουργία κρυπτογράφησης σε επίπεδο hardware (self-encrypting drives). Οι τρεις τύποι κρυπτογράφησης που είναι πιθανό να εντοπιστούν κατά τη διεξαγωγή μιας έρευνας είναι η χρήση κλασικής κρυπτογραφίας, η κρυπτογραφία συμμετρικού κλειδιού και η κρυπτογραφία δημοσίου κλειδιού.

Στην κλασική κρυπτογραφία ως κλειδί μπορεί να θεωρηθεί ο ίδιος ο αλγόριθμος κρυπτογράφησης αφού αν κάποιος γνωρίζει τον αλγόριθμο μπορεί να αποκρυπτογραφήσει τα δεδομένα. Κατά κύριο λόγο στην κλασική κρυπτογραφία συγκαταλέγονται αλγόριθμοι αντικατάστασης και εφαρμόζονται στην κρυπτογράφηση κειμένων. Στους αλγόριθμους αντικατάστασης κάθε χαρακτήρας αντικαθίσταται από έναν άλλο χαρακτήρα ο οποίος παραμένει ο ίδιος (μονοαλφαβητικό σύστημα αντικατάστασης) ή από έναν χαρακτήρα ο οποίος όμως μεταβάλλεται κατά τη διάρκεια της κρυπτογράφησης (πολυαλφαβητικό σύστημα αντικατάστασης) [62].

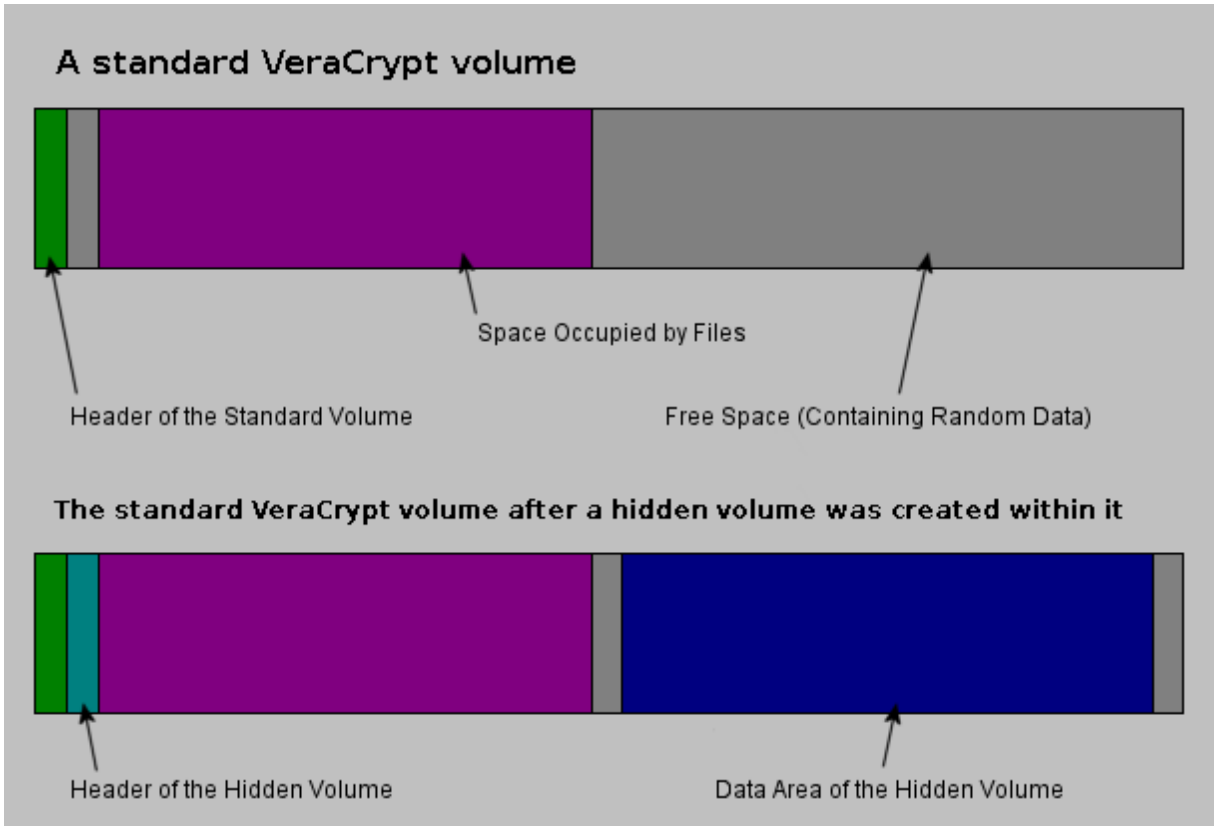
Πλέον, τα ψηφιακά δεδομένα κρυπτογραφούνται με χρήση κλειδιών κρυπτογράφησης. Συγκεκριμένα χρησιμοποιείται η κρυπτογράφηση συμμετρικού κλειδιού και η κρυπτογράφηση δημοσίου κλειδιού. Στην κρυπτογράφηση συμμετρικού κλειδιού το ίδιο κλειδί που χρησιμοποιείται για τη κρυπτογράφηση της πληροφορίας χρησιμοποιείται και για την αποκρυπτογράφησή της, ενώ στην κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιείται ένα δημόσιο και ένα ιδιωτικό κλειδί. Αν η πληροφορία κρυπτογραφηθεί με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και, αντίθετα, αν κρυπτογραφηθεί με το ιδιωτικό κλειδί η αποκρυπτογράφηση είναι δυνατή μόνο με το δημόσιο κλειδί. Οι δύο αυτοί τύποι κρυπτογραφίας εφαρμόζονται σε οποιονδήποτε τύπο δεδομένων, καθώς η κρυπτογράφηση πραγματοποιείται σε επίπεδο bit.

Η δυσκολία στην αντιμετώπιση της κρυπτογραφίας -όταν τα κλειδιά δεν είναι διαθέσιμα με τον οποιονδήποτε τρόπο- έγκειται στη φύση των κλειδιών κρυπτογράφησης και τους περιορισμούς της υπάρχουσας τεχνολογίας. Τα κλειδιά κρυπτογράφησης είναι στην ουσία τυχαίες, μη προβλέψιμες σειρές από bits που μπορούν να βρεθούν μόνο με επίθεση εξαντλητικών δοκιμών (brute-force attack)

μέχρι να βρεθεί το κλειδί. Όμως, το μέγεθος των κλειδιών που χρησιμοποιείται από πολλούς αλγόριθμους, όπως ο AES και ο Twofish, είναι το ελάχιστο 128 bits. Πρακτικά αυτό σημαίνει πως για να βρεθεί το κλειδί πρέπει να γίνουν 2^{128} δοκιμές, κάτι που με την τρέχουσα διαθέσιμη τεχνολογία απαιτεί δισεκατομμύρια χρόνια για να γίνουν όλες οι δοκιμές [63]. Επιπλέον, αν δεν είναι γνωστός ο αλγόριθμος κρυπτογράφησης είναι δύσκολο αυτός να καθοριστεί από τα κρυπτογραφημένα δεδομένα, αφού το κρυπτογράφημα που προκύπτει από τους αλγόριθμους κρυπτογράφησης συμμετρικού και δημοσίου κλειδιού φαίνεται να αποτελείται από τυχαίους χαρακτήρες.

2.2.2.2 Εύλογη αποποίηση

Σε περίπτωση που ανιχνευτεί η χρήση κρυπτογραφίας είναι πιθανό ο χρήστης να εξαναγκαστεί να αποκαλύψει τα κλειδιά κρυπτογράφησης. Γι'αυτό το λόγο υπάρχουν τεχνικές που παρέχουν τη δυνατότητα εύλογης αποποίησης (plausible deniability), δηλαδή της άρνησης χρήσης κρυπτογραφίας ή τον ισχυρισμό χρήσης κρυπτογραφίας για εύλογους σκοπούς χωρίς να μπορεί να αποδειχθεί το αντίθετο ή να αμφισβητηθεί ο ισχυρισμός από οποιονδήποτε. Η αποποίηση κρυπτογραφίας ουσιαστικά πραγματοποιείται με χρήση εμφωλευμένης κρυπτογραφίας. Πιο συγκεκριμένα, εργαλεία όπως το VeraCrypt δημιουργούν κρυπτογραφημένους δίσκους ή αρχεία που συμπεριφέρονται ως κρυπτογραφημένοι δίσκοι, και η πρόσβασή στο περιεχόμενό τους γίνεται με τη χρήση κωδικού πρόσβασης [64]. Οι κρυπτογραφημένοι δίσκοι ή τα αρχεία φαίνεται να αποτελούνται από τυχαία δεδομένα και επομένως είναι δυνατή η ανίχνευσή τους λόγω της υψηλής τους εντροπίας σε σχέση με άλλους τύπους δεδομένων. Η αποποίηση κρυπτογραφίας επιτυγχάνεται όταν στο κρυπτογραφημένο μέσο δημιουργείται ένας κρυπτογραφημένος χώρος στον οποίο η πρόσβαση είναι δυνατή μόνο με ξεχωριστό κωδικό πρόσβασης, διαφορετικά ο χώρος αυτός δεν είναι ορατός με πρόσβαση στο αρχικά κρυπτογραφημένο μέσο [64]. Επομένως, θα μπορούσε κανείς να αποκαλύψει τον κωδικό πρόσβασης για το κρυπτογραφημένο μέσο που είναι ορατό από το σύστημα και περιέχει φαινομενικά ευαίσθητα αρχεία, χωρίς όμως να αποκαλύπτεται η ύπαρξη του εσωτερικού κρυπτογραφημένου χώρου. Αυτό συμβαίνει γιατί πρακτικά ο εσωτερικός κρυπτογραφημένος χώρος είναι τυχαία δεδομένα μέσα στα τυχαία δεδομένα τα οποία απαρτίζουν το κρυπτογραφημένο μέσο. Στο σχήμα 2.1 απεικονίζεται η δομή ενός κρυπτογραφημένου τόμου και ενός κρυφού τόμου που δημιουργείται με το εργαλείο VeraCrypt.



Σχήμα 2.1 Δομή κρυπτογραφημένου και κρυφού τόμου με χρήση του εργαλείου VeraCrypt, όπως απεικονίζεται στο[64]

2.2.3 Στεγανογραφία

Στεγανογραφία είναι η απόκρυψη της πληροφορίας σε ένα άλλο μέσο. Σε αντίθεση με την κρυπτογραφία, όπου η ίδια η πληροφορία μετατρέπεται σε μια ακατάληπτη μορφή και είναι εύκολο να ανιχνευτεί, με τη χρήση στεγανογραφίας η πληροφορία κρύβεται σε ένα άλλο μέσο (κείμενο, εικόνα, ήχος, βίντεο) χωρίς να επιφέρει αντιληπτές τροποποιήσεις στο μέσο. Κατά συνέπεια, ο εντοπισμός της στεγανογραφίας δεν είναι εύκολος. Ουσιαστικά, αν δύο οντότητες επικοινωνούν η στεγανογραφία αποσκοπεί στην απόκρυψη της ίδιας της επικοινωνίας, ενώ η κρυπτογραφία αποσκοπεί στην απόκρυψη της πληροφορίας που ανταλλάσσεται. Υπάρχουν δύο τύποι στεγανογραφίας, η καθαρή στεγανογραφία (pure steganography) και η στεγανογραφία μυστικού κλειδιού (secret key steganography).

Για την εφαρμογή της καθαρής στεγανογραφίας απαιτείται το μέσο κάλυψης (cover), η πληροφορία που θα ενσωματωθεί στο μέσο και ο αλγόριθμος που θα χρησιμοποιηθεί ώστε να πραγματοποιηθεί η ενσωμάτωση. Στην στεγανογραφία μυστικού κλειδιού απαιτείται επιπλέον και ένα κλειδί με το οποίο πραγματοποιείται η διαδικασία της ενσωμάτωσης [65]. Η χρήση του μυστικού κλειδιού προσθέτει ένα επίπεδο ασφάλειας, αφού ακόμα και αν είναι γνωστός ο αλγόριθμος με τον οποίο έχει πραγματοποιηθεί η στεγανογραφία, δεν είναι δυνατή η ανάκτηση της κρυμμένης πληροφορίας χωρίς το κλειδί. Αντίθετα, στην καθαρή στεγανογραφία η πληροφορία είναι ασφαλής όσο παραμένει άγνωστη η χρήση στεγανογραφίας. Επιπλέον, καθώς κάθε εργαλείο στεγανογραφίας έχει διαφορετική υλοποίηση, για τη στεγανάλυση, δηλαδή την ανάκτηση της κρυμμένης πληροφορίας, απαιτείται το ίδιο εργαλείο με το οποίο πραγματοποιήθηκε η στεγανογραφία. Υπάρχουν και τεχνικές οι οποίες δεν

απαιτούν χρήση εργαλείων και στην ουσία αποτελούν τεχνάσματα, όπως, για παράδειγμα, η χρήση λευκού χρώματος κειμένου σε λευκό φόντο, η απόκρυψη κειμένου πίσω από εικόνες σε έγγραφα κειμένου και παρουσιάσεις ή η προσθήκη δεδομένων μετά τα τελευτα bytes ενός αρχείου εικόνας.

2.2.4 Rootkits

Όπως αναφέρθηκε στο πρώτο κεφάλαιο, η συλλογή δεδομένων πραγματοποιείται και σε συστήματα όσο βρίσκονται σε λειτουργία. Η ανάλυση ενός συστήματος σε λειτουργία δίνει τη δυνατότητα συλλογής πολύτιμων δεδομένων που χάνονται όταν τερματίζεται το σύστημα, όπως τρέχουσες διεργασίες, διαδικτυακές συνδέσεις, κλειδιά κρυπτογράφησης, συνδεδεμένοι χρήστες και άλλες πληροφορίες αποθηκευμένες στη μνήμη RAM. Επίσης, όσο το σύστημα είναι σε λειτουργία, κρυπτογραφημένες πληροφορίες βρίσκονται στη μνήμη σε μορφή απλού κειμένου, όπως, για παράδειγμα κωδικοί πρόσβασης και συνομιλίες. Τέλος, η ανάλυση ενεργών συστημάτων πραγματοποιείται όταν δεν είναι δυνατή η διακοπή της λειτουργίας τους, όπως στην περίπτωση που το σύστημα λειτουργεί ως εξυπηρετητής.

Μία τεχνική anti-forensics που επηρεάζει τη συλλογή δεδομένων και την ανάλυση συστημάτων σε λειτουργία είναι η χρήση προγραμμάτων rootkits. Τα rootkits είναι προγράμματα τα οποία παρέχουν πρόσβαση επιπέδου διαχειριστή σε ένα σύστημα παραμένοντας κρυφά από το σύστημα [66], και χρησιμοποιούνται για να κρύψουν αρχεία και διεργασίες. Αυτό που καθιστά τα rootkits κακόβουλα είναι η χρήση τους σε συνδυασμό με κακόβουλο λογισμικό το οποίο αποκρύπτουν από το σύστημα. Έτσι, για παράδειγμα, θα μπορούσε σε ένα σύστημα να εκτελείται ένα πρόγραμμα που τροποποιεί ή καταστρέφει δεδομένα, αποκρύπτει διαδικτυακές συνδέσεις, τροποποιεί τις ρυθμίσεις του συστήματος ή παρεμποδίζει τη λειτουργία των εργαλείων του ερευνητή που χρησιμοποιούνται για την αναζήτηση και συλλογή δεδομένων [66].

2.2.5 Άλλες τεχνικές

Οι παραπάνω μέθοδοι για την απόκρυψη πειστηρίων είναι ανεξάρτητες από το σύστημα στο οποίο εφαρμόζονται. Για παράδειγμα, η κρυπτογραφία περιλαμβάνει ένα ευρύ φάσμα τεχνικών για την κρυπτογράφηση δεδομένων τα οποία μπορεί είτε να μεταφέρονται σε ένα δίκτυο, είτε να είναι αποθηκευμένα σε διάφορα αποθηκευτικά μέσα υπολογιστικών συστημάτων ή κινητών συσκευών. Υπάρχουν, όμως, και τεχνικές οι οποίες εκμεταλλεύονται συγκεκριμένες λειτουργίες ενός συστήματος ή ενός μέσου αποθήκευσης.

2.2.5.1 ADS

Το σύστημα αρχείων NTFS, που χρησιμοποιείται από το λειτουργικό σύστημα Windows, διαθέτει μία λειτουργία που ονομάζεται Alternate Data Streams (ADS) η οποία δημιουργήθηκε για λόγους συμβατότητας με το σύστημα αρχείων HFS (Hierarchical File System) του λειτουργικού συστήματος Macintosh [67]. Με τη λειτουργία ADS, εκτός από την κύρια ροή δεδομένων σε ένα αρχείο (που είναι τα ίδια τα δεδομένα τα οποία περιέχονται στο αρχείο αυτό), υποστηρίζονται και επιπλέον (εναλλακτικές) ροές δεδομένων [68]. Οι εναλλακτικές αυτές ροές δεδομένων παρέχουν τη δυνατότητα ενσωμάτωσης μεταδεδομένων αλλά και αρχείων σε άλλα αρχεία χωρίς να επηρεάζουν τη

λειτουργικότητα, το περιεχόμενο και το μέγεθος του αρχείου στο οποίο ενσωματώνονται. Ακόμα, τα δεδομένα που ενσωματώνονται με τη χρήση των ADS δεν είναι ορατά στο χρήστη, αλλά ούτε και σε εφαρμογές του συστήματος των Windows, ενώ δεν υπάρχει περιορισμός στον τύπο και στο μέγεθος του αρχείου που ενσωματώνεται σε κάποιο άλλο μέσο. Μέχρι και την έκδοση Vista του λειτουργικού συστήματος Windows ήταν δυνατή ακόμα και η απευθείας εκτέλεση κώδικα από ένα ADS [67]. Τα ADS αξιοποιούνται και από κακόβουλο λογισμικό, όπως το ransomware BitPaymer το οποίο αποθηκεύει αντίγραφα του σε κενά αρχεία με χρήση των ADS [69], ο ιός Win2K.Stream [70] και το Rustock Rootkit - Spam Bot [71]. Ωστόσο, πρέπει να σημειωθεί πως το ίδιο το λειτουργικό σύστημα και άλλα προγράμματα χρησιμοποιούν τα ADS για την αποθήκευση πληροφοριών σχετικών με κάποιο αρχείο ή πληροφοριών που σχετίζονται με τον χειρισμό του αρχείου από το σύστημα [67].

2.2.5.2 Ειδικές περιοχές στο δίσκο

Για την αποθήκευση αρχείων στο σκληρό δίσκο δεσμεύεται μία ή παραπάνω συστοιχίες από τομείς (sectors). Αν το αρχείο δεν καταλαμβάνει όλη τη δεσμευμένη συστοιχία, τότε ο χώρος που περισσεύει ονομάζεται slack space. Ο χώρος αυτός συχνά χρησιμοποιείται για την απόκρυψη αρχείων, καθώς με αυτόν τον τρόπο δεν είναι ορατά και προσβάσιμα από το σύστημα.

Για την απόκρυψη αρχείων αξιοποιούνται και δύο ειδικές περιοχές του δίσκου, η περιοχή HPA (Host Protected Area) και η περιοχή DCO (Device Configuration Overlay). Η περιοχή HPA περιλαμβάνει διαγνωστικά προγράμματα, προγράμματα επαναφοράς, boot sectors του λειτουργικού συστήματος, και είναι προσβάσιμη μόνο με ειδικά εργαλεία που ονομάζονται HPA-aware [72]. Η περιοχή DCO παρέχει τη δυνατότητα τροποποίησης του μεγέθους σκληρών δίσκων [72]. Το γεγονός ότι οι περιοχές HPA και DCO δεν είναι ορατές στο χρήστη, το λειτουργικό σύστημα και το BIOS, καθώς και το ότι το μέγεθός τους μπορεί να τροποποιηθεί ώστε να προσεγγίζει αυτό του σκληρού δίσκου, καθιστά τις περιοχές αυτές ιδανικές για την απόκρυψη κάθε είδους πληροφορίας από κώδικα μέχρι και εικόνες δίσκου (disk images) λειτουργικών συστημάτων [73].

Μία ακόμα τεχνική που αξίζει να αναφερθεί είναι η ακούσια σήμανση τομέων του δίσκου ως «bad sectors». Ένας τομέας μαρκάρεται ως «bad sector» από το λειτουργικό σύστημα ή το δίσκο όταν έχει υποστεί φυσική βλάβη ή αν συμβεί κάποιο λογικό σφάλμα κατά την εγγραφή δεδομένων στην περιοχή αυτή, έτσι ώστε να παραλείπεται από το λειτουργικό σύστημα [74]. Επομένως, η εγγραφή δεδομένων σε μία περιοχή του δίσκου και η σήμανσή της ως «bad sector» θα αποκρύψει τα δεδομένα αυτά από το λειτουργικό σύστημα, αλλά και από εργαλεία ανάλυσης πειστηρίων από το δίσκο [75].

2.3 Απόκρυψη Ιχνών

Η απόκρυψη ιχνών περιλαμβάνει τεχνικές για την καταστροφή ή την τροποποίηση δεδομένων που αποδεικνύουν κάποια ενέργεια ή οδηγούν στην πηγή αυτής. Οι τεχνικές αυτές αποσκοπούν στον αποπροσανατολισμό της έρευνας και επηρεάζουν τη φάση της εξέτασης, όταν είναι αδύνατος ο εντοπισμός ιχνών, και τη φάση της ανάλυσης, όταν τα ίχνη έχουν τροποποιηθεί ή πλαστογραφηθεί. Η εξαγωγή εσφαλμένων συμπερασμάτων λόγω των τροποποιημένων ιχνών έχει επιπτώσεις και στη φάση της έκθεσης αναφοράς.

2.3.1 Live OS και Εικονικές Μηχανές

Παρόλο που η καταστροφή και η απόκρυψη πειστηρίων μπορούν να δυσχεράνουν σημαντικά τη διαδικασία της έρευνας, θα ήταν σαφώς αποτελεσματικότερη η απώλεια πειστηρίων εξ' αρχής. Γι' αυτό το λόγο χρησιμοποιούνται τεχνικές και εργαλεία τα οποία αποσκοπούν στην εξάλειψη πειστηρίων από το σύστημα μετά τη χρήση τους.

Ένα live λειτουργικό σύστημα φορτώνει στον υπολογιστή από κάποιο εξωτερικό αποθηκευτικό μέσο, όπως USB stick (live USB), εξωτερικό δίσκο ή CD/DVD (live CD), χωρίς να αποθηκεύονται δεδομένα στο σκληρό δίσκο του συστήματος. Τα live λειτουργικά συστήματα χρησιμοποιούνται μεταξύ άλλων για την αποσφαλμάτωση ή επαναφορά ενός συστήματος και για την πραγματοποίηση ασφαλών συναλλαγών ή άλλων διαδικτυακών δραστηριοτήτων από μη έμπιστα συστήματα [76]. Υπάρχουν όμως και live λειτουργικά συστήματα τα οποία σχεδιάστηκαν για να παρέχουν ασφάλεια, ανωνυμία, και ιδιωτικότητα στο χρήστη παρέχοντας λειτουργίες, όπως διαγραφή δεδομένων μετά την απενεργοποίηση του συστήματος ή κρυπτογράφηση των δεδομένων που αποθηκεύονται στο αποθηκευτικό μέσο [77-78].

Οι Εικονικές Μηχανές (Virtual Machines) μπορούν επίσης να χρησιμοποιηθούν εναλλακτικά για τη «φιλοξενία» λειτουργικών συστημάτων στο ήδη υπάρχον λειτουργικό σύστημα. Οι Εικονικές Μηχανές εξομοιώνουν ένα υπολογιστικό σύστημα το οποίο, όμως, αποτελείται από λογισμικό (software) [79]. Επιπλέον, η εικονική μηχανή (από τη στιγμή που είναι αρχείο) μπορεί να «τρέχει» από κάποιο εξωτερικό μέσο αποθήκευσης, ενώ είναι ιδιαίτερα εύκολη η επαναφορά της σε μία αρχική κατάσταση ή η διαγραφή της εξαλείφοντας κάθε ίχνος δραστηριότητας που πραγματοποιήθηκε στην εικονική μηχανή.

2.3.2 Φορητές εφαρμογές

Φορητές (portable apps) είναι οι εφαρμογές οι οποίες δεν απαιτούν εγκατάσταση. Αυτό τις καθιστά ιδανικές για κακόβουλη χρήση αφού αφήνουν περιορισμένα ψηφιακά ίχνη στο σύστημα στο οποίο εκτελούνται, ενώ είναι δυνατή και η εκτέλεσή τους από κάποιο εξωτερικό αποθηκευτικό μέσο. Καθώς πολλά εργαλεία στεγανογραφίας είναι φορητά, η αδυναμία εύρεσής τους στο σύστημα πιθανόν να μην οδηγούσε τον ερευνητή στην αναζήτηση στεγανογραφημένων αρχείων, αλλά ακόμα και αν υπήρχε η υποψία χρήσης στεγανογραφίας η στεγανάλυση να ήταν δύσκολη ή ακόμα και αδύνατη χωρίς τη χρήση του εργαλείου με το οποίο πραγματοποιήθηκε η στεγανογραφία, ιδίως, αν το εργαλείο υλοποιεί κάποιον εξειδικευμένο αλγόριθμο στεγανογραφίας.

2.3.3 Πλαστογράφηση Πειστηρίων

Η πλαστογράφηση πειστηρίων έχει ως στόχο τον αποπροσανατολισμό της διερεύνησης περιστατικών ασφάλειας και περιλαμβάνει τεχνικές για τη δημιουργία ψευδών πειστηρίων με σκοπό την προσποίηση κάποιας άλλης οντότητας. Παράλληλα χρησιμοποιείται και για πρόσβαση σε συστήματα χρησιμοποιώντας στοιχεία που θεωρούνται αξιόπιστα από το σύστημα, ή για την απόκρυψη των στοιχείων του συστήματος του χρήστη. Η τροποποίηση των πληροφοριών MAC, που αναφέρθηκε στις τεχνικές καταστροφής πειστηρίων, αποτελεί και τεχνική πλαστογράφησης πειστηρίων, καθώς οι τροποποιημένες χρονοσφραγίδες αποτελούν ψευδείς πληροφορίες που μπορεί να οδηγήσουν σε λανθασμένα συμπεράσματα, αλλά και στην αδυναμία παρουσίασής τους ως πειστήρια. Μεταξύ των

δεδομένων που μπορούν να πλαστογραφηθούν βρίσκονται διευθύνσεις IP, διευθύνσεις MAC, διευθύνσεις ηλεκτρονικού ταχυδρομείου και η γεωγραφική τοποθεσία [80].

2.3.4 Δίκτυα Ανωνυμίας

2.3.4.1 Onion Routing

Η δρομολόγηση Onion είναι ένα σύστημα διαδικτυακής επικοινωνίας που παρέχει ανωνυμία στους χρήστες. Η ανωνυμία στην επικοινωνία επιτυγχάνεται με τη χρήση πολλαπλών ενδιάμεσων κόμβων και πολλαπλών επιπέδων κρυπτογράφησης [81]. Πιο συγκεκριμένα, ένας σταθμός χρησιμοποιεί έναν Onion Routing Proxy ο οποίος εγκαθιδρύει μία σύνδεση με τον προορισμό μέσω τυχαία επιλεγμένων Onion Routers. Ο αποστολέας για να στείλει ένα μήνυμα εφαρμόζει επίπεδα κρυπτογράφησης χρησιμοποιώντας για κάθε επίπεδο το δημόσιο κλειδί κάθε κόμβου (onion router). Με αυτόν τον τρόπο ο αρχικός κόμβος θα αποκωδικοποιήσει το πρώτο επίπεδο, χωρίς να είναι σε θέση να αποκωδικοποιήσει το επόμενο επίπεδο το οποίο είναι κρυπτογραφημένο με το κλειδί του επόμενου σταθμού. Το μήνυμα θα είναι πλήρως αποκρυπτογραφημένο μόνο στον κόμβο εξόδου (τελευταίος κόμβος) ο οποίος στην ουσία είναι αυτός που επικοινωνεί με τον παραλήπτη. Ένα ακόμα στοιχείο το οποίο συμβάλει στην ανωνυμία είναι το γεγονός πως κάθε κόμβος «γνωρίζει» μόνο τον προηγούμενο και τον επόμενο κόμβο, χωρίς να έχει πληροφορίες σχετικά με το αν είναι τελικοί, αρχικοί ή ενδιάμεσοι κόμβοι [81]. Έτσι, καθίσταται πρακτικά αδύνατη η ιχνηλάτηση της επικοινωνίας σε ένα τέτοιο δίκτυο.

2.3.4.2 Δίκτυα P2P

Τα δίκτυα peer-to-peer (P2P) αποτελούνται από ομότιμους κόμβους που μοιράζονται πόρους μεταξύ τους. Οι κόμβοι θεωρούνται ομότιμοι, καθώς ανα πάσα στιγμή μπορούν είτε να ζητήσουν είτε να προσφέρουν κάποιον πόρο, σε αντίθεση με το μοντέλο πελάτη-εξυπηρετητή (client-server) στο οποίο ο πόροι βρίσκονται στον εξυπηρετητή και οι πελάτες μπορούν μόνο να αιτηθούν κάποιον πόρο και ο εξυπηρετητής μόνο να προσφέρει τους αιτούμενους πόρους. Δίκτυα όπως το Freenet και το I2P (Invisible Internet Project) βασίζονται στο μοντέλο P2P παρέχοντας επιπλέον και ανωνυμία στους χρήστες.

Το δίκτυο Freenet είναι αδόμητο, δηλαδή, κάθε κόμβος στο δίκτυο συνδέεται τυχαία με γειτονικούς κόμβους. Αυτή η μορφή του δικτύου εξασφαλίζει ως έναν βαθμό την ανωνυμία των χρηστών, από τη στιγμή που δεν μπορεί να καθοριστεί με βεβαιότητα αν το εισερχόμενο αίτημα σε κάποιον κόμβο πηγάζει ή προωθείται από τον γειτονικό κόμβο από τον οποίο στάλθηκε το αίτημα [82]. Επιπλέον, τα δεδομένα που αποθηκεύονται σε κάθε κόμβο είναι κρυπτογραφημένα, ώστε να είναι δύσκολος ο καθορισμός τους από τον ιδιοκτήτη του κόμβου. Αυτό εξασφαλίζει την αποποίηση ευθύνης του ιδιοκτήτη όσον αφορά τα αποθηκευμένα αρχεία [82]. Παρομοίως, το I2P αποτελεί ένα P2P, αδόμητο δίκτυο που έχει ως στόχο την παροχή ανωνυμίας στους χρήστες. Ωστόσο, σε αντίθεση με το Freenet το οποίο ουσιαστικά αποτελεί ένα σύστημα κατανεμημένης αποθήκης αρχείων [82], το I2P εστιάζει στην παροχή ανώνυμης επικοινωνίας παρέχοντας και δυνατότητα διαμοιρασμού αρχείων [83].

2.3.5 VPN

Τα δίκτυα VPN (Virtual Private Network) είναι εικονικά δίκτυα που αξιοποιούν το δημόσιο Διαδίκτυο για τη δημιουργία εικονικών τοπικών δικτύων και την ανταλλαγή κρυπτογραφημένης κίνησης μεταξύ των οντοτήτων στο δίκτυο αυτό [84]. Πολύ συχνά, για λόγους ανωνυμίας ή παράκαμψης περιορισμών σε ιστοσελίδες, οι χρήστες του Διαδικτύου χρησιμοποιούν υπηρεσίες VPN εγκαθιδρύοντας μία VPN σύνδεση με έναν εξυπηρετητή της υπηρεσίας VPN μέσω του οποίου δρομολογείται η κίνηση του χρήστη από και προς το Διαδίκτυο. Πρακτικά αυτό σημαίνει πως στο Διαδίκτυο θα είναι «ορατά» τα στοιχεία του εξυπηρετητή και όχι του χρήστη. Καθώς η χρήση δικτύου Onion είναι ορατή από τους Παρόχους Υπηρεσιών Διαδικτύου (ISP – Internet Service Provider) η σύνδεση στο δίκτυο onion μπορεί να γίνει μέσω ενός εξυπηρετητή VPN (Onion over VPN), έτσι ώστε να αποκρύπτεται και η πρόσβαση στο δίκτυο [85].

2.4 Επίθεση σε εργαλεία και διαδικασίες

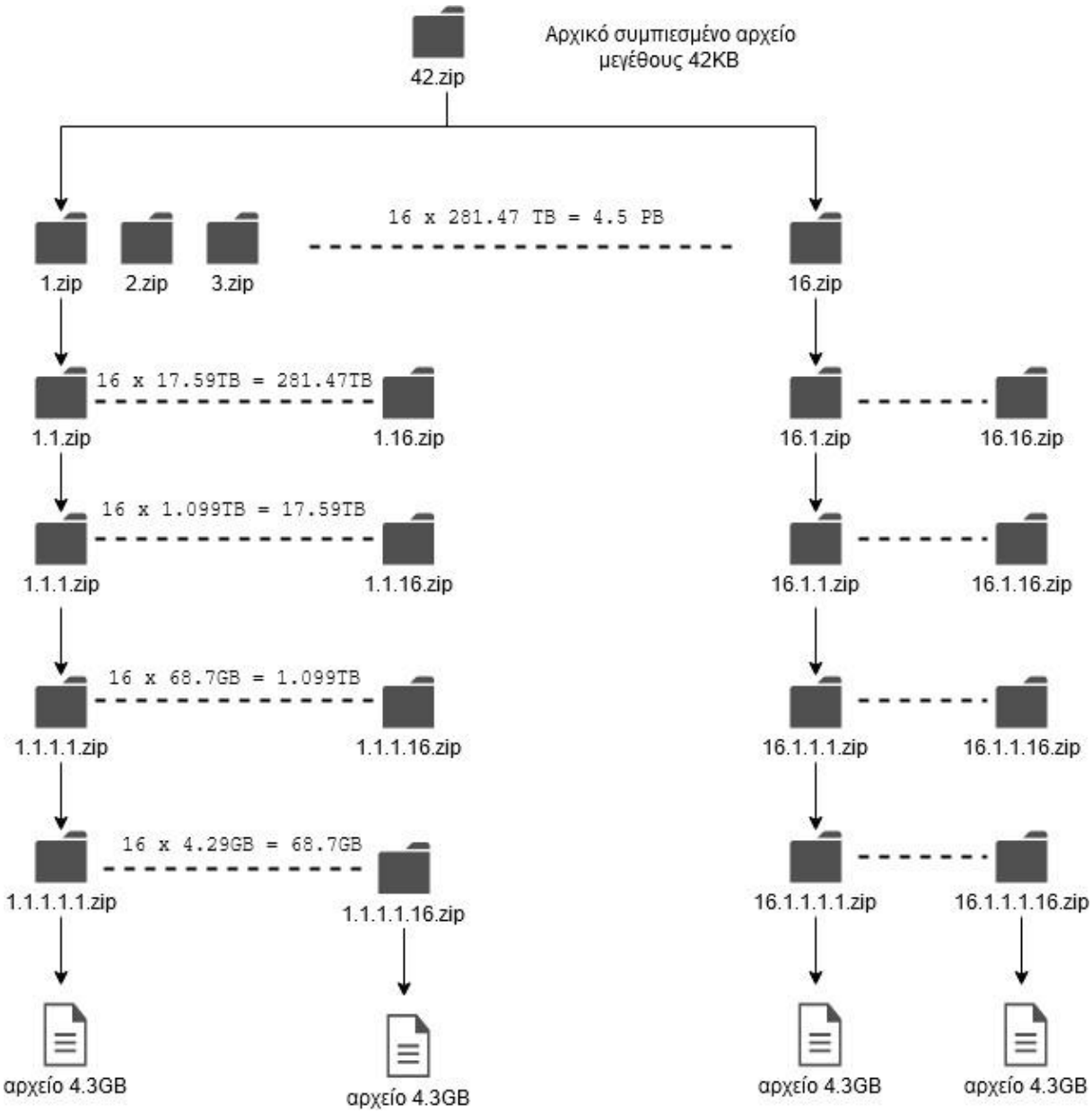
Μία ακόμα τεχνική που στοχεύει στην παρεμπόδιση της ερευνητικής διαδικασίας είναι η επίθεση στα εργαλεία και τις διαδικασίες της έρευνας. Η επίθεση στα εργαλεία αποσκοπεί στην παραγωγή εσφαλμένων αποτελεσμάτων και στη διακοπή της λειτουργίας των εργαλείων ή κάποιας φάσης της ερευνητικής διαδικασίας. Οι τεχνικές αυτής της κατηγορίας μπορούν να επηρεάσουν κάθε στάδιο της ερευνητικής διαδικασίας, από τη συλλογή των δεδομένων μέχρι και την σύνταξη αναφοράς.

Βασική επιδίωξη κατά τη διάρκεια μιας έρευνας αποτελεί η διασφάλιση της ακεραιότητας των ψηφιακών δεδομένων σε κάθε φάση της ερευνητικής διαδικασίας. Πλέον, η ελεύθερη πρόσβαση σε εργαλεία forensics, καθώς και η διαθέσιμη τεκμηρίωση των εργαλείων αυτών, δίνει τη δυνατότητα σε χρήστες να εντοπίσουν ευπάθειες στα εργαλεία [86]. Αυτό βεβαίως συμβάλει στην βελτίωση των εργαλείων, ωστόσο μπορεί κανείς να εκμεταλλευτεί τις ευπάθειες αποσκοπώντας στην υπονόμευση της αξιοπιστίας των πειστηρίων και της ομαλής διεξαγωγής της έρευνας.

Η τροποποίηση της υπογραφής αρχείων, η οποία αναφέρθηκε ως τεχνική στις μεθόδους απόκρυψης δεδομένων, μπορεί να θεωρηθεί και ως επίθεση στα εργαλεία τα οποία κάνουν αναζήτηση αρχείων με βάση την υπογραφή τους, αφού εμφανίζουν λανθασμένα αποτελέσματα. Οι B. Cusack και A. Homewood αναζητώντας σφάλματα (bugs) σε εργαλεία Forensics παρατήρησαν πως τροποποιημένα αρχεία (με αντικατάσταση τυχαίων byte στα αρχεία) οδηγούσαν ορισμένα εργαλεία σε κατάρρευση λόγω της αδυναμίας τους να επεξεργαστούν μη αναμενόμενη είσοδο. Κάτι τέτοιο μπορεί να επιφέρει σημαντικές καθυστερήσεις στη διαδικασία της έρευνας σε μια προσπάθεια του ερευνητή να εντοπίσει και να αντιμετωπίσει τα σφάλματα [30].

Ένας άλλος τύπος επίθεσης είναι η άρνηση εξυπηρέτησης (Denial of Service - DoS) η οποία έχει ως στόχο την εξάντληση πόρων του συστήματος που χρειάζεται ένα εργαλείο forensics για να λειτουργήσει. Ένας τύπος επίθεσης DoS είναι τα αρχεία «42.zip» [86][30]. Ένα αρχείο 42.zip έχει συμπιεσμένο μέγεθος 42KB, ωστόσο αν αποσυμπιεστεί πλήρως, τα αποσυμπιεσμένα αρχεία σαν σύνολο έχουν μέγεθος 4.5PB. Κατά συνέπεια, ένα εργαλείο forensics που ανοίγει αυτόματα τέτοιου τύπου αρχεία οδηγεί το σύστημα σε κατάρρευση [86]. Πιο συγκεκριμένα, το αρχικό συμπιεσμένο αρχείο περιέχει 16 συμπιεσμένα αρχεία μεγέθους 42KB, κάθε ένα από αυτά τα αρχεία περιλαμβάνει

συμπιεσμένα 16 αρχεία μεγέθους 42KB, τα οποία με τη σειρά τους περιλαμβάνουν 16 συμπιεσμένα αρχεία μεγέθους 42KB κ.ο.κ., και κάθε τελικό συμπιεσμένο αρχείο περιλαμβάνει ένα αρχείο 4.3GB. Έτσι δημιουργούνται πέντε επίπεδα συμπιεσμένων αρχείων. Για την καλύτερη κατανόηση της δομής του αρχείου δίνεται το σχήμα 2.2.



Σχήμα 2.2 Δομή αρχείου 42.zip

Σχετικά με την επίθεση στην ερευνητική διαδικασία, έγινε μία σύντομη αναφορά στο εργαλείο USBKill. Το USBKill είναι ένα πρόγραμμα που εκτελείται στο σύστημα και το τερματίζει αν ανιχνεύει κάποια άγνωστη συσκευή USB, αποσκοπώντας στην παρεμπόδιση της συλλογής δεδομένων από το σύστημα ή την ανάλυση του στην περίπτωση όπου χρησιμοποιούνται εργαλεία από κάποια εξωτερική συσκευή. Αυτού του είδους οι μηχανισμού ονομάζονται «kill switches» και χρησιμοποιούνται για τον άμεσο τερματισμό μίας ενέργειας. Ένα ακόμα εργαλείο, το Killswitch, παρέχει τη δυνατότητα στον χρήστη να τερματίσει τη συσκευή του (υπολογιστής ή κινητό) απομακρυσμένα [87].

Στον τομέα της ανάλυσης κακόβουλου λογισμικού (malware forensics) οι τεχνικές anti-debugging και anti-virtualization [88] που υλοποιούνται από ορισμένα malware, αποσκοπούν στην παρεμπόδιση της διαδικασίας της ανάλυσης. Τα εργαλεία αποσφαλμάτωσης (debugging) και οι εικονικές μηχανές προκαλούν αλλαγές στο υλικό και το γενικότερο περιβάλλον του συστήματος. Οι αλλαγές αυτές ανιχνεύονται από τα κακόβουλα προγράμματα τα οποία έχουν τη δυνατότητα ανίχνευσης της παρουσίας εργαλείων αποσφαλμάτωσης ή δημιουργίας εικονικών μηχανών που βρίσκονται εγκατεστημένα στο σύστημα ή εκτελούνται [88]. Έτσι, ένα κακόβουλο πρόγραμμα μπορεί να τροποποιήσει τη λειτουργία του ή να μην εκτελεστεί καθόλου δυσχεραίνοντας τη διαδικασία της ανάλυσής του.

Επίλογος

Σε αυτό το κεφάλαιο έγινε η ταξινόμηση και παρουσίαση σε θεωρητικό επίπεδο των πιο κοινών τεχνικών anti-forensics. Παρόλο που η κατηγοριοποίηση επιλέχθηκε με στόχο τη σαφή ταξινόμηση των τεχνικών, όπως προκύπτει από τη μελέτη τους, η κατηγοριοποίησή τους σχετίζεται και με τον τρόπο προσέγγισης αυτών. Για παράδειγμα, η τροποποίηση της υπογραφής και της κατάληξης ενός αρχείου, έχει ως αποτέλεσμα την απόκρυψη πειστηρίων, σε περίπτωση που το ενδιαφέρον της έρευνας περιορίζεται σε συγκεκριμένους τύπους αρχείων, αλλά και την επίθεση σε εργαλεία τα οποία θα εμφανίσουν λανθασμένα αποτελέσματα. Επίσης, η τροποποίηση μεταδεδομένων συγκαταλέγεται στην καταστροφή πειστηρίων όταν τα ίδια τα μεταδεδομένα αποτελούν πειστήρια, αλλά και στην απόκρυψη πειστηρίων σε περίπτωση που τροποποιηθούν οι χρονοσημάνσεις ενός αρχείου και θεωρηθεί εσφαλμένα πως χρονικά δεν σχετίζεται με το αντικείμενο της έρευνας. Η τροποποίηση μεταδεδομένων θα μπορούσε να θεωρηθεί και επίθεση σε εργαλεία τα οποία δημιουργούν χρονοδιάγραμμα γεγονότων βασιζόμενα στις χρονοσφραγίδες.

Κεφάλαιο 3 Εργαλεία και πρακτικές εφαρμογές Anti-Forensics

Εισαγωγή

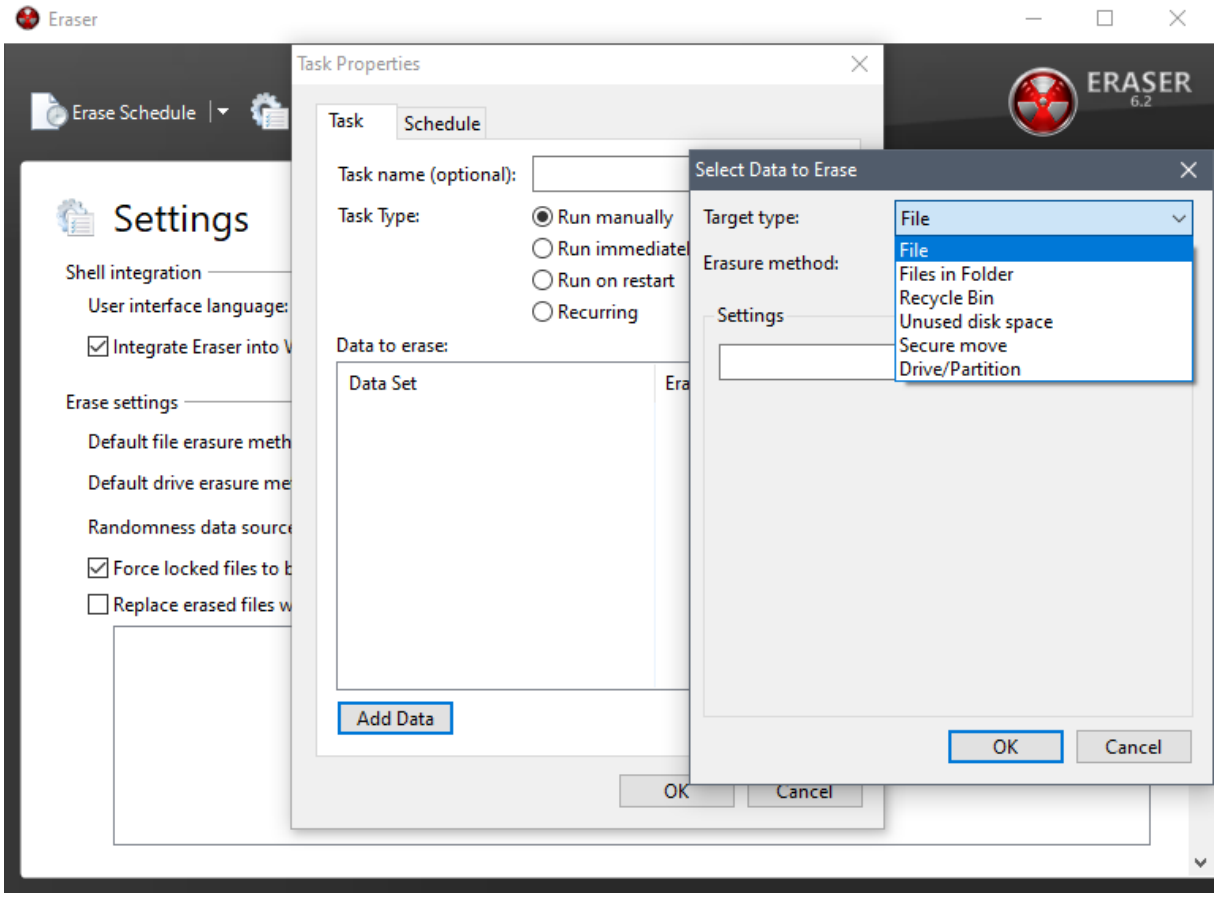
Αφού έχει γίνει μία πρώτη γνωριμία με τις βασικότερες τεχνικές anti-forensics σε θεωρητικό επίπεδο, στο τρίτο κεφάλαιο εφαρμόζονται πρακτικά ορισμένες τεχνικές με στόχο την καλύτερη κατανόηση των τεχνικών, αλλά και τη δυνατότητα αναγνώρισης και εντοπισμού τους κατά τη διεξαγωγή μιας έρευνας. Η εφαρμογή των τεχνικών πραγματοποιείται σε περιβάλλον Windows 10 Home, και για την ανάλυση των αποτελεσμάτων χρησιμοποιούνται ελεύθερα διαθέσιμα εργαλεία. Τα εργαλεία που χρησιμοποιούνται για την εφαρμογή των τεχνικών anti-forensics είναι επίσης ελεύθερα διαθέσιμα. Η ανάλυση εικόνων δίσκου γίνεται με το πρόγραμμα Autopsy, ένα ανοιχτού κώδικα εργαλείο ανάλυσης πειστηρίων [89]. Οι εικόνες δίσκων δημιουργήθηκαν με το εργαλείο FTKImager [90].

3.1 Εργαλεία καταστροφής δεδομένων

Τα εργαλεία καταστροφής δεδομένων που παρουσιάζονται είναι ελεύθερα διαθέσιμα και ανοικτού κώδικα. Πρέπει να σημειωθεί πως οι τεχνικές καθαρισμού δίσκων με επεγγραφή δεδομένων, και τα εργαλεία που αναφέρονται, είναι κατάλληλα μόνο για σκληρούς δίσκους (HDD) και όχι για δίσκους στερεάς κατάστασης (SSD). Κάθε κατασκευαστής δίσκων SSD διαθέτει δικό του πρόγραμμα ασφαλούς ολικής διαγραφής δεδομένων, ενώ η λειτουργία αυτή παρέχεται και από το BIOS αν υποστηρίζεται από τη μητρική πλακέτα του συστήματος.

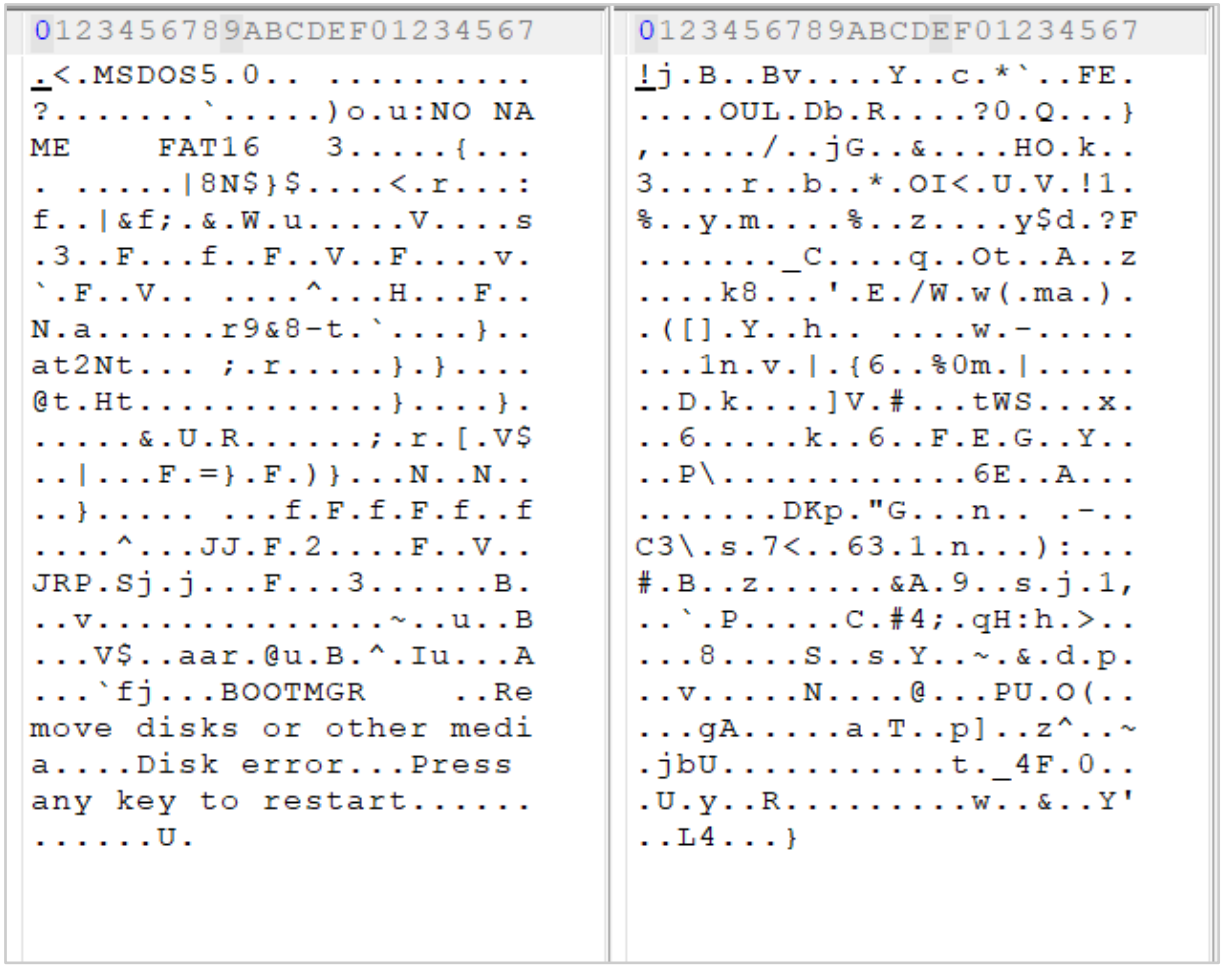
3.1.1 Eraser

Το εργαλείο Eraser [91] είναι, προς το παρόν, διαθέσιμο μόνο για το λειτουργικό σύστημα Windows. Ωστόσο, ο λόγος για τον οποίο επιλέχθηκε είναι ορισμένες από τις λειτουργίες του. Μία από αυτές τις λειτουργίες είναι η δυνατότητα δημιουργίας προγραμματισμένων ενεργειών, όπως για παράδειγμα η διαγραφή ενός δίσκου σε κάποια ορισμένη ημέρα και ώρα ή η επαναλαμβανόμενη διαγραφή στοιχείων ανά κάποια χρονική περίοδο. Μία ακόμα λειτουργία που παρέχει είναι η αντικατάσταση των διαγραμμένων αρχείων με κάποια άλλα επιλεγμένα αρχεία ώστε να καθιστά δυνατή την εύλογη αποποίηση ευθύνης, δηλαδή την άρνηση καταστροφής του αρχείου χωρίς δυνατότητα αμφισβήτησης. Το Eraser παρέχει τη δυνατότητα καταστροφής αρχείων, καθαρισμού δίσκων ή τμημάτων τους, καθώς και καθαρισμού ελεύθερων θέσεων στο δίσκο όπου πιθανόν να υπάρχουν προηγουμένως διαγραμμένα αρχεία. Οι βασικές λειτουργίες του εργαλείου Eraser, όπως ο προγραμματισμός διαγραφής και οι τύποι των διαγραφόμενων στοιχείων απεικονίζονται στο σχήμα 3.1.

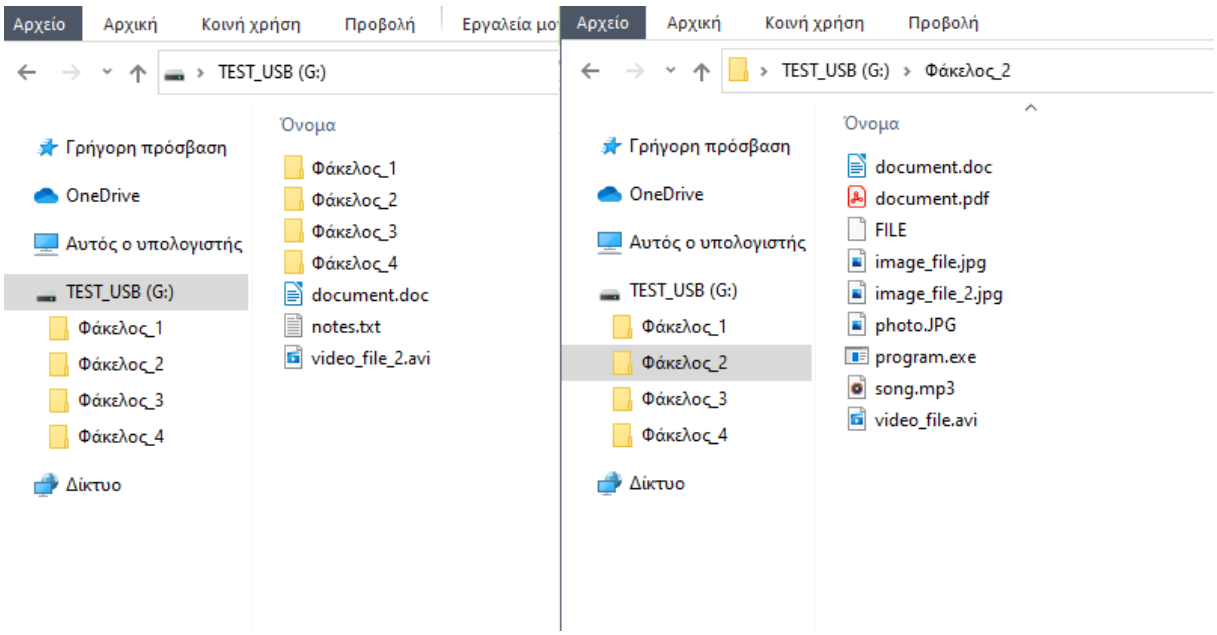


Σχήμα 3.1 Το εργαλείο Eraser

Μετά από τον καθαρισμό ενός USB stick με το εργαλείο Eraser και τη μέθοδο 'DoD 5220.22-M' (τριών περασμάτων επεγγραφής), το Autopsy δεν ήταν σε θέση να εξάγει δεδομένα από αυτό. Στο σχήμα 3.2 φαίνονται τα περιεχόμενα του USB stick, με τη χρήση ενός hex editor, πριν και μετά τον πλήρη καθαρισμό του με το εργαλείο Eraser.



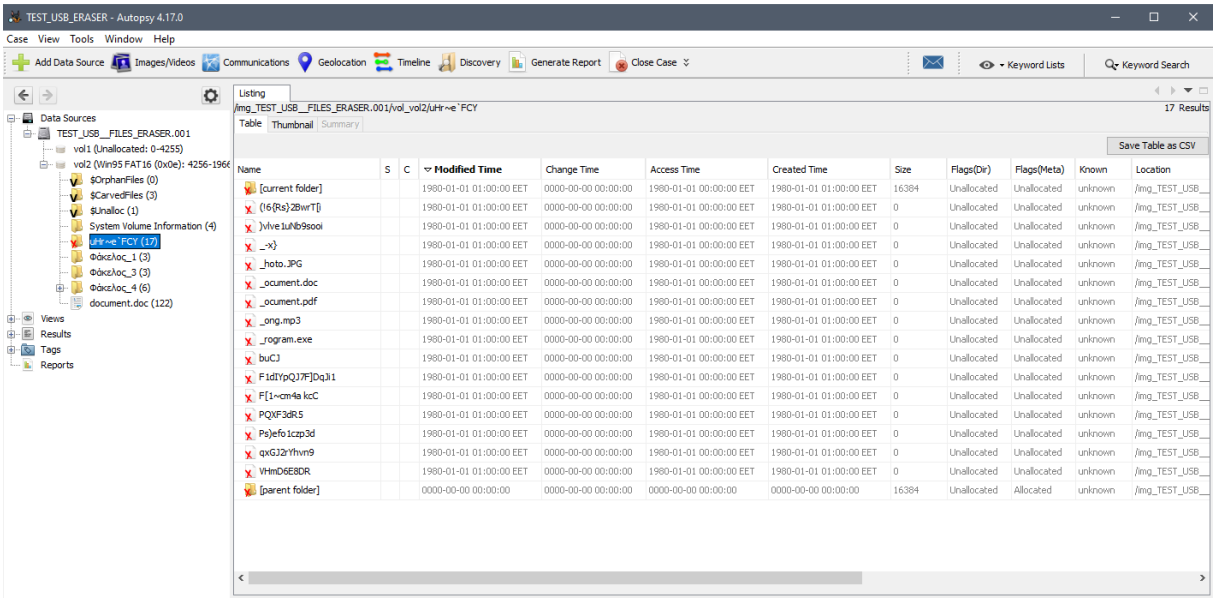
Σχήμα 3.2 Το περιεχόμενο ενός USB stick πριν (αριστερά) και μετά (δεξιά) την πλήρη διαγραφή του περιεχομένου του.



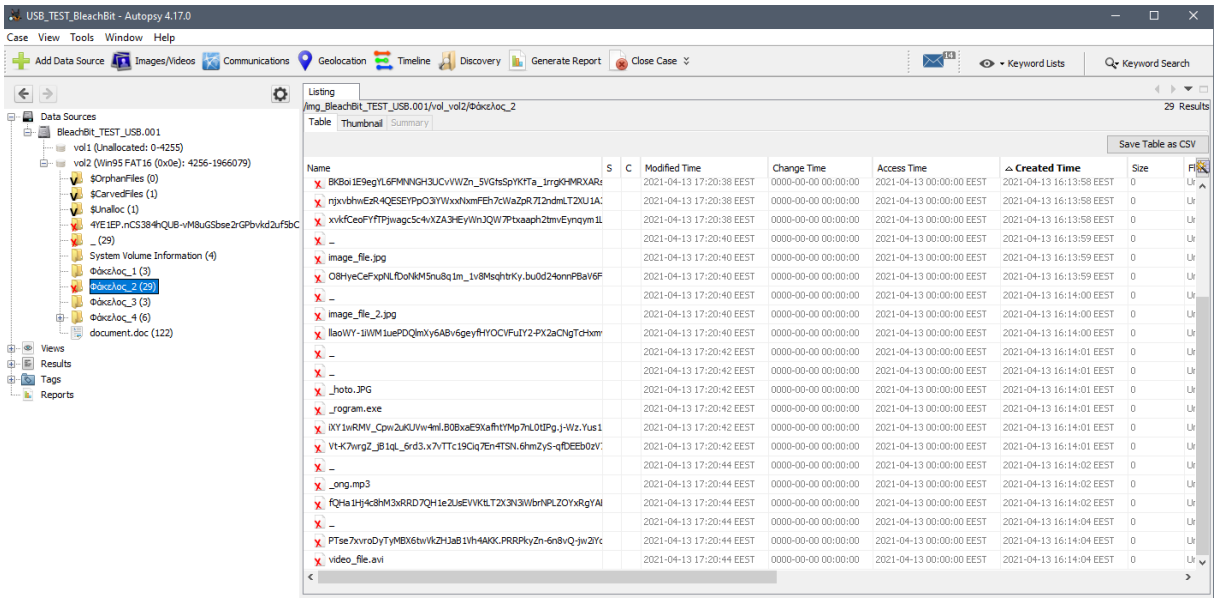
Σχήμα 3.3 Περιεχόμενο του USB stick

Στο παραπάνω σχήμα (σχήμα 3.3) φαίνονται τα αρχεία ένός USB stick. Αναλύοντάς το με το εργαλείο Autopsy μετά από διαγραφή του φακέλου ‘Φάκελος_2’ με το πρόγραμμα Eraser και δύο άλλων αρχείων εικόνας με απλή διαγραφή (χρήση συνδυασμού πλήκτρων Shift+Delete) παρατηρούμε τα εξής:

- Το όνομα του φακέλου που διαγράφηκε αντικαταστάθηκε με τυχαία σύμβολα.
- Οι χρονοσφραγίδες MAC των αρχείων που διαγράφηκαν έχουν την τιμή ‘1980-01-01 01:00:00 EET’ σε αντίθεση με τα αρχεία που διαγράφηκαν μέσω του συστήματος στα οποία οι χρονοσφραγίδες δεν επηρεάστηκαν.
- Μετά τη διαγραφή των αρχείων με το Eraser δεν είναι δυνατή η ανάκτηση των αρχείων, ενώ τα αρχεία που διαγράφηκαν είναι πλήρως ανακτήσιμα (από τη στιγμή που δεν έχουν επεγγραφεί με νέα δεδομένα).
- Από τα αρχεία που διαγράφηκαν με το εργαλείο Eraser διατηρήθηκαν ορισμένα από τα ονόματα των αρχείων.



Σχήμα 3.4 Εμφάνιση του περιεχομένου του USB stick στο πρόγραμμα Autopsy μετά την καταστροφή αρχείων με το Eraser



Σχήμα 3.5 Εμφάνιση του περιεχομένου του USB stick στο πρόγραμμα Autopsy μετά την καταστροφή αρχείων με το BleachBit

3.1.2 BleachBit

Το BleachBit [92] είναι ένα εργαλείο ασφαλούς καταστροφής αρχείων και φακέλων αλλά και άλλων δεδομένων του συστήματος, όπως ιστορικού αναζήτησης φυλλομετρητών, προσωρινής μνήμης εφαρμογών, αρχείων καταγραφής κ.α. Το εργαλείο αυτό επιλέχθηκε επειδή καλύπτει, μεταξύ άλλων, τα τρία δημοφιλέστερα λειτουργικά συστήματα (Windows, Linux, MacOS), αλλά και για τη φορητή έκδοση του εργαλείου που είναι διαθέσιμη για το λειτουργικό σύστημα Windows.

Μετά τη διαγραφή του φακέλου ‘Φάκελος_2’, τα ονόματα των αρχείων και του φακέλου διατηρούνται ωστόσο τα αρχεία δεν είναι ανακτήσιμα. Σε αντίθεση με το Eraser οι χρονοσφραγίδες δεν τροποποιούνται. Επιπλέον, παρατηρούμε στο σχήμα 3.5 πως ανάμεσα στα διαγραμμένα αρχεία εμφανίζονται εγγραφές που έχουν ως όνομα τυχαίες συμβολοσειρές ή τον χαρακτήρα ‘_’, κάτι που συμβαίνει και με τον φάκελο που διαγράφηκε.

3.1.3 DBAN

Το DBAN (Darik's Boot and Nuke) είναι ένα ακόμα ανοιχτού κώδικα εργαλείο ασφαλούς διαγραφής δεδομένων από σκληρούς δίσκους [93]. Το εργαλείο αυτό επιλέχθηκε επειδή είναι ανεξάρτητο λειτουργικού συστήματος και εκτελείται από κάποιο εξωτερικό μέσο αποθήκευσης. Επομένως, μπορεί να χρησιμοποιηθεί ακόμα και σε περίπτωση που το λειτουργικό σύστημα ή κάποιος σκληρός δίσκος δημιουργεί πρόβλημα στην ορθή λειτουργία του συστήματος καθώς και να διαγράψει τα δεδομένα του δίσκου στο οποίο βρίσκεται εγκατεστημένο το κύριο λειτουργικό σύστημα.

3.1.4 Unix utilities

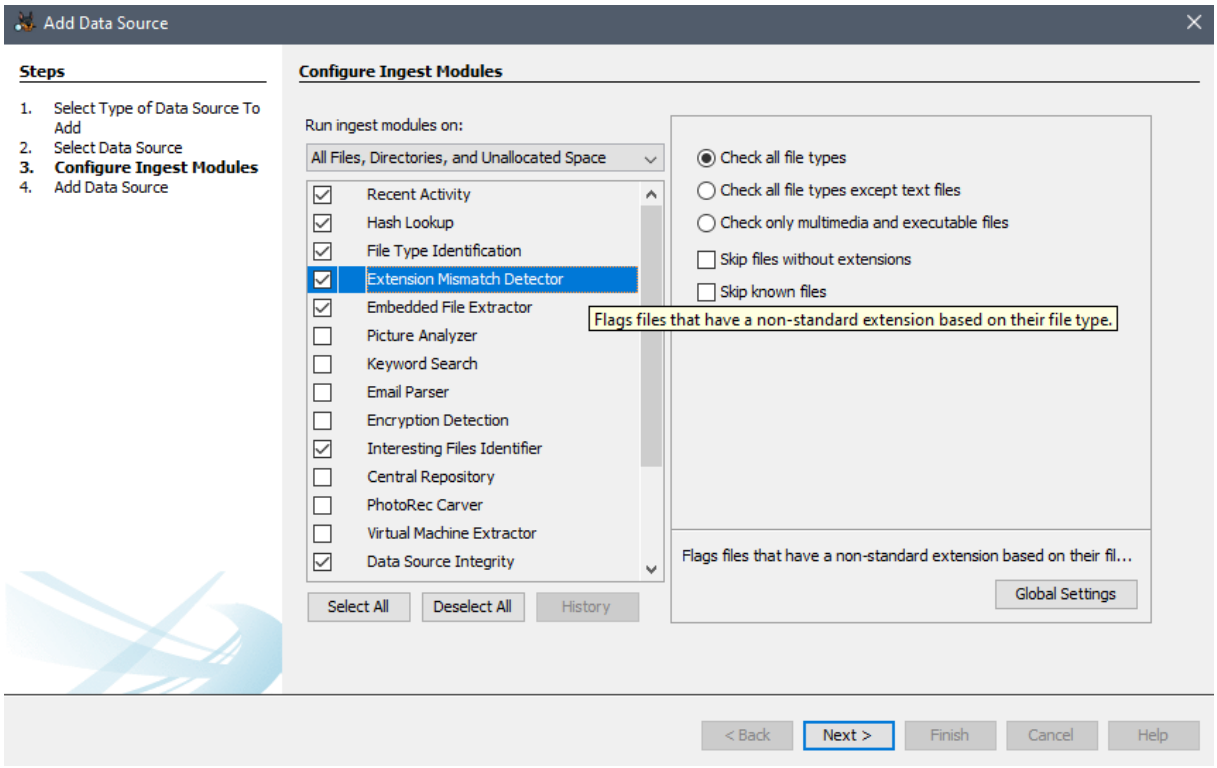
Τα λειτουργικά συστήματα Linux και Unix διαθέτουν προεγκατεστημένες εντολές οι οποίες μπορούν να αξιοποιηθούν για την ασφαλή καταστροφή αρχείων. Η εντολή dd [94] χρησιμοποιείται για αντιγραφή και μετατροπή δεδομένων, και χρησιμοποιείται από τους ερευνητές για τη δημιουργία αντιγράφου του δίσκου που προορίζεται για ανάλυση. Ωστόσο, μπορεί ακόμα να χρησιμοποιηθεί για την καταστροφή δεδομένων σε ένα αρχείο ή αποθηκευτικό μέσο. Με την εντολή 'dd if=/dev/zero of=/dev/sdX', όπου sdX το όνομα του δίσκου, εγγράφονται μηδενικά στον δίσκο που ορίζεται ως αρχείο εξόδου (output file - of). Επίσης, με την εντολή 'dd if=/dev/random of=/dev/sdX' εγγράφονται τυχαία δεδομένα στο δίσκο [95]. Ως έξοδος της εντολής μπορεί να οριστεί ένα αρχείο, ένας σκληρός δίσκος ή τμήμα αυτού. Η εντολή shred επεγγράφει αρχεία με μηδενικά ή με τυχαία bytes από ένα επιλεγμένο αρχείο και παρέχει τη δυνατότητα διαγραφής του αρχείου μετά την επεγγραφή [96]. Παρομοίως, η εντολή scrub χρησιμοποιείται για επεγγραφή δεδομένων με χρήση μεθόδων καταστροφής δεδομένων όπως DoD 5220.22-M και η Gutmann[4] [97].

3.2 Τροποποίηση δεδομένων

3.2.1 Τροποποίηση επεκτάσεων και υπογραφών

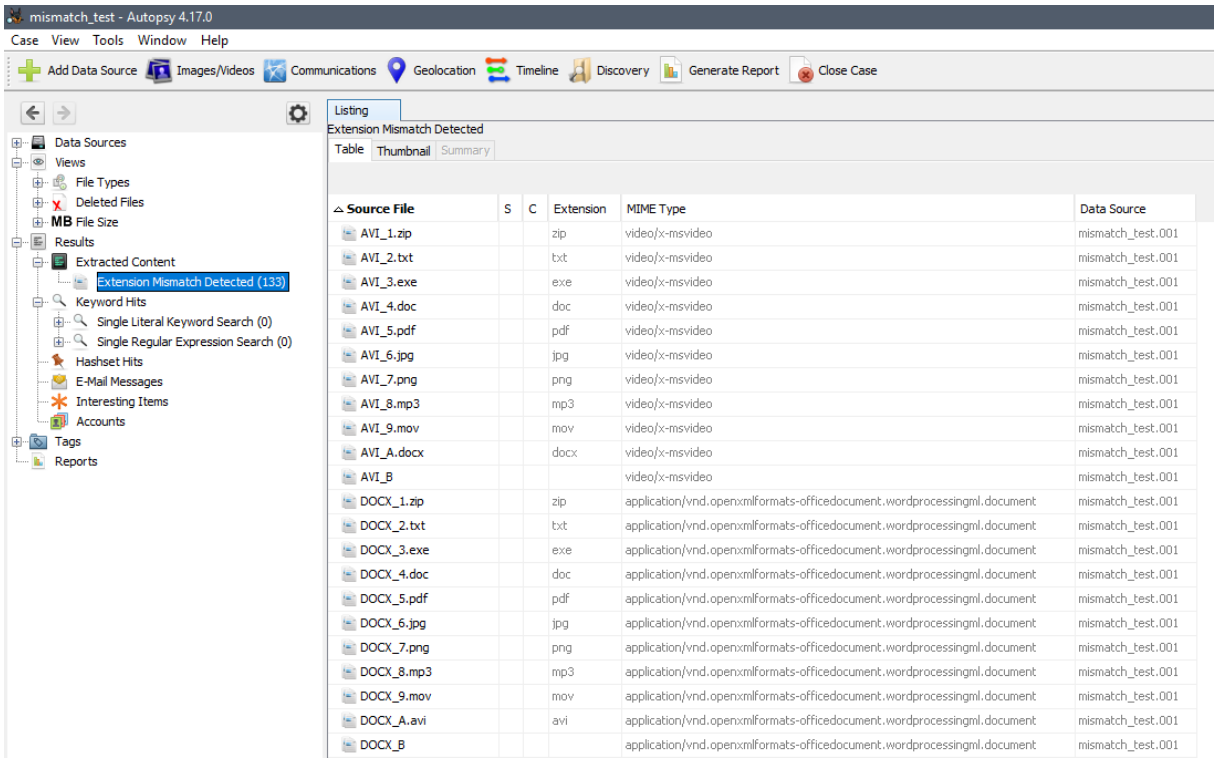
Μία πολύ απλή τεχνική απόκρυψης αρχείων είναι η αλλαγή της επέκτασης ενός αρχείου. Αν για παράδειγμα η έρευνα περιορίζεται σε αναζήτηση εικόνων και η κατάληξη ενός αρχείου εικόνας έχει αλλάξει σε κατάληξη εκτελέσιμου αρχείου, το αρχείο αυτό θα αγνοηθεί από εργαλεία που πραγματοποιούν αναζήτηση εξετάζοντας μόνο την κατάληξη των αρχείων. Ωστόσο, πολλά προγράμματα forensics παρέχουν τη δυνατότητα ανίχνευσης ασυμβατότητας της κατάληξης ενός αρχείου με την υπογραφή του. Για την παρουσίαση αυτής της τεχνικής χρησιμοποιήθηκε το εργαλείο ανοικτού κώδικα Autopsy και αρχεία κειμένου, εικόνας, ήχου, βίντεο, εκτελέσιμα και συμπιεσμένα αρχεία, με διαφορετικές καταλήξεις και χωρίς κατάληξη. Το Autopsy παρέχει τη δυνατότητα εντοπισμού ασυμβατότητας μεταξύ της υπογραφής του αρχείου και της κατάληξής του όπως φαίνεται και στο σχήμα 3.6.

[4] Η μέθοδος Gutmann εφαρμόζει 35 περάσματα επεγγραφής τυχαίων μοτίβων και καθορισμένων μοτίβων σε τυχαία σειρά.



Σχήμα 3.6 Επιλογή λειτουργίας εντοπισμού ασυμβατότητας μεταξύ υπογραφής και κατάληξης των αρχείων

Το Autopsy ήταν σε θέση να εντοπίσει την ασυμβατότητα μεταξύ τύπου αρχείου και επέκτασης (σχήμα 3.7) σε όλα τα αρχεία πλην των εκτελέσιμων αρχείων κάτι που σημαίνει πως η αλλαγή μόνο της κατάληξης ενός εκτελέσιμου αρχείου αρκεί για να την απόκρυψή του με αυτή την απλή τεχνική. Επίσης, το Autopsy δεν ανίχνευσε τα αρχεία ZIP με κατάληξη .docx και .xlsx, κάτι που οφείλεται στο ότι τα αρχεία ZIP μοιράζονται την ίδια υπογραφή με διάφορα αρχεία, όπως τα αρχεία docx και xlsx.



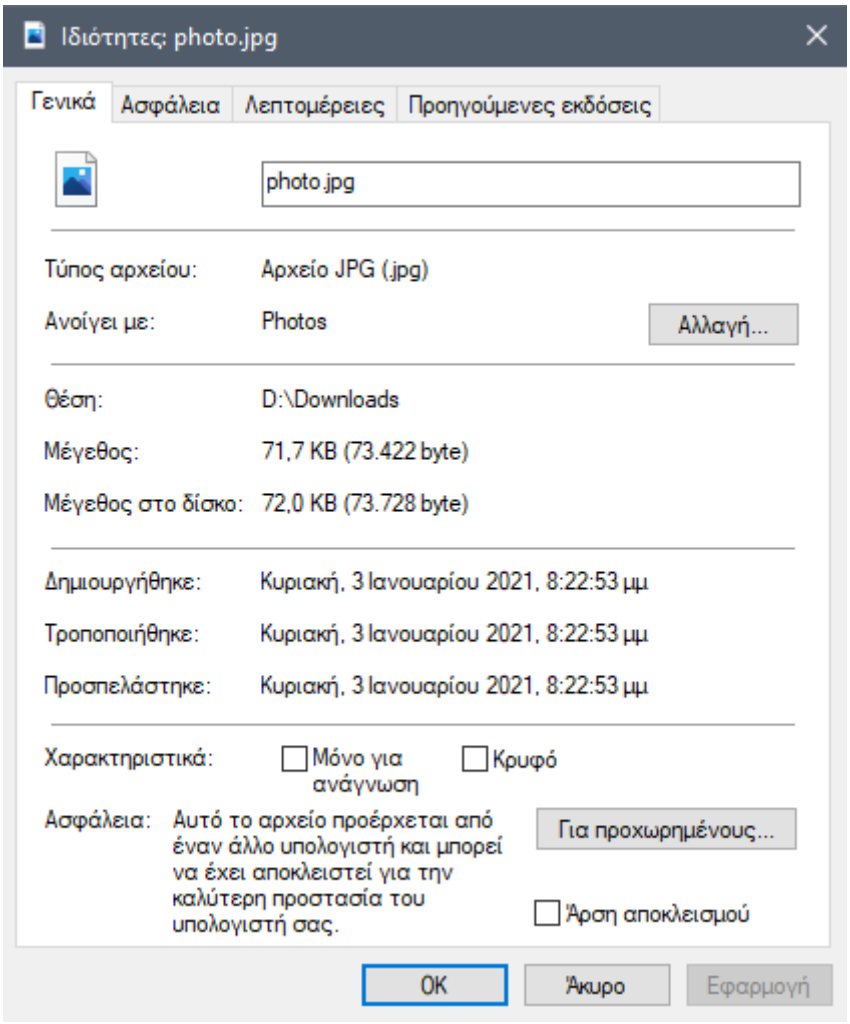
Σχήμα 3.7 Αποτελέσματα χρήσης της λειτουργίας ασυμβατότητας στο εργαλείο Autopsy

Για την αποφυγή ανίχνευσης ασυμβατότητας είναι δυνατόν να τροποποιηθεί και η υπογραφή ενός αρχείου. Η τροποποίηση των byte του αρχείου γίνεται με τη χρήση εργαλείων που ονομάζονται hex editors. Προσθέτοντας στα αρχεία τα byte της υπογραφής του τύπου αρχείου που υποδηλώνει η τροποποιημένη κατάληξή τους το Autopsy δεν εντόπισε καμία ασυμβατότητα. Για τα αρχεία με κατάληξη .txt και τα αρχεία χωρίς κατάληξη αρκεί η εισαγωγή χαρακτήρων που δεν ανήκουν σε κάποια υπογραφή. Με αυτόν τον τρόπο, θα μπορούσε κανείς να τροποποιήσει αρχεία όπως έγγραφα και εικόνες, ώστε να φαίνονται σαν αρχεία του συστήματος που δεν σχετίζονται με την έρευνα.

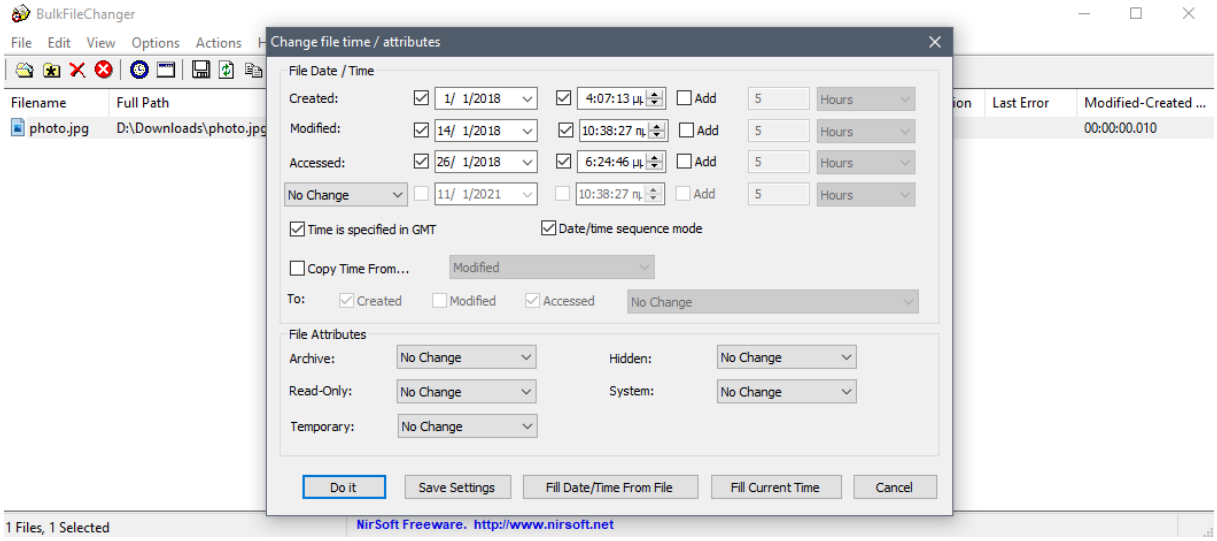
3.2.2 Τροποποίηση χρονοσφραγίδων

Οι χρόνοι MAC (Modification, Access, Creation) των αρχείων αποτελούν σπουδαία πηγή πληροφοριών, αφού μπορούν να αξιοποιηθούν για τη μείωση του όγκου των αρχείων που σχετίζονται με κάποια έρευνα, και βοηθούν στη δημιουργία χρονοδιαγραμμάτων των ενεργειών που έλαβαν χώρα σε κάποιο περιστατικό ασφάλειας. Καθώς οι χρόνοι MAC κατέχουν σημαντικό ρόλο στη διεξαγωγή ερευνών πρέπει να δίνεται ιδιαίτερη προσοχή στην ορθότητά τους, καθότι η τροποποίησή τους είναι πολύ εύκολη. Ένα εργαλείο με το οποίο μπορεί κανείς να τροποποιήσει αυτούς τους χρόνους είναι το BulkFileChanger από τη συλλογή εργαλείων Nirsoft για το λειτουργικό σύστημα Windows [98].

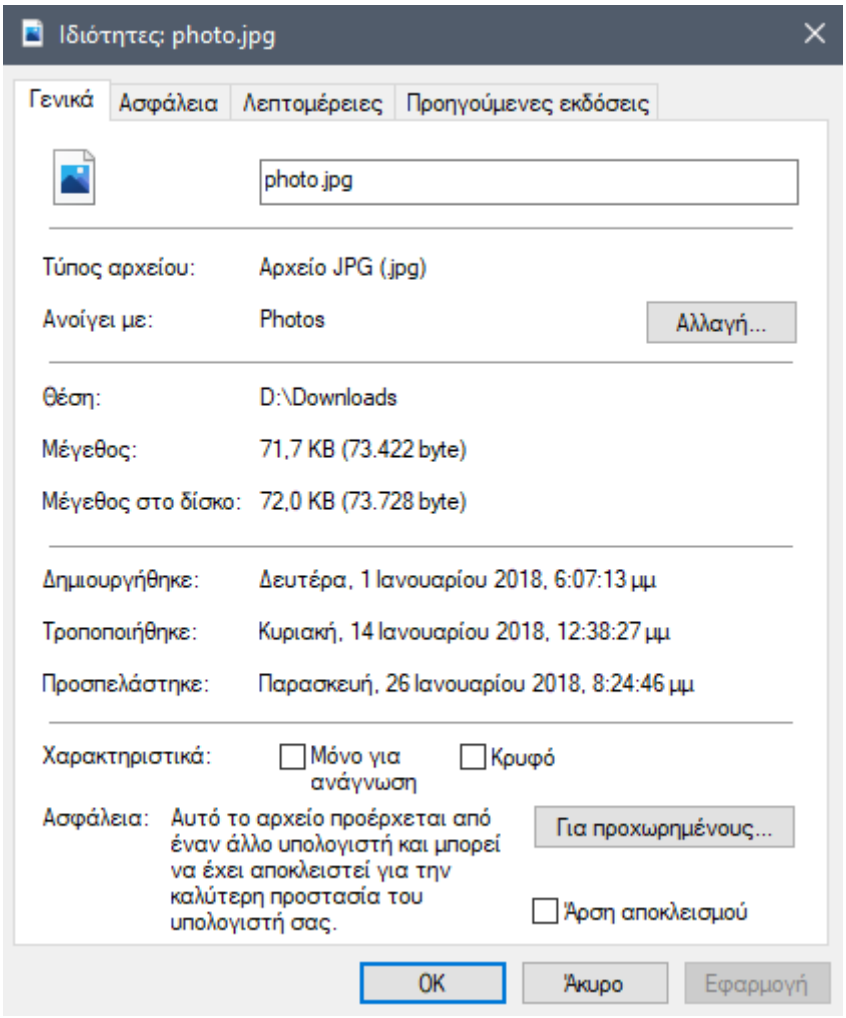
Διαθέτουμε ένα αρχείο εικόνας (“photo.jpg”) με τους χρόνους MAC που φαίνονται στο σχήμα 3.8. Το BulkFileChanger παρέχει μεταξύ άλλων τη δυνατότητα αλλαγής της ημερομηνίας και ώρας δημιουργίας, τροποποίησης και προσπέλασης του αρχείου (σχήμα 3.9).



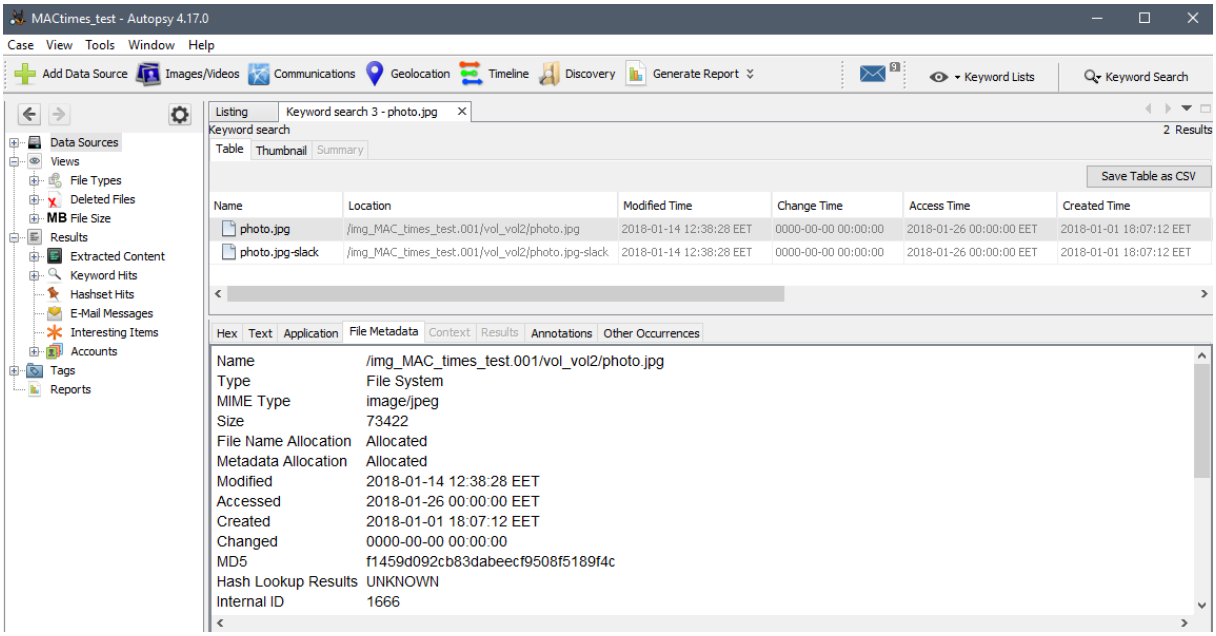
Σχήμα 3.8 Αρχικές χρονοσφραγίδες αρχείου



Σχήμα 3.9 Τροποποίηση χρονοσφραγίδων με το πρόγραμμα BulkFileChanger



Σχήμα 3.10 Εμφάνιση τροποποιημένων χρονοσφραγίδων από την εξερεύνηση αρχείων του συστήματος



Σχήμα 3.11 Εμφάνιση τροποποιημένων χρονοσφραγίδων στο Autopsy

Οι τροποποιημένοι χρόνοι είναι ορατοί από την εξερεύνηση αρχείων του συστήματος (σχήμα 3.10) αλλά και από το εργαλείο Autopsy (σχήμα 3.11).

Η ανίχνευση τροποποιήσεων στις χρονοσφραγίδες ενός αρχείου στο σύστημα αρχείων είναι δυνατή μέσα από την εξέταση δύο πεδίων, του $STANDARD_INFORMATION και του $FILE_NAME. Το σύστημα αρχείων NTFS διαθέτει αρχεία που ορίζουν και οργανώνουν το σύστημα αρχείων, όπως το αρχείο $AttrDef το οποίο περιέχει μία λίστα με πεδία στα οποία συγκαταλέγονται και τα δύο παραπάνω πεδία [99]. Και τα δύο πεδία περιλαμβάνουν τους χρόνους MAC ενός αρχείου, ωστόσο μία σημαντική διαφορά μεταξύ τους έγκειται στο γεγονός ότι οι εγγραφές του πεδίου $STANDARD_INFORMATION τροποποιούνται στο επίπεδο χρήστη (user space) του λειτουργικού συστήματος και είναι οι εγγραφές που «διαβάζει» η εξερεύνηση αρχείων και προγράμματα όπως το Autopsy. Αντίθετα, οι εγγραφές του πεδίου $FILE_NAME τροποποιούνται μόνο από τον πυρήνα (kernel) του λειτουργικού συστήματος [100]. Επομένως, συγκρίνοντας τις εγγραφές των χρόνων MAC στα πεδία $STANDARD_INFORMATION και $FILE_NAME είναι δυνατός ο εντοπισμός τροποποιήσεων των χρονοσφραγίδων. Ωστόσο, μετά από μετακίνηση ή μετονομασία του αρχείου σε άλλο φάκελο, το πεδίο $FILE_NAME αποκτά τους (τροποποιημένους) χρόνους του πεδίου $STANDARD_INFORMATION [100]. Είναι σημαντικό να λαμβάνεται υπόψη ο τρόπος με τον οποίο μεταβάλλονται οι χρονοσημάνσεις των δύο αυτών πεδίων ανάλογα με τις ενέργειες που δέχεται ένα αρχείο, αλλά και οι διαδικασίες που πιθανόν να τροποποιούν τις χρονοσημάνσεις, όπως, για παράδειγμα, σε περίπτωση σάρωσης των αρχείων από αντιικό πρόγραμμα. Στον πίνακα 3.1 καταγράφονται οι χρονοσημάνσεις που τροποποιούνται από διαφορετικές ενέργειες σε ένα αρχείο στο λειτουργικό σύστημα Windows [101-102].

Πίνακας 3.1 Ενέργειες και χρόνοι που τροποποιούνται (το '✔δηλώνει τροποποίηση)

	$STANDARD_INFORMATION			$FILE_NAME		
	Modified	Access	Creation	Modified	Access	Creation
Μετονομασία	-	-	-	-	-	-
Μετακίνηση (Τοπικά)	-	-	-	✔εκτός Windows 10	-	-
Μετακίνησ (Μεταξύ Τομέων)	-	✔	✔- στα Windows 10	✔	✔	✔
Αντιγραφή	-	✔	✔	✔	✔	✔
Πρόσβαση	-	✔- στα Windows 10	-	-	-	-
Τροποποίηση	✔	✔- στα Windows 10	-	✔- στα Windows 10	✔- στα Windows 10	-
Δημιουργία	✔	✔	✔	✔	✔	✔
Διαγραφή	-	-	-	-	-	-

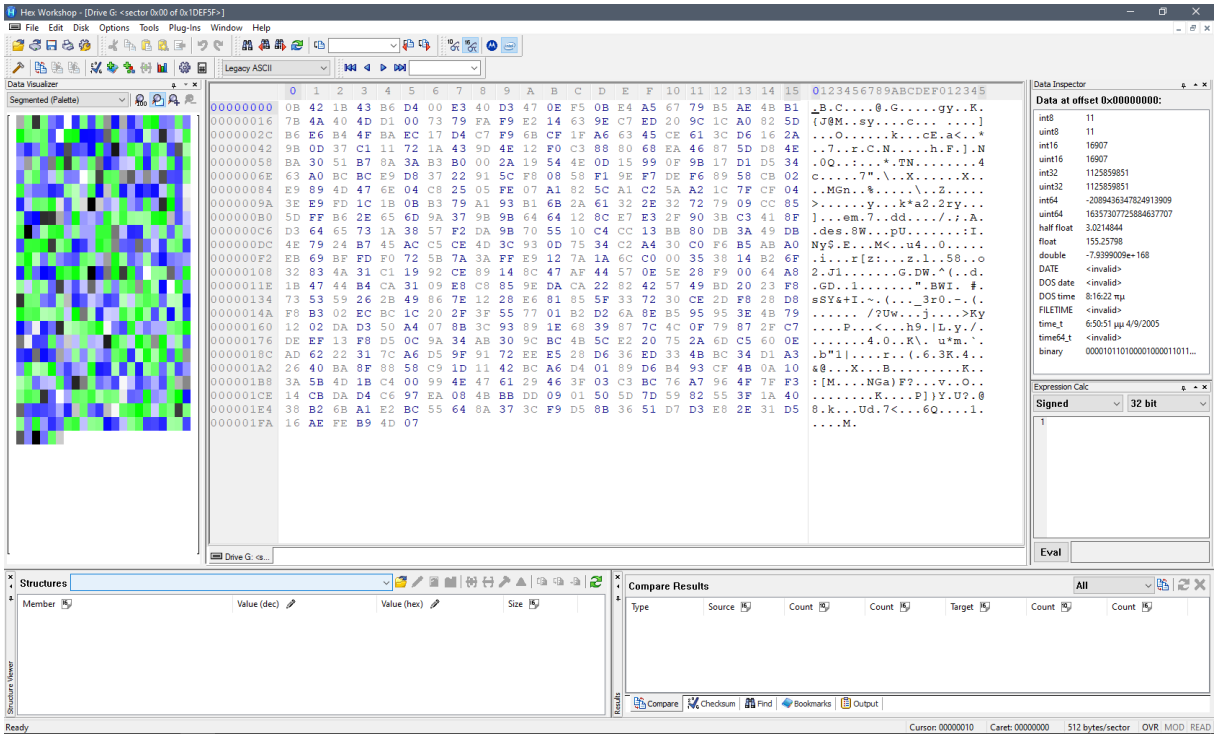
Οι Palmbach και Breitinger [100] εξέτασαν επιπλέον αρχεία του συστήματος, όπως το $USNjrnl το οποίο αποθηκεύει πληροφορίες σχετικά με αλλαγές σε αρχεία, linkfiles και αρχεία prefetch, στα οποία θα γίνει αναφορά στο 4ο κεφάλαιο, και αρχεία καταγραφής γεγονότων (Windows event logs). Έτσι, πρότειναν νέους κανόνες αναφορικά με τις χρονοσημάνσεις του πεδίου $STANDARD_INFORMATION ενός αρχείου σε σχέση με χρονοσημάνσεις των αρχείων του συστήματος [100].

3.3 Απόκρυψη αρχείων

3.3.1 VeraCrypt

Το VeraCrypt είναι ένα ελεύθερο, ανοικτού κώδικα πρόγραμμα και είναι διαθέσιμο για μία πληθώρα λειτουργικών συστημάτων. Παρέχει τη δυνατότητα κρυπτογράφησης αποθηκευτικών μέσων, δημιουργίας εικονικών κρυπτογραφημένων δίσκων καθώς και δημιουργίας κρυμμένων τόμων (volumes), ακόμα και λειτουργικών συστημάτων (αυτή τη στιγμή υποστηρίζονται μόνο εκδόσεις Windows) [64]. Όταν δημιουργείται ένα αρχείο εικονικού κρυπτογραφημένου δίσκου, το αρχείο δεν χρειάζεται επέκταση και δεν φαίνεται να έχει κάποια υπογραφή, αλλά αποτελείται από τυχαία bytes, με αποτέλεσμα να είναι αδύνατη η αναγνώρισή του ως δίσκου με κάποια βεβαιότητα. Για να λειτουργήσει το αρχείο αυτό ως δίσκος πρέπει να γίνει η προσάρτησή του (mount) μέσα από το πρόγραμμα και να εισαχθεί ο κωδικός που επιλέχθηκε κατά τη δημιουργία του εικονικού δίσκου [64].

Δοκιμάζοντας να εισάγουμε μία κρυπτογραφημένη μονάδα δίσκου (ένα USB stick) σε ένα σύστημα με Windows 10, το σύστημα ζητάει διαμόρφωση του δίσκου, καθώς δεν είναι σε θέση να εντοπίσει κάποιο σύστημα αρχείων. Εξετάζοντας το δίσκο με έναν hex editor (σχήμα 3.12), παρατηρούμε πως το περιεχόμενό του είναι παρόμοιο με την περίπτωση της διαγραφής δεδομένων με επεγγραφή, όπως παρουσιάστηκε παραπάνω, στο υποκεφάλαιο για την καταστροφή δεδομένων (σχήμα 3.2). Επομένως, θα μπορούσε κανείς να υποθέσει πως στη μονάδα δίσκου έχει γίνει καταστροφή δεδομένων, ενώ στην πραγματικότητα είναι ένας κρυπτογραφημένος δίσκος.



Σχήμα 3.12 Εξέταση μονάδας δίσκου σε πρόγραμμα hex editor μετά την κρυπτογράφησή του με το εργαλείο VeraCrypt

3.3.2 Στεγανογραφία

Για την εφαρμογή στεγανογραφίας υπάρχουν εργαλεία τα οποία είτε υλοποιούν γνωστούς αλγορίθμους όπως ο LSB και ο MF-5 ή κάποιον αποκλειστικό αλγόριθμο. Ο εντοπισμός στεγανογραφίας δεν είναι εύκολος, ιδίως, αν δεν υπάρχει στο σύστημα και το μέσο (αρχείο) που χρησιμοποιήθηκε για την ενσωμάτωση της πληροφορίας, έτσι ώστε να γίνει σύγκριση του μέσου πριν και μετά τη στεγανογραφία. Αν δηλαδή υπάρχει το αρχείο διπλότυπο με διαφορά στο μέγεθος του ή στην τιμή hash, τότε πολύ πιθανό το αρχείο αυτό να χρησιμοποιήθηκε ως φορέας για την απόκρυψη κάποιου μηνύματος ή αρχείου. Ωστόσο, καθώς το αρχείο-φορέας μπορεί να έχει διαγραφεί, να βρίσκεται σε διαφορετικό μέρος στο σύστημα ή σε εξωτερικό αποθηκευτικό μέσο, αυτή η προσέγγιση είναι ασύμφορη πόσο μάλλον όταν ο όγκος τον συλλεχθέντων δεδομένων είναι πολύ μεγάλος.

Μία άλλη προσέγγιση είναι ο εντοπισμός εργαλείων στεγανογραφίας στο σύστημα, κάτι που θα υποδηλώνει πιθανή χρήση στεγανογραφίας για απόκρυψη δεδομένων [103]. Ορισμένα εργαλεία στεγανογραφίας απαιτούν εγκατασταση στο σύστημα ωστε να λειτουργήσουν (π.χ. Xiao Steganography, Invisible Secrets) καθιστώντας τον εντοπισμό τους πιο εύκολο από τα φορητά (portable) εργαλεία στεγανογραφίας τα οποία δεν απαιτούν εγκατάσταση και είναι δυνατή η εκτέλεσή τους από κάποιο εξωτερικό αποθηκευτικό μέσο. Παρόλα αυτά, ακόμα και τα φορητά προγράμματα αφήνουν ίχνη στο σύστημα. Τέλος, η χρήση εργαλείων που εντοπίζουν στεγανογραφία σε αρχεία αποτελεί μία ακόμα προσέγγιση. Υπάρχουν προγράμματα τα οποία εντοπίζουν συγκεκριμένους αλγόριθμους στεγανογραφίας όπως τα StegExpose και StegSecret τα οποία ανιχνεύουν στεγανογραφία LSB, και εργαλεία όπως το StegSpy που ανιχνεύουν στεγανογραφία από ορισμένα προγράμματα [104-106].

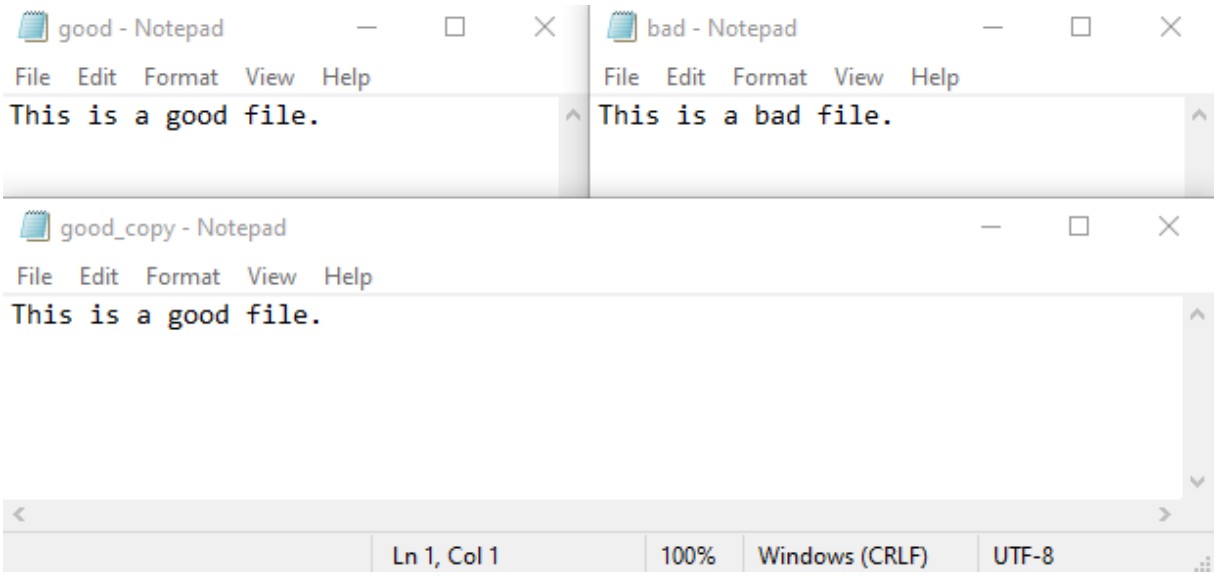
Ο πίνακας 3.2 περιλαμβάνει μερικά από τα πιο γνωστά εργαλεία στεγανογραφίας. Σκοπός του πίνακα είναι να αποτελέσει ένα σημείο αναφοράς ώστε αν ανιχνευτεί κάποιο από τα εργαλεία που καταγράφονται να προσανατολιστεί κατάλληλα η έρευνα. Για παράδειγμα, αν ανιχνευτεί το εργαλείο SteganPEG σε κάποιο σύστημα, περαιτέρω έρευνα θα περιοριστεί μόνο σε αρχεία εικόνας JPG, αφού είναι τα μόνα που υποστηρίζει το συγκεκριμένο πρόγραμμα ως μέσο κάλυψης. Βέβαια, πέρα από τα διαθέσιμα εργαλεία στεγανογραφίας υπάρχουν διαθέσιμες βιβλιοθήκες για την υλοποίηση στεγανογραφίας για διάφορες γλώσσες προγραμματισμού, ενώ θα μπορούσε κάποιος με γνώσεις προγραμματισμού να υλοποιήσει έναν δικό του αλγόριθμο στεγανογραφίας.

Πίνακας 3.2 Χαρακτηριστικά εργαλείων στεγανογραφίας

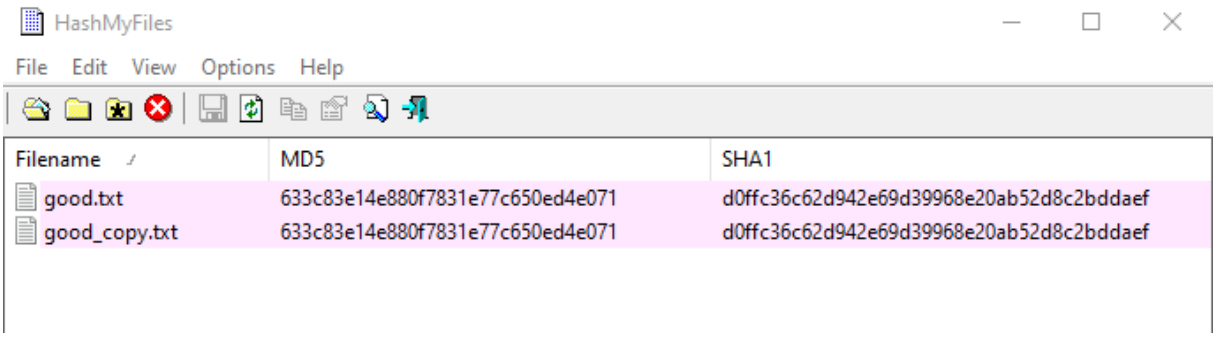
Πρόγραμμα	Υποστηριζόμενο μέσο (φορέας)	Υποστηριζόμενη πληροφορία	Αλγόριθμοι στεγανογραφίας	Εγκατάσταση	Κρυπτογράφηση πληροφορίας	Λειτουργικό Σύστημα
S-tools	BMP, GIF, WAV	Χωρίς περιορισμό	Ιδιωτικός αλγόριθμος	Όχι	IDEA, DES, 3DES, MDC	Windows
Steg-hide	BMP, JPG, WAV, AU	Χωρίς περιορισμό	Γραφο-θεωρητική προσέγγιση	Όχι	Blowfish, DES, 3DES, RC2, Rijndael, κ.α.	Windows, Linux, Unix
Hide'N'Send	JPG	Χωρίς περιορισμό	F5, M-F5, LSB, M-LSB	Όχι	AES, RC2, RC4	Windows
OpenStego	BMP, GIF, JPG, PNG	Χωρίς περιορισμό	RandomLSB	Ναι	AES	Windows, Linux, macOS
SteganPEG	JPG	Χωρίς περιορισμό	Ιδιωτικός αλγόριθμος	Ναι	Rotatocrypt	Windows
SSuite Picsel	BMP, JPG, PNG	Αρχεία TXT	Ιδιωτικός αλγόριθμος	Όχι	-	Windows
Xiao Steganography	BMP, WAV, PNG, WMF	Χωρίς περιορισμό	LSB	Ναι	DES, 3DES, RC2, RC4	Windows
StegoSuite	BMP, GIF, JPG, PNG	Χωρίς περιορισμό	Ιδιωτικός αλγόριθμος	Ναι	AES	Linux

3.3.3 ADS

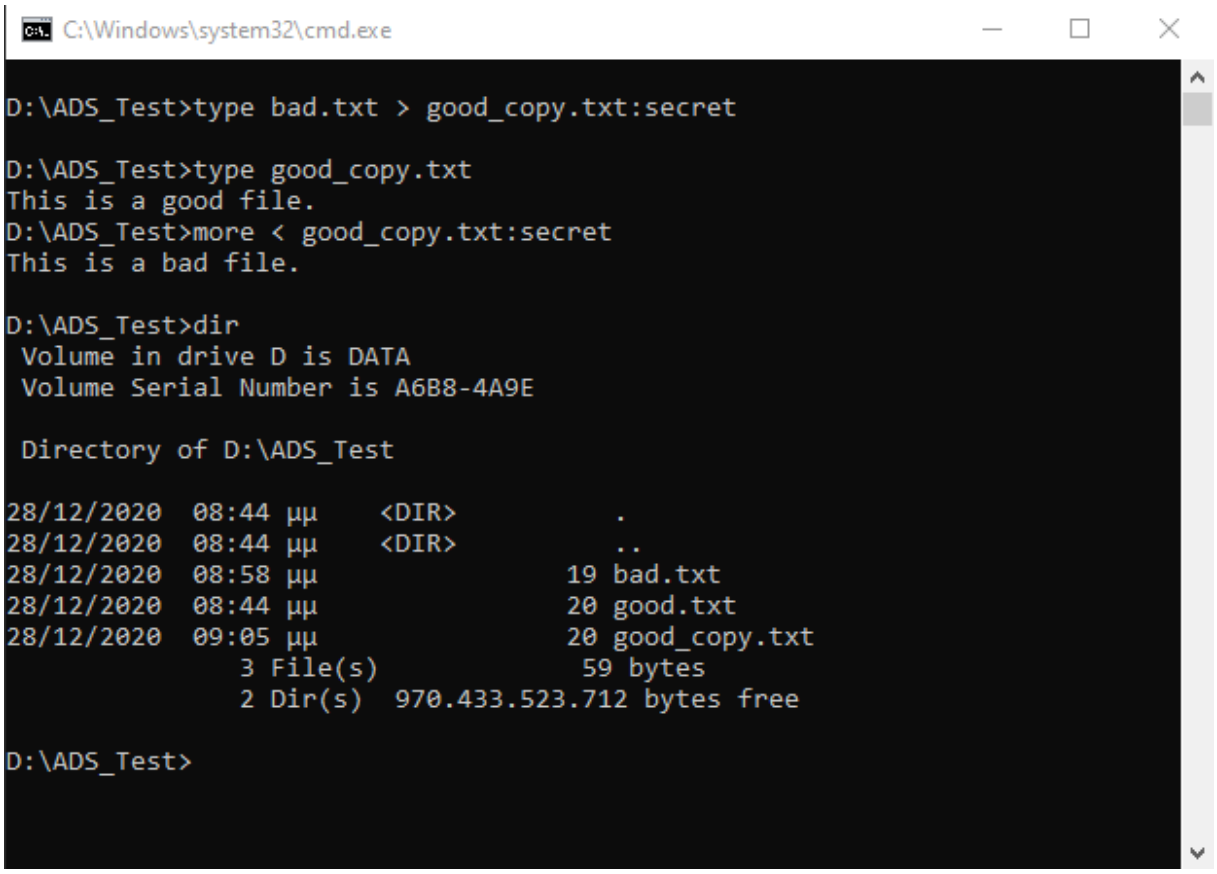
Όπως αναφέρθηκε στο δεύτερο κεφάλαιο, οι εναλλακτικές ροές δεδομένων (Alternate Data Streams) είναι μία λειτουργία που παρέχεται από το σύστημα αρχείων NTFS και επιτρέπει την ενσωμάτωση δεδομένων (αρχείων ή μεταδεδομένων) σε ένα αρχείο, χωρίς να επηρεάζει τη λειτουργικότητά του. Ένα ADS δημιουργείται από το τερματικό με τη χρήση εντολής της μορφής
'type *δεδομένα* > *αρχείο*:*όνομα_ADS'*, όπου τα δεδομένα μπορεί να είναι κείμενο ή αρχείο οποιασδήποτε μορφής. Για παράδειγμα, έχουμε ένα αρχείο κειμένου με όνομα 'good.txt', και ένα αρχείο με όνομα 'bad.txt' με περιεχόμενο όπως φαίνεται στο σχήμα 3.13. Για να λόγους σύγκρισης, δημιουργείται ένα αντίγραφο του αρχείου good.txt με όνομα 'good_copy.txt'. Η αλλαγή ονόματος δεν επηρεάζει την τιμή hash του αρχείου η οποία εξαρτάται από το περιεχόμενο του αρχείου, όπως φαίνεται και στο σχήμα 3.14.



Σχήμα 3.13 Περιεχόμενο αρχείων good.txt, bad.txt και good_copy.txt

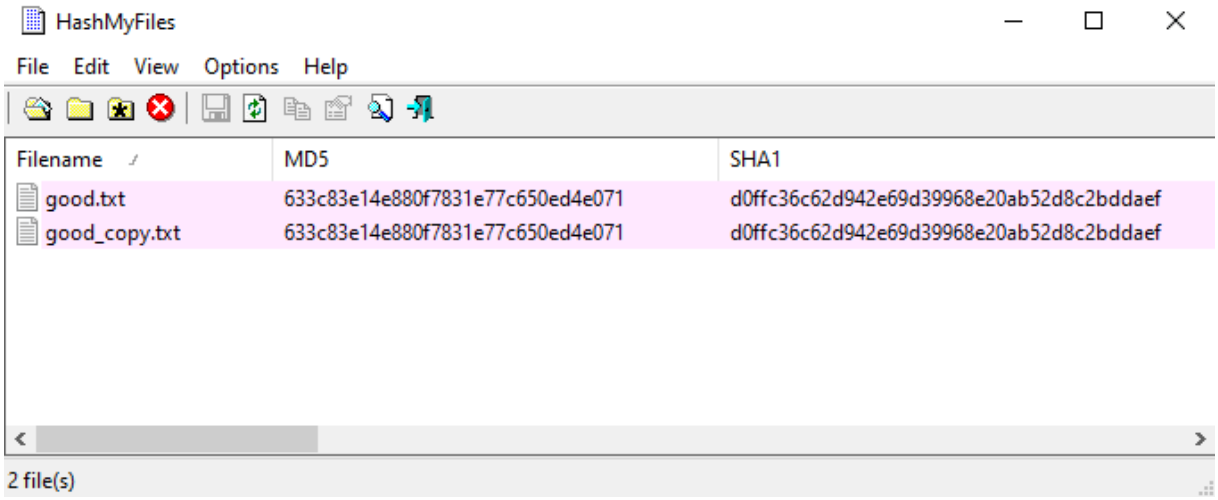


Σχήμα 3.14 Σύγκριση τιμών hash του αρχείου good.txt και του αντίγραφού του, good_copy.txt



Σχήμα 3.15 Δημιουργία ADS στο αρχείο good_copy.txt και εμφάνιση περιεχομένου του φακέλου στο οποίο βρίσκεται με τη χρήση τερματικού

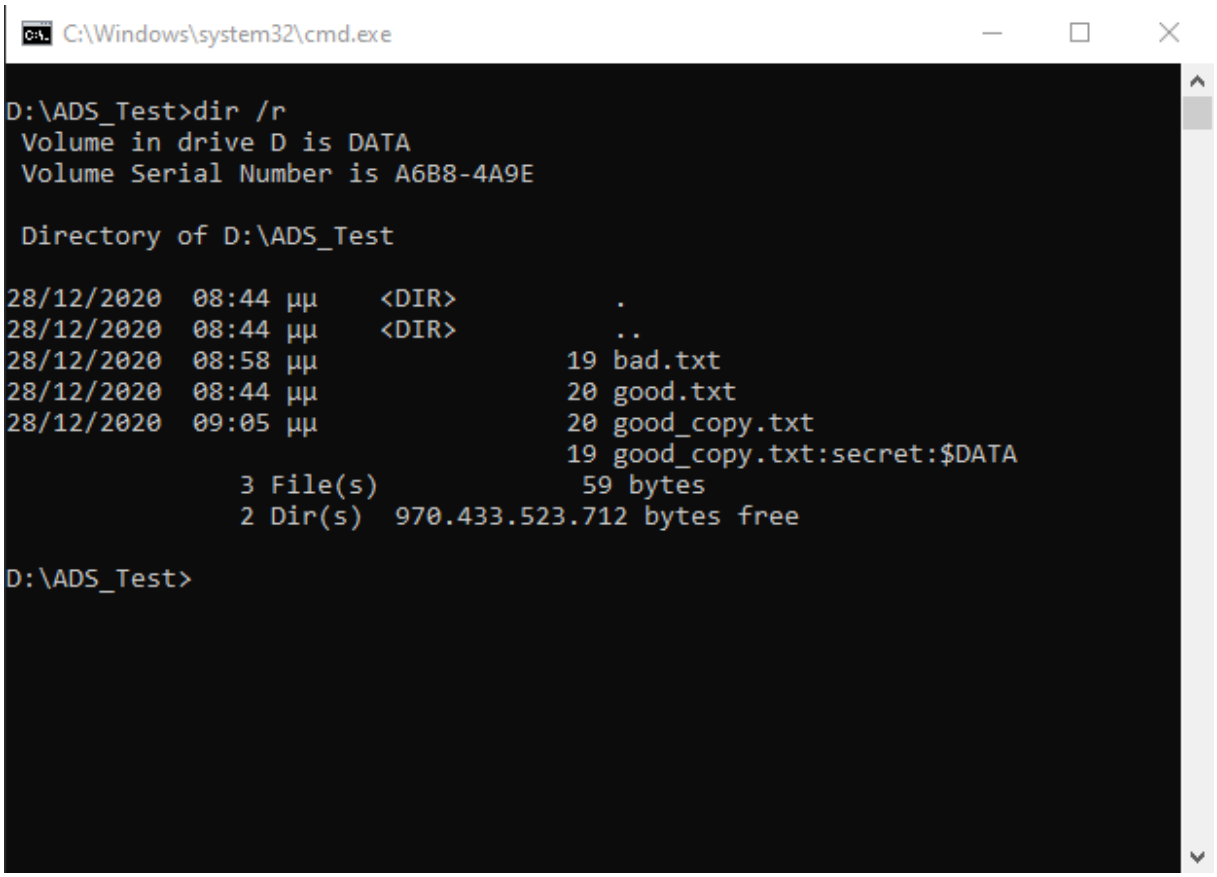
Στο σχήμα 3.15 μπορεί κανείς να παρατηρήσει τα εξής σημεία:
Μετά τη δημιουργία του ADS με όνομα 'secret' στο αρχείο good_copy.txt, το μέγεθος και το περιεχόμενο του αρχείου δεν μεταβλήθηκε, ενώ η πρόσβαση στο ADS του αρχείου γίνεται με την εντολή 'more < good_copy.txt:secret'. Επίσης, το ADS δεν είναι εμφανές με την εντολή dir. Αξίζει να αναφερθεί πως μετά τη δημιουργία του ADS, η επανεξέταση των τιμών hash του αρχείου δεν δείχνει καμία μεταβολή της αρχικής τιμής, όπως φαίνεται και στο σχήμα 3.16.



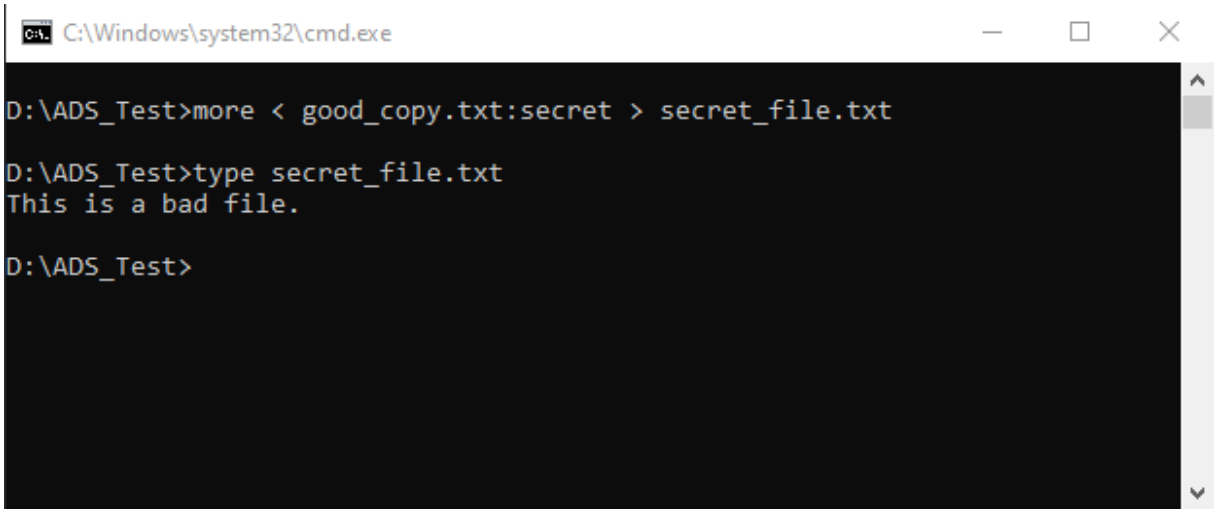
Σχήμα 3.16 Σύγκρησι τιμών hash αρχείου 'good.txt' και του αντιγράφου του, good_copy.txt, μετά τη δημιουργία ADS στο δεύτερο

Ο εντοπισμός των ADS μπορεί να γίνει από το τερματικό με χρήση της εντολής 'dir /r' (σχήμα 3.17). Ακόμα, μπορούν να χρησιμοποιηθούν εργαλεία όπως τα Streams, AlternateStreamView, Stream Detector, ADS Spy κ.α. Τα δύο τελευταία παρέχουν τη δυνατότητα φιλτραρίσματος των ADS που χρησιμοποιούνται από το λειτουργικό σύστημα και άλλα προγράμματα.

Η ανάκτηση των ADS γίνεται με την εντολή 'more < *αρχείο*:*όνομα_ADS* > *αρχείο_εξόδου*' όπως φαίνεται και στο σχήμα 3.18, όπου το ADS αποθηκεύεται στο αρχείο secret_file.txt.



Σχήμα 3.17 Προβολή των ADS στο τερματικό με την εντολή 'dir /r'



Σχήμα 3.18 Ανάκτηση του ADS με την εντολή 'more < good_copy.txt:secret > secret_file.txt'

3.4 Απόκρυψη Ιχνών

Στο παρόν υποκεφάλαιο παρουσιάζονται δύο λειτουργικά συστήματα τα οποία καλύπτουν πολλές από τις τεχνικές απόκρυψης ιχνών που έχουν αναφερθεί, το Tails και το Kodachi.

3.4.1 Tails

Το Tails είναι ένα φορητό live λειτουργικό σύστημα που έχει ως στόχο την παροχή ανωνυμίας στους χρήστες. Όσον αφορά την απόκρυψη ιχνών στο σύστημα, το Tails μπορεί να εγκατασταθεί σε ένα USB stick και να εκτελεστεί στη μνήμη RAM, χωρίς να αφήνει δεδομένα στον σκληρό δίσκο παρά μόνο (προαιρετικά) σε μία κρυπτογραφημένη περιοχή του USB stick. Επιπλέον, μετά τον τερματισμό του λειτουργικού συστήματος ή την εξαγωγή του USB stick τα δεδομένα από τη μνήμη RAM διαγράφονται ώστε να μην είναι δυνατή η εξαγωγή δεδομένων μετά από ανάλυση της μνήμης RAM ή τεχνικών cold boot attack [77]. Όσον αφορά την απόκρυψη ιχνών στο Διαδίκτυο, το Tails χρησιμοποιεί αποκλειστικά δρομολόγηση μέσω δικτύου onion και προγράμματα υπηρεσιών ανώνυμης ανταλλαγής μηνυμάτων και διαμοιρασμού αρχείων.

3.4.2 Linux Kodachi

Το Linux Kodachi αποτελεί άλλο ένα live λειτουργικό σύστημα με παρόμοια λειτουργία όπως αυτή του Tails. Μπορεί, δηλαδή, να εκτελεστεί από κάποιο εξωτερικό αποθηκευτικό μέσο χωρίς να αφήνει ίχνη στο σύστημα και η δρομολόγηση γίνεται μέσω onion routing. Ωστόσο, το Linux Kodachi παρέχει επιπλέον και υπηρεσίες VPN. Το Linux Kodachi σε αντίθεση με το Tails δεν παρέχει κρυπτογραφημένο χώρο μόνιμης αποθήκευσης, αλλά είναι κάτι που μπορεί να γίνει χειροκίνητα με χρήση εργαλείων κρυπτογράφησης.

Επίλογος

Στο 3ο κεφάλαιο έγινε πρακτική εφαρμογή ορισμένων τεχνικών και εργαλείων anti-forensics από κάθε κατηγορία που παρουσιάστηκε στο δεύτερο κεφάλαιο. Ακόμα, συζητήθηκαν τρόποι εντοπισμού ορισμένων τεχνικών και η αντιμετώπιση της χρήσης ADS για απόκρυψη αρχείων, καθώς, σε αντίθεση με τις υπόλοιπες τεχνικές μπορεί να αντιμετωπιστεί εύκολα. Για τις υπόλοιπες τεχνικές παρουσιάζονται γενικότεροι τρόποι προσέγγισης στο επόμενο κεφάλαιο.

Κεφάλαιο 4 Αντιμετώπιση τεχνικών anti-forensics

Εισαγωγή

Αφού, πλέον, έχουν αναλυθεί οι τεχνικές anti-forensics και έχει συζητηθεί ο τρόπος με τον οποίο επηρεάζουν την ψηφιακή εγκληματολογική έρευνα, μένει να διερευνηθούν τρόποι προσέγγισής τους τόσο με τεχνικά όσο και μη-τεχνικά μέσα. Στα τεχνικά μέσα συγκαταλέγονται λειτουργίες του συστήματος τις οποίες μπορεί να αξιοποιήσει ο ερευνητής, ώστε να εντοπίσει ίχνη εργαλείων anti-forensics, καθώς και ίχνη αρχείων ενδιαφέροντος τα οποία πιθανόν να έχουν καταστραφεί ή αποκρυφθεί. Επειδή, όμως, η πρόσβαση σε κάποιο σύστημα δεν είναι πάντοτε δυνατή ή δεν είναι δυνατή η τεχνική αντιμετώπιση των τεχνικών αυτών, δίνεται βάση και σε μη-τεχνικές προσεγγίσεις όπως η αξιοποίηση πληροφοριών OSINT και η διεύρυσνη της έρευνας πέρα από τα ψηφιακά μέσα.

4.1 Ο ρόλος της εκπαίδευσης

Μία βασική προσέγγιση για την αντιμετώπιση των τεχνικών anti-forensics είναι η τεχνική αντιμετώπισή τους, όπως παρουσιάστηκε σε ορισμένα παραδείγματα του προηγούμενου κεφαλαίου. Για την τεχνική αντιμετώπιση είναι αναγκαία η εξοικείωση του ερευνητή με τις υπάρχουσες τεχνικές anti-forensics, έτσι ώστε να είναι σε θέση αρχικά να τις εντοπίζει και στη συνέχεια να τις προσεγγίζει κατάλληλα, καθώς η άγνοια του ερευνητή μπορεί να οδηγήσει στη καταστροφή πειστηρίων ή στην παράλειψή τους αν δεν καταφέρει να τα εντοπίσει [107]. Η εξοικείωση με τις τεχνικές anti-forensics επιτυγχάνεται, σαφώς, μέσα από την εμπειρία, αλλά και τις γνώσεις του εκάστοτε ερευνητή οι οποίες αποκτώνται με τη συνεχή εκπαίδευση και ενημέρωση του για τις τρέχουσες εξελίξεις στο χώρο της κυβερνοασφάλειας.

Για την εκπαίδευση των ερευνητών σε προσωπικό επίπεδο υπάρχουν φορείς που παρέχουν πιστοποιήσεις στον τομέα της ψηφιακής εγκληματολογίας και ορισμένες από αυτές τις πιστοποιήσεις καλύπτουν στην ύλη τους και τεχνικές anti-forensics, ενώ παρέχονται και σεμινάρια που ειδικεύονται σε τεχνικές anti-forensics. Όμως, η εκπαίδευση των ερευνητών είναι κάτι το οποίο θα πρέπει να παρέχεται από τα ιδιωτικά ή δημόσια κέντρα ερευνών και να μην αφήνεται στην κρίση του εκάστοτε ερευνητή, από τη στιγμή που πιθανώς να υπάρχουν χρονικοί ή οικονομικοί περιορισμοί. Επιπλέον, δεν πρέπει να λησμονούμε πως οι άνθρωποι μπορεί να υπερεκτιμούν τις γνώσεις και τις ικανότητές τους. Οι Kruger και Dunning μέσα από πειραματικές μεθόδους έδειξαν ότι άτομα με λιγότερες δυνατότητες και γνώσεις σε έναν τομέα τείνουν να υπερεκτιμούν τις ικανότητές τους σχετικά με αυτόν τον τομέα [108], κάτι που αργότερα ονομάστηκε φαινόμενο Ντάνινγκ–Κρούγκερ **(**Dunning-Kruger effect).

4.2 Εκμετάλλευση λειτουργιών του συστήματος

Σε πολλές περιπτώσεις δεν είναι δυνατή η άμεση αντιμετώπιση ορισμένων τεχνικών anti-forensics και επομένως ο ερευνητής πρέπει να γνωρίζει εναλλακτικές μεθόδους προσέγγισης των τεχνικών αυτών. Για παράδειγμα, η χρήση ADS είναι μία τεχνική που ανιχνεύεται και αντιμετωπίζεται άμεσα με τη χρήση του τερματικού ή εργαλείων, ενώ η καταστροφή αρχείων ή η κρυπτογράφηση είναι τεχνικές

που πολλές φορές αντιμετωπίζονται δύσκολα και χρειάζονται μία έμμεση προσέγγιση. Επομένως, είναι σημαντικό ο ερευνητής να γνωρίζει λειτουργίες και περιοχές του συστήματος οι οποίες μπορούν να του παρέχουν σημαντικές πληροφορίες. Παρακάτω παρουσιάζονται ορισμένες λειτουργίες του λειτουργικού συστήματος Windows που μπορούν να αποβούν χρήσιμες για την αντιμετώπιση ορισμένων τεχνικών anti-forensics.

4.2.1 Μητρώο

Το Μητρώο είναι μία ιεραρχημένη βάση δεδομένων στην οποία βρίσκονται αποθηκευμένες ρυθμίσεις του λειτουργικού συστήματος Windows και άλλων προγραμμάτων του συστήματος [109]. Αποτελεί μία σπουδαία πηγή πληροφοριών για το σύστημα, αφού ο ερευνητής μπορεί μεταξύ άλλων να αντλήσει πληροφορίες, όπως εγκατεστημένες εφαρμογές αλλά και απομεινάρια αυτών ενώ έχουν απεγκατασταθεί ή διαγραφεί από το σύστημα, συσκευές που έχουν συνδεθεί στο σύστημα, δίκτυα στα οποία έχει συνδεθεί, καθώς και αρχεία και εφαρμογές στα οποία είχε πρόσφατα πρόσβαση ο χρήστης. Ο λόγος για τον οποίο γίνεται αναφορά στο μητρώο είναι αφενός μεν το γεγονός ότι αποτελεί σημαντική πηγή πειστηρίων σε κάθε έρευνα, αφετέρου δε ότι μπορεί να βοηθήσει και στην προσέγγιση ορισμένων τεχνικών anti-forensics, αφού περιέχει ίχνη από εκτελέσιμα προγράμματα τα οποία πιθανόν να αποδεικνύουν κάποια ενέργεια, όπως για παράδειγμα, χρήση εργαλείων κρυπτογράφησης ή στεγανογραφίας, αλλά και την ύπαρξη αρχείων τα οποία πιθανόν να μην βρίσκονται πλέον στο σύστημα.

Όσον αφορά τα δομικά χαρακτηριστικά του, το μητρώο έχει δομή δέντρου στο οποίο κάθε κόμβος ονομάζεται «κλειδί» (key) και κάθε κλειδί μπορεί να περιέχει υποκλειδιά ή/και τιμές (values). Οι τιμές αποτελούν τα δεδομένα που βρίσκονται αποθηκευμένα στη βάση και αξιοποιούνται από το σύστημα και άλλες εφαρμογές. Η δομή είναι παρόμοια με αυτή των καταλόγων (κλειδιά) και των αρχείων (τιμές). Το μητρώο αποτελείται από πέντε βασικά κλειδιά ρίζες (root keys - hives) [110] τα οποία παρουσιάζονται συνοπτικά στον πίνακα 4.1.

Πίνακας 4.1 Κλειδιά ρίζες του μητρώου

Κλειδί	Περιεχόμενο
HKEY_CLASSES_ROOT (HKCR)	Καθορίζει τύπους αρχείων και ιδιότητες που σχετίζονται με αυτούς.
HKEY_CURRENT_USER (KHCU)	Περιλαμβάνει τις προτιμήσεις του τρέχοντα συνδεδεμένου χρήστη.
HKEY_LOCAL_MACHINE (HKLM)	Περιλαμβάνει πληροφορίες σχετικά με το σύστημα, όπως δεδομένα για το υλικό (hardware) και το λειτουργικό σύστημα.
HKEY_USERS (HKU)	Ορίζει τις προκαθορισμένες ρυθμίσεις για χρήστες του συστήματος και τις ρυθμίσεις του τρέχοντα χρήστη.
HKEY_CURRENT_CONFIG (HKCC)	Περιλαμβάνει πληροφορίες σχετικά με τις τρέχουσες ρυθμίσεις του υλικού.

Η δομή των κλειδιών SAM, SECURITY, SOFTWARE και SYSTEM στο ριζικό κλειδί HKEY_LOCAL_MACHINE, καθώς και οι αλλαγές σε καθένα από αυτά, αποθηκεύονται σε αρχεία στον κατάλογο %SystemRoot%\System32\config με αντίστοιχα ονόματα. Τα κλειδιά που σχετίζονται με τον εκάστοτε συνδεδεμένο στο σύστημα χρήστη και βρίσκονται στο ριζικό κλειδί HKEY_CURRENT_USER, αποθηκεύονται αρχείο %USERPROFILE%\NTUSER.DAT και το αρχείο \%LocalAppData%\Microsoft\Windows\usrClass.dat.

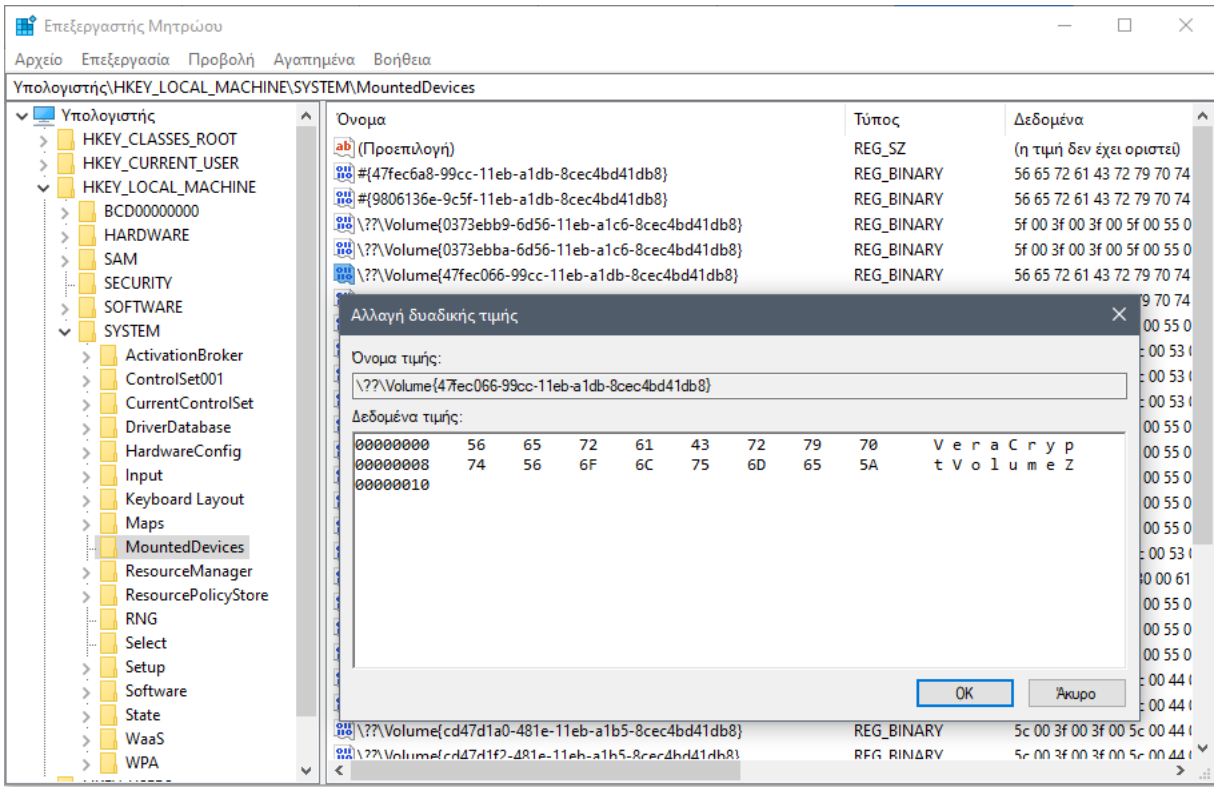
Η προβολή και επεξεργασία του περιεχομένου του μητρώου μπορεί να γίνει με το πρόγραμμα επεξεργασίας regedit.exe που υπάρχει προεγκατεστημένο στο λειτουργικό σύστημα Windows. Παρακάτω παρουσιάζονται ορισμένα κλειδιά ενδιαφέροντος για τον εντοπισμό τεχνικών anti-forensics. Είναι σημαντικό να αναφερθεί πως μεταξύ των διαφορετικών εκδόσεων των Windows ορισμένα κλειδιά μπορεί να μην υπάρχουν, να βρίσκονται σε διαφορετική θέση στο μητρώο ή να έχουν διαφορετική ονομασία, καθώς επίσης, και ότι ορισμένα κλειδιά του μητρώου δημιουργούνται αφού συνδεθεί ο χρήστης στο σύστημα.

4.2.1.1 Συσκευές

Κάθε φορά που συνδέεται μία συσκευή στον υπολογιστή, το λειτουργικό σύστημα Windows αποθηκεύει πληροφορίες σχετικά με τη συσκευή στο μητρώο. Στις πληροφορίες αυτές περιλαμβάνονται, μεταξύ άλλων, ο σειριακός αριθμός της συσκευής, ο τύπος της συσκευής, το όνομα, ο κατασκευαστής και το μοντέλο. Επίσης, περιλαμβάνονται χρονοσφραγίδες σχετικά με την πρώτη φορά που συνδέθηκε η συσκευή στο σύστημα και την τελευταία φορά που συνδέθηκε και αποσυνδέθηκε από το σύστημα. Αυτές οι πληροφορίες μπορούν να αξιοποιηθούν για την αναζήτηση και ανάλυση συσκευών που ενδεχομένως να περιέχουν αρχεία τα οποία αφορούν την υπό διερεύνηση υπόθεση.

Στο κλειδί HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum βρίσκεται το υποκλειδί USBSTOR στο οποίο αποθηκεύονται πληροφορίες σχετικά με συσκευές USB που έχουν συνδεθεί στο σύστημα. Το κλειδί USBSTOR περιλαμβάνει υποκλειδιά της μορφής 'Disk&Ven_<*προμηθευτής*>&Prod_<*προϊόν*>&Rev_<*αριθμός έκδοσης*>' από τα οποία αντλούμε πληροφορίες σχετικά με τον κατασκευαστή και το μοντέλο της συσκευής [111]. Επιπλέον, αποθηκεύεται ο σειριακός αριθμός της συσκευής (αν δεν έχει σειριακό αριθμό δημιουργείται ένας από το σύστημα).

Στο κλειδί HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices αποθηκεύονται πληροφορίες σχετικά με συσκευές που έχουν προσαρτιστεί στο σύστημα. Το κλειδί αυτό έχει ιδιαίτερη σημασία, καθώς, με το κλειδί αυτό μπορεί να εντοπιστεί η χρήση κρυπτογραφημένων τόμων. 'Οπως φαίνεται στο σχήμα 4.1 αποθηκεύονται και κρυπτογραφημένοι τόμοι που δημιουργήθηκαν με το εργαλείο VeraCrypt.

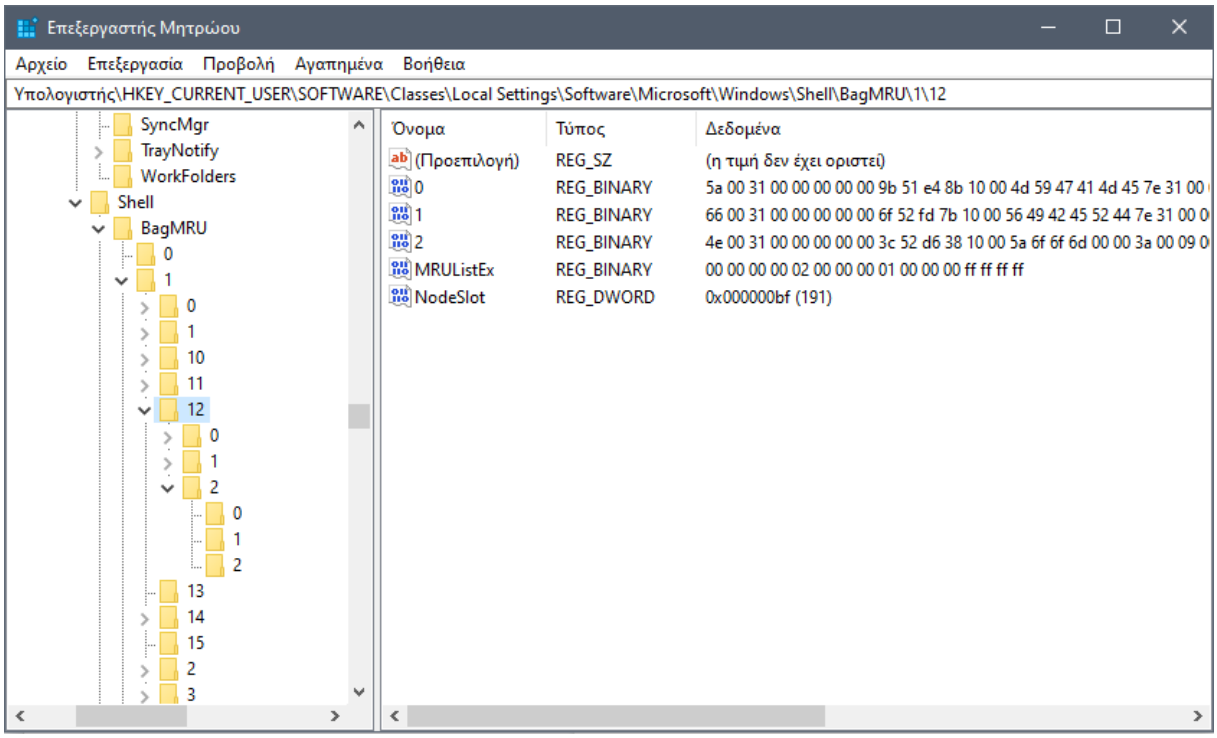


Σχήμα 4.1 Εντοπισμός κρυφού τόμου στο κλειδί MountedDevices

4.2.1.2 Shellbags

Τα shellbags είναι κλειδιά του μητρώου τα οποία περιέχουν ρυθμίσεις για καταλόγους που έχουν ανοιχτεί στο γραφικό περιβάλλον του λειτουργικού συστήματος Windows. Συγκεκριμένα, στα shellbags αποθηκεύονται οι επιλογές του χρήστη σχετικά με την προβολή των αρχείων σε έναν κατάλογο (όπως μέθοδος ταξινόμησης, μέγεθος εικονιδίων, τύπος προβολής), αλλά και χρονοσφραγίδες των χρόνων πρόσβασης και τροποποίησης των καταλόγων αυτών. Στα shellbags διατηρούνται εγγραφές και για καταλόγους που έχουν διαγραφεί από το σύστημα, καθώς και για καταλόγους που έχουν προσπελαστεί σε κάποιο εξωτερικό μέσο αποθήκευσης. Επομένως, ακόμα και αν έχει καταστραφεί κάποιος κατάλογος μπορεί ακόμα να αποδειχθεί ότι υπήρχε ο κατάλογος στο σύστημα και ο χρήστης είχε πρόσβαση σε αυτόν, αφού, όπως προαναφέρθηκε, οι πληροφορίες στα shellbags αποθηκεύονται μόνο εφόσον ο χρήστης έχει ανοίξει έναν κατάλογο με τη χρήση του γραφικού περιβάλλοντος. Οι πληροφορίες σχετικά με τα shellbags βρίσκονται στα κλειδιά BagMRU και Bags κάτω από το κλειδί HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell (στο λειτουργικό σύστημα Windows 10).

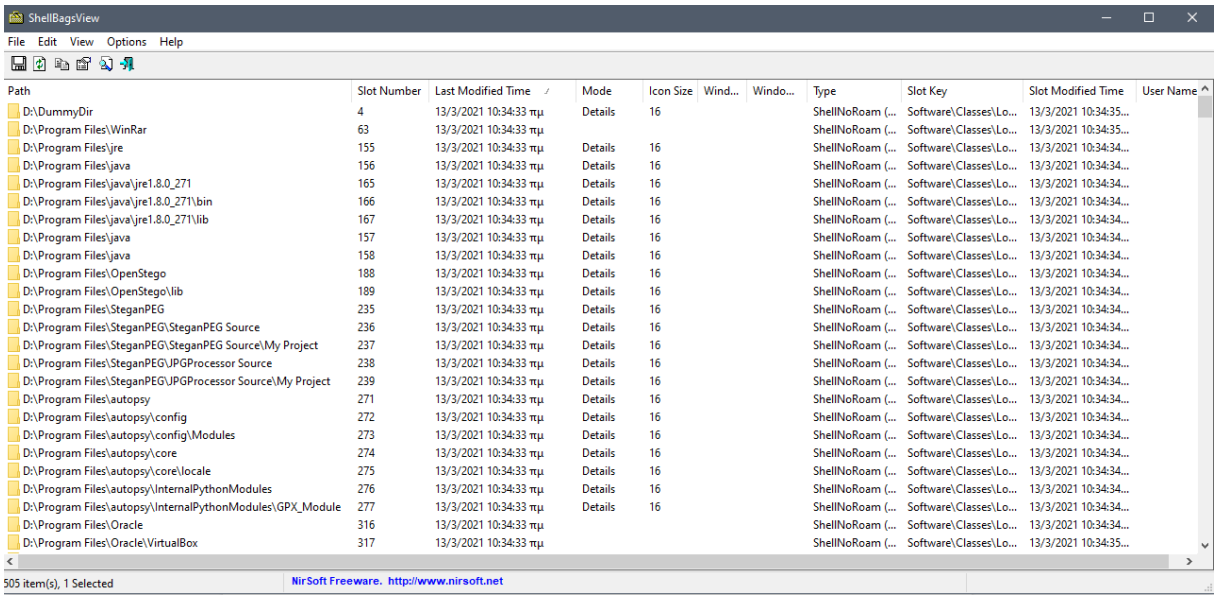
Το κλειδί BagMRU περιλαμβάνει αριθμημένα υποκλειδιά που αντιστοιχούν σε φακέλους. Αν οι φάκελοι έχουν υποφακέλους, τότε τα αντίστοιχα αριθμημένα κλειδιά περιλαμβάνουν με τη σειρά τους αριθμημένα υποκλειδιά για κάθε υποφάκελο. Η δομή αυτή φαίνεται στην στο σχήμα 4.2. Στο κλειδί Bags αποθηκεύονται ρυθμίσεις που σχετίζονται με την εμφάνιση του περιεχομένου των φακέλων, όπως το μέγεθος των εικονιδίων των αρχείων που περιλαμβάνει και το κριτήριο ταξινόμησης των αρχείων. Κάθε εγγραφή (υποκλειδί) του κλειδιού BagMRU αντιστοιχίζεται με μία από τις αριθμημένες εγγραφές του κλειδιού Bags με την τιμή NodeSlot (απεικονίζεται στο σχήμα 4.2) [112] .



Σχήμα 4.2 Δομή κλειδιού BagMRU

Υπάρχουν εργαλεία που αυτοματοποιούν την προβολή του περιεχομένου των shellbags, όπως τα ShellBag View, ShellBags Explorer και ShellBagger. Στην εικόνα παρουσιάζονται τα αποτελέσματα της χρήσης του εργαλείου ShellBagsView. Μετά από δοκιμή του προγράμματος ShellBagsView, φαίνεται πως στο εργαλείο αυτό οι ημερομηνίες τροποποίησης ξεκινούν από την ημερομηνία της τελευταίας ενημέρωσης του λειτουργικού συστήματος, κάτι που δεν συμβαίνει με το εργαλειο ShellBag View. Αυτό (όπως θα συζητηθεί παρακάτω) αναδεικνύει την ανάγκη δοκιμής των εργαλείων και κατανόηση του τρόπου λειτουργίας τους, αλλά και τη χρήση περισσότερων εργαλείων για τη διασταύρωση των αποτελεσμάτων. Τα κλειδιά και οι τιμές των shellbags βρίσκονται στο αρχείο %UserProfile%\NTUSER.DAT ενώ από την έκδοση Windows Vista και μετά βρίσκονται και στο αρχείο %UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat.

Όπως φαίνεται στο σχήμα 4.3, χρησιμοποιώντας το εργαλείο ShellBagsView εντοπίζουμε φακέλους εργαλείων στεγανογραφίας (OpenStego και SteganPEG), οι οποίοι έχουν προσπελαστεί αλλά δεν υπάρχουν πλέον στο σύστημα.



Σχήμα 4.3 Προβολή περιεχομένου shellbags με το εργαλείο ShellBagsView

4.2.1.3 MRU

Τα κλειδιά και οι τιμές που περιέχουν τα αρχικά 'MRU' (Most Recently Used) δηλώνουν τις πιο πρόσφατες ενέργειες. Παραπάνω έγινε αναφορά στην τιμή MRUListEx η οποία δηλώνει τη σειρά με την οποία προσπελάστηκαν οι υποκατάλογοι. Έτσι και τα προγράμματα της σουίτας γραφείου Microsoft Office, η οποία βρίσκεται προεγκατεστημένη σε πολλές εκδόσεις των Windows, αποθηκεύουν στο μητρώο τα πιο πρόσφατα ανοιγμένα αρχεία στο κλειδί 'File MRU' με την πλήρη διαδρομή προς το αρχείο αυτό. Με αυτόν τον τρόπο μπορεί να αποδειχθεί η πρόσβαση σε κάποιο αρχείο ενδιαφέροντος, καθώς και η τοποθεσία αυτού στο σύστημα ή σε κάποιο εξωτερικό μέσο αποθήκευσης. Στα Windows 10, το κλειδί File MRU για κάθε πρόγραμμα βρίσκεται στη θέση HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\xx.x.*ονομα_προγράμματος*, όπου xx.x ο αριθμός έκδοσης της σουίτας Microsoft Office. Για παράδειγμα, το κλειδί File MRU για το πρόγραμμα Word του Microsoft Office 2016 βρίσκεται στη θέση HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\File MRU.

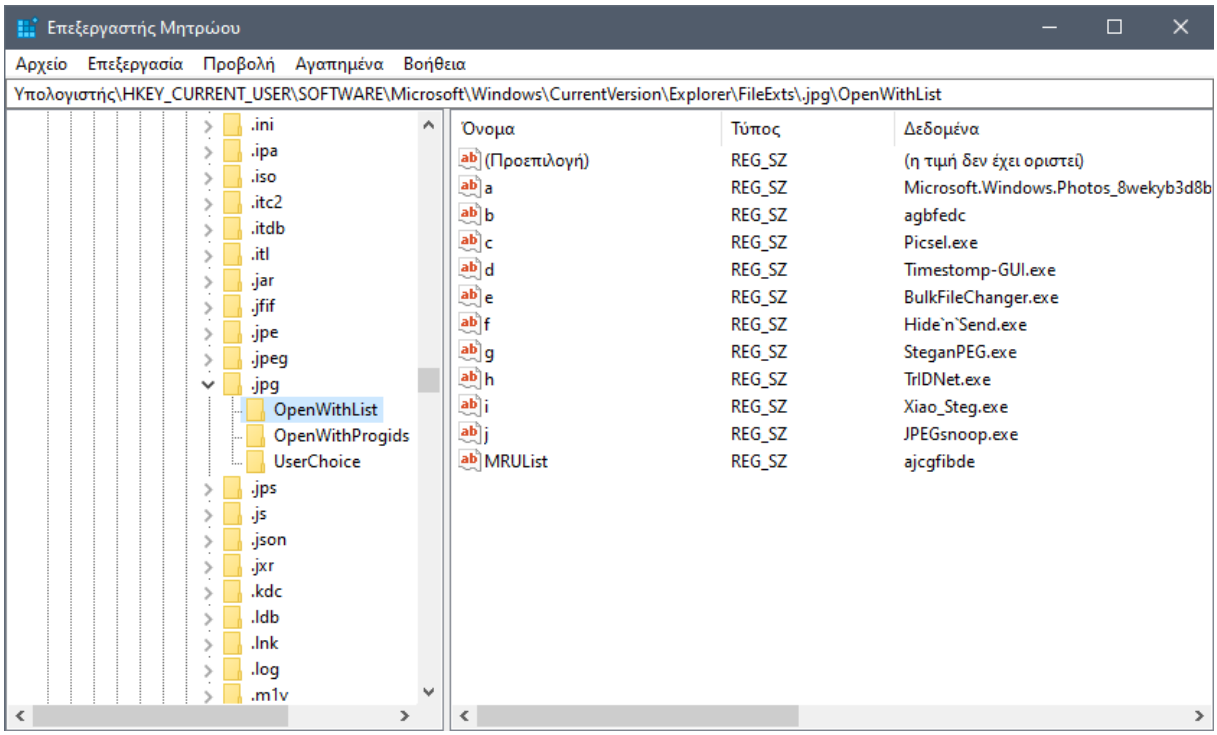
Ένα κλειδί ιδιαίτερου ενδιαφέροντος είναι το HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 στο οποίο αποθηκεύονται ρυθμίσεις σχετικά με τα παράθυρα διαλόγου που ανοίγουν τα προγράμματα για άνοιγμα ή αποθήκευση αρχείων:

- CIDSizeMRU: Περιλαμβάνει πληροφορίες σχετικά με το μέγεθος του παράθυρου διαλόγου που έχει ανοίξει κάθε πρόγραμμα.
- OpenSavePidlMRU: Περιλαμβάνει υποκλειδιά που αντιστοιχούν σε επεκτάσεις αρχείων και κάθε ένα από αυτά περιέχει αρχεία τα οποία έχουν ανοιχτεί ή αποθηκευτεί με χρήση παραθύρου διαλόγου [113].
- LastVisitedPidlMRU: Καταγράφει τα προγράμματα με τα οποία άνοιξαν τα αρχεία στο κλειδί OpenSavePidlMRU [113].
- LastVisitedPidlMRULegacy: Οι τιμές του είναι παρόμοιες με του LastVisitedPidlMRU.

Με τα παραπάνω κλειδιά δίνεται η δυνατότητα ανίχνευσης εργαλείων anti-forensics και τα αρχεία που άνοιξαν ή αποθήκευσαν, όπως, για παράδειγμα, εργαλεία στεγανογραφίας τα οποία χρησιμοποιούν παράθυρο διαλόγου για επιλογή φορέα, αλλά και για την αποθήκευση του στεγανογραφήματος.

4.2.1.4 OpenWithList

Ενδιαφέρον παρουσιάζει και το κλειδί HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xxx\OpenWithList, όπου το .xxx αντισοιχεί σε καταλήξεις αρχείων. Στο κλειδί αυτό περιέχονται τιμές οι οποίες δηλώνουν το πρόγραμμα με το οποίο πραγματοποιήθηκε πρόσβαση σε αρχεία με την κατάληξη που υποδηλώνεται στη θέση '.xxx'. Επίσης περιέχεται και η τιμή MRUList η οποία δηλώνει τη σειρά χρήσης των προγραμμάτων. Έτσι, στο σχήμα 4.4 φαίνονται εργαλεία που χρησιμοποιήθηκαν για εφαρμογή στεγανογραφίας σε αρχεία εικόνας με κατάληξη .jpg.



Σχήμα 4.4 Εντοπισμός εργαλείων στεγανογραφίας στο κλειδί OpenWithList για αρχεία JPG

4.2.1.5 Application Compatibility

Το ShimCache, ή αλλιώς AppCompatCache, είναι ένας μηχανισμός των Windows ο οποίος εξασφαλίζει τη συμβατότητα των εφαρμογών μεταξύ των εκδόσεων του λειτουργικού συστήματος Windows [114]. Η τιμή AppCompatCache βρίσκεται στο κλειδί HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session_Manager\AppCompatCache και περιλαμβάνει πληροφορίες σχετικά με προγράμματα που έχουν εκτελεστεί ή έχουν προβληθεί μέσω της εξερεύνησης αρχείων, όπως τη θέση του εκτελέσιμου αρχείου στο σύστημα, την πιο πρόσφατη χρονική στιγμή τροποποίησης και μια τιμή που δηλώνει αν το πρόγραμμα έχει εκτελεστεί ή όχι.

Αναζητώντας στο μητρώο ονόματα φορητών εφαρμογών που έχουν εκτελεστεί στο σύστημα από κάποιο εξωτερικό μέσο αποθήκευσης, βλέπουμε εγγραφές στο κλειδί HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows_NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store. Οι τιμές σε αυτό το κλειδί έχουν ως όνομα την πλήρη διαδρομή προγραμμάτων που έχουν εκτελεστεί στο σύστημα.

4.2.1.6 FeatureUsage

Το λειτουργικό σύστημα Windows 10 εισήγαγε τη λειτουργία FeatureUsage η οποία αποθηκεύει στο μητρώο πληροφορίες σχετικά με εφαρμογές όταν βρίσκονται στη γραμμή εργασιών (taskbar) [115]. Οι πληροφορίες αυτές βρίσκονται σε πέντε υποκλειδιά κάτω από το κλειδί HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage και παρουσιάζονται συνοπτικά στον πίνακα 4.2 [115-116]:

4.1 Υποκλειδιά στο κλειδί FeatureUsage

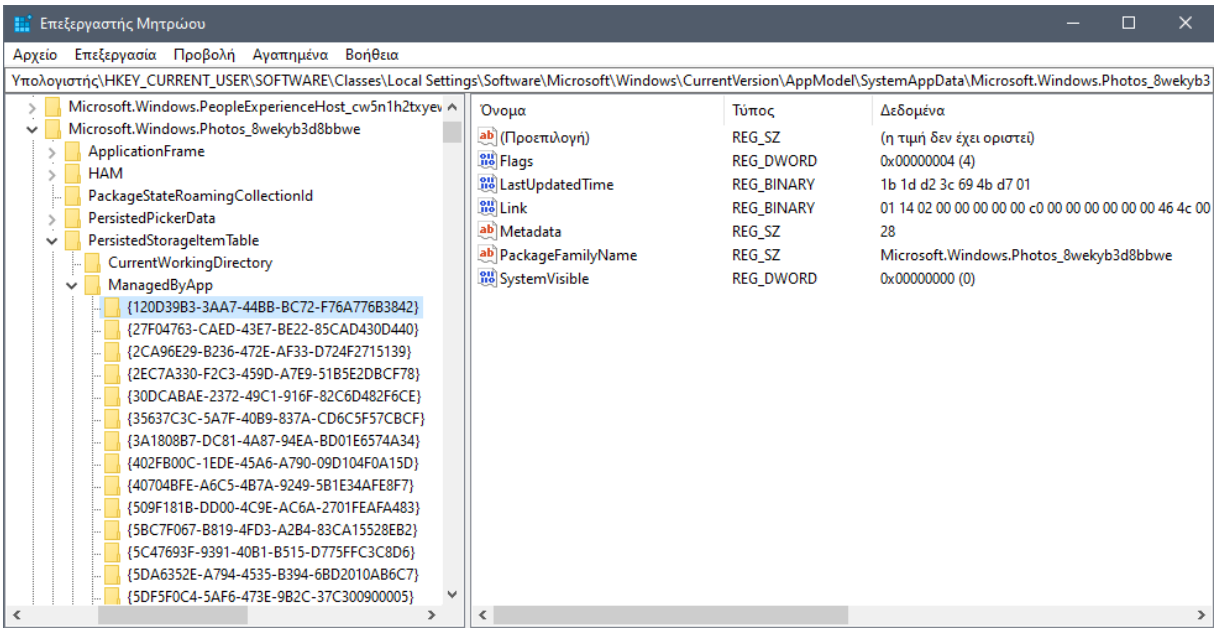
Κλειδί	Περιεχόμενο
AppBadgeUpdated	Πλήθος αλλαγών του εικονιδίου εφαρμογής στη γραμμή εργασιών.
AppLaunch	Πλήθος εκτελέσεων καρφιτσωμένης εφαρμογής στη γραμμή εργασιών.
AppSwitched	Πλήθος αριστερών κλικ σε εφαρμογές στη γραμμή εργασιών.
ShowJumpView	Πλήθος δεξιών κλικ σε εφαρμογές στη γραμμή εργασιών.
TrayButtonClicked	Πλήθος αριστερών κλικ σε λειτουργίες της γραμμής εργασιών (ρολόι, εργασίες, ειδοποιήσεις, αναζήτηση και Έναρξη).

Από τα παραπάνω κλειδιά το AppSwitched είναι αυτό που μπορεί να αξιοποιηθεί για τον εντοπισμό εργαλείων anti-forensics που έχουν εκτελεστεί στο σύστημα

4.2.1.7 Κλειδιά Εφαρμογών

Τα κλειδιά που δημιουργούν τα εγκατεστημένα προγράμματα στο σύστημα παρέχουν επίσης χρήσιμες πληροφορίες που μπορούμε να αντλήσουμε σχετικά με αρχεία. Για παράδειγμα, όπως αναφέρθηκε παραπάνω σχετικά με τα κλειδιά MRU, τα προγράμματα της σουίτας γραφείου Microsoft Office αποθηκεύουν πληροφορίες σχετικά με τα έγγραφα που έχουν ανοίξει χρησιμοποιώντας τα προγράμματα αυτά. Επίσης, το πρόγραμμα συμπίεσης αρχείων και φακέλων WinRAR, καταγράφει τα συμπιεσμένα αρχεία που έχουν προβληθεί με αυτό, στο κλειδί HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory.

Φαίνεται πως η χρήση του προεγκατεστημένου προγράμματος προβολής εικόνων των Windows 10 δημιουργεί εγγραφές στο μητρώο. Συγκρίνοντας δύο στιγμιότυπα του μητρώου, ένα πριν την προβολή μιας εικόνας με και ένα μετά την προβολή της εικόνας, μπορούμε να δούμε πως δημιουργούνται υποκλειδιά και τιμές στο κλειδί HKEY_CURRENT_USER\SOFTWARE\Classes\Local-Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Photos_8wekyb3d8bbwe\PersistedStorageItemTable\ManagedByApp. Συγκεκριμένα, κάτω από τον κόμβο ManagedByApp δημιουργούνται κλειδιά της μορφής '{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}' (όπου κάθε 'X' ένα δεκαεξαδικό ψηφίο) και αποτελούν μοναδικά αναγνωριστικά όπως απεικονίζεται στο σχήμα 4.5. Κάθε τέτοιο κλειδί δημιουργείται για κάθε αρχείο εικόνας και βίντεο που υπάρχει στον κατάλογο όπου βρισκόταν το αρχείο όταν άνοιξε με το πρόγραμμα προβολής εικόνων (και για το ίδιο το αρχείο), και φαίνεται πως υπάρχει ένα όριο μέχρι 30 εγγραφές. Σε κάθε κλειδί αποθηκεύονται ως τιμές, μεταξύ άλλων, η πλήρης διαδρομή της θέσης του αρχείου και ο χρόνος τροποποίησης της εγγραφής. Τα κλειδιά ανανεώνονται με το άνοιγμα ενός επόμενου αρχείου εικόνας και παραμένουν ακόμα και μετά από επόμενη εκκίνηση του συστήματος.



Σχήμα 4.5 Υποκλειδιά στο κλειδί ManagedByApp που αντιστοιχούν σε αρχεία

4.2.2 Αρχεία συστήματος

4.2.2.1 Thumbnails

Το λειτουργικό σύστημα Windows διατηρεί αρχεία προσωρινής μνήμης με μικρογραφίες εικόνων (thumbnail cache), έτσι ώστε να επιταχύνεται η διαδικασία φόρτωσης των καταλόγων στο γραφικό περιβάλλον. Στην έκδοση Windows XP τα αρχεία αυτά βρίσκονται στον ίδιο κατάλογο με τις εικόνες και ονομάζονταν thumbs.db, ενώ από την έκδοση Vista και μετά τα αρχεία προσωρινής μνήμης μικρογραφιών διατηρούνται σε μία κεντρική τοποθεσία, στον κατάλογο %userprofile%\AppData\Local\Microsoft\Windows\Explorer, όπου κάθε αρχείο έχει όνομα του τύπου thumbcache_xxx.db, με 'xxx' έναν αριθμό που συμβολίζει το μέγιστο μέγεθος των διαστάσεων των μικρογραφιών [117]. Στην ίδια τοποθεσία βρίσκονται και τα αρχεία iconcache_xxx.db στα οποία αποθηκεύονται μικρογραφίες των εικονιδίων προγραμμάτων. Η αξία αυτών των αρχείων έγκειται στο ότι διατηρούν μικρογραφίες από εικόνες και προγράμματα τα οποία δεν υπάρχουν πλέον στο σύστημα. Ένα εργαλείο με το οποίο μπορούν να προβληθεί το περιεχόμενο των αρχείων thumbcache_xxx.db και iconcache_xxx.db είναι το Thumbcache Viewer.

4.2.2.2 Prefetch

Σκοπός του prefetching είναι η επιτάχυνση της διαδικασίας εκτέλεσης προγραμμάτων φορτώνοντας τα πιο συχνά χρησιμοποιούμενα προγράμματα στη μνήμη RAM [118]. Σε κάθε αρχείο prefetch, που δημιουργείται για κάθε πρόγραμμα που έχει εκτελεστεί, αποθηκεύονται πληροφορίες όπως το πλήθος εκτελέσεων του προγράμματος, η ώρα και ημερομηνία της τελευταίας εκτέλεσης, η πλήρης διαδρομή προς το εκτελέσιμο αρχείο, ενώ, για κάθε εκτελέσιμο αποθηκεύονται και άλλα αρχεία που χρησιμοποιήθηκαν από το πρόγραμμα. Για την προβολή των αρχείων prefetch μπορεί να χρησιμοποιηθεί το εργαλείο γραφικού περιβάλλοντος WinPrefetchView ή το εργαλείο γραμμής εντολών PECmd.

4.2.2.3 Jump List

Τα Jump Lists (λίστες συντομεύσεων) είναι λίστες που διατηρούν τα προγράμματα και περιέχουν τα πιο πρόσφατα αντικείμενα στα οποία είχε πρόσβαση ο χρήστης μέσω αυτών των προγραμμάτων [119]. Ακόμα και αν ο χρήστης απενεργοποιήσει αυτή τη λειτουργία το σύστημα καταγράφει φακέλους τους οποίους προσπέλασε ο χρήστης. Σε περίπτωση που διαγραφεί ο φάκελος από το σύστημα διαγράφεται και η σχετική εγγραφή, όμως διατηρούνται οι εγγραφές φακέλων που βρίσκονταν σε κάποιο εξωτερικό αποθηκευτικό μέσο όταν προσπελάστηκαν. Η λειτουργία αυτή είναι διαθέσιμη από την έκδοση Windows 7 και μετά, και τα αρχεία jump lists βρίσκονται στον κατάλογο %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\.

4.2.2.4 Hibernation file

Για να επιτευχθεί η επαναφορά του συστήματος στην κατάσταση που βρισκόταν πριν την αδρανοποίησή του, η τρέχουσα κατάστασή του επεξεργαστή και το περιεχόμενο της μνήμης RAM αποθηκεύονται στο σκληρό δίσκο, σε ένα αρχείο με όνομα pagefile.sys [120]. Το αρχείο pegafile.sys διατηρείται στον σκληρό δίσκο μέχρι την επόμενη αδρανοποίηση του συστήματος. Απο τη στιγμή που

περιέχει τα δεδομένα της μνήμης RAM αποτελεί μία χρήσιμη πηγή πειστηρίων, καθώς παρέχει εφήμερα δεδομένα στα οποία διαφορετικά θα ήταν αδύνατο να έχει πρόσβαση ο ερευνητής. Στο σύστημα, το αρχείο αυτό αποθηκεύεται στον ριζικό κατάλογο όπου είναι εγκατεστημένο το λειτουργικό σύστημα (C:/).

.

4.3 Live forensics

Στο πρώτο κεφάλαιο έγινε μία σύντομη αναφορά για τους τύπους συλλογής δεδομένων από ένα υπολογιστικό σύστημα. Η συλλογή δεδομένων αποτελεί ένα από τα βασικά στάδια της ερευνητικής διαδικασίας και πραγματοποιείται όταν το σύστημα είναι απενεργοποιημένο ή/και όσο είναι σε λειτουργία. Σε ένα σύστημα το οποίο βρίσκεται σε λειτουργία είναι δυνατή η συλλογή πτητικών δεδομένων από τη μνήμη RAM, όπως κωδικοί και κλειδιά κρυπτογράφησης, διαδικτυακές συνδέσεις, μηνύματα από συνομιλίες, κ.λπ [121], καθώς και τα πτητικά δεδομένα από το μητρώο στο λειτουργικό σύστημα Windows. Επιπλέον, αν το σύστημα είναι συνδεδεμένο στο cloud όπου ο χρήστης αποθηκεύει δεδομένα, ο ερευνητής μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα στα οποία υπό άλλες συνθήκες, χωρίς τη συνεργασία του χρήστη θα είχε δύσκολα πρόσβαση και πιθανόν να ερχόταν αντιμέτωπος με τα εμπόδια που αναφέρθηκαν στο πρώτο κεφάλαιο, δηλαδή τεχνικά και νομικά ζητήματα που σχετίζονται με την πρόσβαση σε δεδομένα του νέφους.

Ένας ακόμα πολύ βασικός λόγος ανάλυσης ενός συστήματος σε λειτουργία είναι η παράκαμψη της κρυπτογραφίας. Στη μνήμη RAM βρίσκονται κλειδιά κρυπτογράφησης τα οποία μπορούν να ανακτηθούν και να χρησιμοποιηθούν για την αποκρυπτογράφηση δεδομένων [122]. Επιπλέον, όταν ο χρήστης ανοίγει ένα κρυπτογραφημένο αρχείο, η αποκρυπτογραφημένη του μορφή αποθηκεύεται στη μνήμη RAM, επομένως είναι δυνατή η ανάκτηση του αρχείου ή τμημάτων αυτού (σε περίπτωση όπου μέρος του έχει επεγγραφεί από άλλα δεδομένα). Τέλος, τα δεδομένα ενός σκληρού δίσκου που παρέχει κρυπτογράφηση σε επίπεδο hardware (self-encrypting drive - SED) είναι αποκρυπτογραφημένα όσο το σύστημα βρίσκεται σε λειτουργία, κάτι που συμβαίνει και στην περίπτωση κρυπτογράφησης ολόκληρου του δίσκου με χρήση λογισμικού. Στην περίπτωση του δημιουργού της σελίδας Silk Road, λίγο πριν τη σύλληψή του, οι πράκτορες κατάφεραν αποσπώντας του την προσοχή να πάρουν τον φορητό του υπολογιστή όσο βρισκόταν σε λειτουργία, παρακάμπτοντας με αυτόν τον τρόπο την κρυπτογράφηση του δίσκου και αποκτώντας πρόσβαση σε μία πληθώρα αποδεικτικών στοιχείων σχετικά με τις δράσεις του [123].

4.4 Εργαλεία

Η βελτίωση των εργαλείων μπορεί επίσης να συμβάλλει στην τεχνική αντιμετώπιση ορισμένων τεχνικών anti-forensics. Για παράδειγμα, οι επιθέσεις σε εργαλεία ανάλυσης πειστηρίων μπορούν να αποφευχθούν με τη καλύτερη διαχείριση συμπιεσμένων αρχείων, για την αντιμετώπιση αρχείων zip-bombs [124], καθώς και με τη χρήση αποδοτικότερων μεθόδων για την αναγνώριση του τύπου των αρχείων. Οι Amirani, Toorani και Beheshti πρότειναν μία μέθοδο με χρήση μηχανικής μάθησης για την αναγνώριση του τύπου ενός αρχείου, η οποία είναι ανεξάρτητη από την υπογραφή και την επέκταση του αρχείου και βασίζεται μόνο στο περιεχόμενο του [125].

Παραμένοντας στα εργαλεία είναι σημαντικό να αναφερθεί η ανάγκη χρήσης μία ποικιλίας προγραμμάτων. Παρά το γεγονός ότι σουίτες εργαλείων για εγκληματολογική ανάλυση, όπως οι Autopsy, EnCase και FTK, παρέχουν πολλές δυνατότητες για την ανίχνευση ορισμένων τεχνικών anti-forensics (όπως η ασυμφωνία κατάληξης και υπογραφής ενός αρχείου ή η κρυπτογραφία) δεν καλύπτουν όλες τις πιθανές τεχνικές. Για αυτό το λόγο, ο ερευνητής πρέπει να γνωρίζει τα διαθέσιμα εργαλεία που υπάρχουν και ειδικεύονται στον εντοπισμό ή την αντιμετώπιση ορισμένων τεχνικών anti-forensics, όπως η ανίχνευση ADS, η ανίχνευση στεγανογραφίας, η ανίχνευση rootkits κ.α. Η ανάγκη χρήσης μιας πληθώρας εργαλείων αφορά και τα εργαλεία που παρέχουν την ίδια λειτουργία, από τη στιγμή που διαφορετικά εργαλεία πιθανόν να παράγουν διαφορετικά αποτελέσματα για την ίδια ενέργεια, κάτι που οφείλεται στη διαφορετική υλοποίηση και λειτουργία των εργαλείων. Για παράδειγμα, όπως αναφέρθηκε παραπάνω, κατά τη δοκιμή δύο προγραμμάτων προβολής των shellbags παρατηρήθηκαν διαφορές στον χρόνο τροποποίησης των εγγραφών, καθώς στο ένα από αυτά οι χρόνοι ορισμένων εγγραφών ήταν αρχικοποιημένοι στη χρονική στιγμή όπου έγινε η τελευταία ενημέρωση του συστήματος.

4.5 Μη-τεχνική προσέγγιση

Σύμφωνα με τον Brian Carrier η ερευνητική διαδικασία θα πρέπει να στραφεί σε φυσικές μεθόδους όπως συνεντεύξεις και ανακρίσεις, προσέγγιση κοντινών προσώπων ενός υπόπτου, παρακολούθηση της τηλεφωνικής επικοινωνίας και η εγκατάσταση keylogger στον υπολογιστή του υπόπτου [126]. Η άντληση πληροφοριών μέσα από ανακρίσεις και από την προσέγγιση κοντινών προσώπων ενός υπόπτου έχουν συμβάλει στην εξιχνίαση υποθέσεων, όπως στην περίπτωση όπου οι αρχές κατάφεραν να πείσουν τον γιο ενός υπόπτου για εμπρησμό να αναβαθμίσει μία εφαρμογή εντοπισμού που υπήρχε εγκατεστημένη στο κινητό του, μέσω της οποίας θα ήταν σε θέση να εντοπίσουν την τοποθεσία του υπόπτου την στιγμή του εμπρησμού [127]. Ωστόσο, η παρακολούθηση των συνομιλιών και η εγκατάσταση keylogger στον υπολογιστή του υπόπτου πιθανόν να παραβιάζουν νόμους που αφορούν την ιδιωτικότητα του ατόμου και να δημιουργούν ηθικά και νομικά ζητήματα. Επομένως, τέτοιες ενέργειες είναι εφικτές σε εταιρικά περιβάλλοντα ή οργανισμούς όπου δηλώνονται ρητά σε πολιτικές στις οποίες οι εργαζόμενοι καλούνται να συναινέσουν.

4.5.1 OSINT

OSINT (Open-source intelligence) είναι πληροφορίες που υπάρχουν ελεύθερα διαθέσιμες από δημόσιες πηγές όπως το Διαδίκτυο, τις δημόσιες βιβλιοθήκες και τις εφημερίδες. Οι πληροφορίες αυτές αξιοποιούνται από τους ερευνητές και μπορούν να χρησιμοποιηθούν και για την προσέγγιση υποθέσεων στις οποίες οι τεχνικές anti-forensics αποτελούν εμπόδιο, όπως στην προαναφερθείσα υπόθεση του δημιουργού της ιστοσελίδας Silk Road. Καθώς η ιστοσελίδα βρισκόταν στο ανώνυμο δίκτυο Tor, οι χρήστες χρησιμοποιούσαν ψευδώνυμα και οι συναλλαγές πραγματοποιούνταν με bitcoins, ο εντοπισμός του ιδιοκτήτη της σελίδας ήταν δύσκολη. Ωστόσο, ο εντοπισμός του δημιουργού βασίστηκε σε πληροφορίες OSINT οι οποίες ήταν διαθέσιμες με αναζητήσεις στο Διαδίκτυο [128].

Σε έρευνά τους, οι Kanta, Coisel και Scanlon μελέτησαν την προοπτική αξιοποίησης πληροφορίων OSINT για το σπάσιμο κωδικών πρόσβασης και κρυπτογράφησης [129]. Η μελέτη των συνηθειών

των χρηστών σχετικά με τους κωδικούς πρόσβασης δείχνει πως ένα μεγάλο μέρος των χρηστών επιλέγει κωδικούς πρόσβασης που περιέχουν προσωπικά δεδομένα ή ενδιαφέροντα του χρήστη, ώστε να είναι δυνατή η εύκολη ανάκλησή τους. Από έρευνα που πραγματοποίησε η Google το 2019 προέκυψε πως το 59% των συμμετεχόντων χρησιμοποιούσε ημερομηνίες, ονόματα συγγενών, κατοικιδίων ή το δικό τους όνομα [130]. Ενώ θα περίμενε κανείς πως η χρήση τόσο απλών κωδικών συναντάται μόνο σε κοινούς χρήστες ήταν και ο λόγος που οδήγησε στη σύλληψη του χάκερ Jeremy Hammond, αφού ο κωδικός πρόσβασής του ήταν το όνομα της γάτας του με πρόθεμα '123' [131]. Επομένως, η πληροφορίες OSINT μπορούν να αποτελέσουν ένα χρήσιμο εργαλείο για την εύρεση κωδικών πρόσβασης με τη δημιουργία αποτελεσματικότερων επιθέσεων λεξικού για κάθε στόχο [129].

4.5.2 Ανθρώπινος παράγοντας

Οι πληροφορίες OSINT και η υπόθεση του Jeremy Hammond μας οδηγούν στο θέμα του ανθρώπινου παράγοντα και, συγκεκριμένα, στα σφάλματα και τις παραλείψεις ως αποτέλεσμα των περιορισμένων γνώσεων ενός ατόμου, της αδυναμίας υπολογισμού όλων των πιθανών παραγόντων, αλλά και του ανθρώπινου χαρακτήρα.

4.5.2.1 Επίπεδο γνώσεων

Ίσως κανείς να αναμένει πως τα ηλεκτρονικά εγκλήματα, όπως η παράνομη πρόσβαση ή η επίθεση σε ένα σύστημα, πραγματοποιούνται αποκλειστικά από άτομα με άριστες τεχνολογικές γνώσεις, με αποτέλεσμα ο εντοπισμός τους να αποτελεί πρόκληση. Ωστόσο, αυτό δεν είναι κάτι που ισχύει πάντα. Ο όρος «script kiddies» αναφέρεται σε άτομα που χρησιμοποιούν έτοιμα εργαλεία για να πραγματοποιήσουν επιθέσεις σε συστήματα χωρίς, όμως, να έχουν ιδιαίτερες γνώσεις σχετικά με τον τρόπο λειτουργίας τους και χωρίς επίγνωση των επιπτώσεων των πράξεών τους και των ιχνών που αφήνουν πίσω τους. Επιπλέον, η υποκλοπή δεδομένων, όταν αυτή γίνεται εσωτερικά ενός οργανισμού ή εταιρείας, ή η κατοχή παιδικής πορνογραφίας μπορούν να πραγματοποιηθούν από άτομα με οποιοδήποτε επαγγελματικό υπόβαθρο.

4.5.2.2 Αστάθμητοι παράγοντες

Αλλά, ακόμα και στις περιπτώσεις που τα ηλεκτρονικά εγκλήματα πραγματοποιούνται από άτομα με άριστες γνώσεις πληροφορικής, θα πρέπει να λαμβάνεται υπόψιν η περίπτωση ανθρώπινου λάθους και παραλήψεων που οφείλονται στην αδυναμία υπολογισμού όλων των παραμέτρων. Για παράδειγμα, όπως προαναφέρθηκε, ο εντοπισμός του δημιουργού της ιστοσελίδας Silk Road, έγινε από μία ανάρτησή του χρησιμοποιώντας το ψευδώνυμο altoid, και δίνοντας την προσωπική του διεύθυνση email για να ζητήσει συμβουλές σχετικά με την ιστοσελίδα του. Παρόλο που η αρχική ανάρτησή του είχε διαγραφεί, παρέμεινε ως αναφορά σε μία σχετική απάντηση [128].

Άλλο ένα παράδειγμα αποτελούν οι λειτουργίες του συστήματος. Όπως είδαμε, υπάρχουν πολλές λειτουργίες τις οποίες μπορεί να εκμεταλλευτεί ο ερευνητής για τον εντοπισμό ή την παράκαμψη τεχνικών anti-forensics. Στο μητρώο μπορεί κανείς να βρει ίχνη αρχείων και προγραμμάτων που έχουν εκτελεστεί στο σύστημα, διασκορπισμένα σε διάφορα κλειδιά. Επιπλέον, δεν υπάρχει κάποιο

επίσημο διαθέσιμο εγχειρίδιο για τα κλειδιά του μητρώου και τις πληροφορίες που καταγράφονται σε κάθε ένα από αυτά, ενώ σε κάθε επόμενη έκδοση των Windows προστίθενται νέες λειτουργίες (και, άρα, νέα κλειδιά) με αποτέλεσμα να είναι δύσκολο να προβλέψει ο χρήστης όλες τις επιπτώσεις που επιφέρουν οι ενέργειές του στο σύστημα.

4.5.2.3 Ανθρώπινη φύση

Οι άνθρωποι έχουν ορισμένες αδυναμίες και κάποια χαρακτηριστικά τα οποία τους οδηγούν στο να κάνουν σφάλματα. Όπως ήδη αναφέρθηκε, οι χρήστες τείνουν να χρησιμοποιούν ως κωδικούς ονόματα και ημερομηνίες και άλλες πληροφορίες που τους αφορούν προσωπικά. Αυτό συμβαίνει γιατί για να αποθηκευτεί μία πληροφορία στην ανθρώπινη μνήμη θα πρέπει να κωδικοποιηθεί και να της αποδοθεί κάποιο νόημα [132]. Μία μεγάλου μήκους, τυχαία συμβολοσειρά (δύο στοιχεία που χαρακτηρίζουν έναν ισχυρό κωδικό) δεν έχει κάποιο νόημα η ίδια και ο μόνος τρόπος για να αποθηκευτεί και να παραμείνει στη μακρόχρονη μνήμη είναι η επανάληψη. Όταν, όμως, οι χρήστες διαθέτουν κατά μέσο όρο 38 διαδικτυακούς λογαριασμούς [133] η εκμάθηση τέτοιου είδους κωδικών είναι μία κοπιαστική διαδικασία που πολλοί δεν διατίθενται να ακολουθήσουν. Για αυτό το λόγο, ένα μεγάλο ποσοστό των χρηστών χρησιμοποιεί εύκολους κωδικούς, επαναχρησιμοποιεί τους κωδικούς του [130] ή κάνει ελάχιστες τροποποιήσεις [134]. Επίσης, ένα σημαντικό ποσοστό των χρηστών καταγράφει τους κωδικούς πρόσβασής του είτε φυσικά είτε σε κάποιο ηλεκτρονικό αρχείο [135]. Επομένως, το στάδιο της συλλογής πειστηρίων δεν πρέπει να περιορίζεται μόνο σε ψηφιακά μέσα αποθήκευσης, αλλά και στο χώρο όπου γίνεται η κατάσχεση του αποθηκευτικού μέσου για αναζήτηση στοιχείων (χαρτάκια σημειώσεων, σημειωματάρια, ακόμα και επιφάνειες) για καταγεγραμμένους κωδικούς.

Το 1943 ο Maslow παρουσίασε σε επιστημονική του εργασία μία ιεράρχηση των αναγκών του ανθρώπου με τη μορφή μιας πυραμίδας [136]. Ανάμεσα σε αυτές τις ανάγκες συμπεριλαμβάνεται η ανάγκη της εκτίμησης είτε σε προσωπικό επίπεδο, μέσω επιτευγμάτων και ανάπτυξης ικανοτήτων, είτε ως ένα αίσθημα που εισπράττει από τρίτους μέσω του σεβασμού και της υπόληψης. Ίσως η ανάγκη αυτή εξηγεί την τάση των εγκληματιών να μοιράζονται τα κατορθώματά τους τους με άλλους, ακόμα και να τα αναρτούν στα μέσα κοινωνικής δικτύωσης, κάτι που πολλές φορές οδηγεί στη σύλληψή τους [137-138]. Οπότε, βλέπουμε για μία ακόμα φορά την ανάγκη της επέκτασης της έρευνας πέρα από το υπό ανάλυση ψηφιακό μέσο, καθώς επίσης και τη σημασία της εκμετάλλευσης των πληροφοριών που υπάρχουν ελεύθερα στο Διαδίκτυο.

Επίλογος

Σε αυτό το κεφάλαιο μελετήθηκαν τρόποι προσέγγισης των τεχνικών anti-forensics, τόσο για τον εντοπισμό όσο και για την αντιμετώπισή τους. Συγκεκριμένα, μελετήθηκαν λειτουργίες του λειτουργικού συστήματος Windows που μπορούν να εκμεταλλευτούν οι ερευνητές για τον εντοπισμό εργαλείων anti-forensics και την πρόσβαση του χρήστη σε αρχεία και καταλόγους, ενώ δόθηκε ιδιαίτερη σημασία και στα εργαλεία που χρησιμοποιούνται για την ανάλυση πειστηρίων. Επιπλέον, διερευνήθηκαν μη-τεχνικοί μέθοδοι προσέγγισης που μπορούν να ενισχύσουν την ερευνητική διαδικασία όταν τα τεχνικά μέσα δεν είναι επαρκή. Η μη-τεχνική προσέγγιση των τεχνικών anti-forensics μπορεί να επιτευχθεί μέσα από τη διεύρυνση της έρευνας πέρα από τα υπό ανάλυση

ψηφιακά μέσα και λαμβάνοντας υπόψιν τον ανθρώπινο παράγοντα που τον οδηγούν σε λάθη και παραλείψεις.

Κεφάλαιο 5 Μελέτη Περίπτωσης

Σε αυτό το κεφάλαιο πραγματοποιείται η μελέτη περίπτωσης εφαρμογής τεχνικών anti-forensics σε μία υπόθεση υποκλοπής δεδομένων και η προσέγγισή της με τεχνικά μέσα που μελετήθηκαν στο τέταρτο κεφάλαιο.

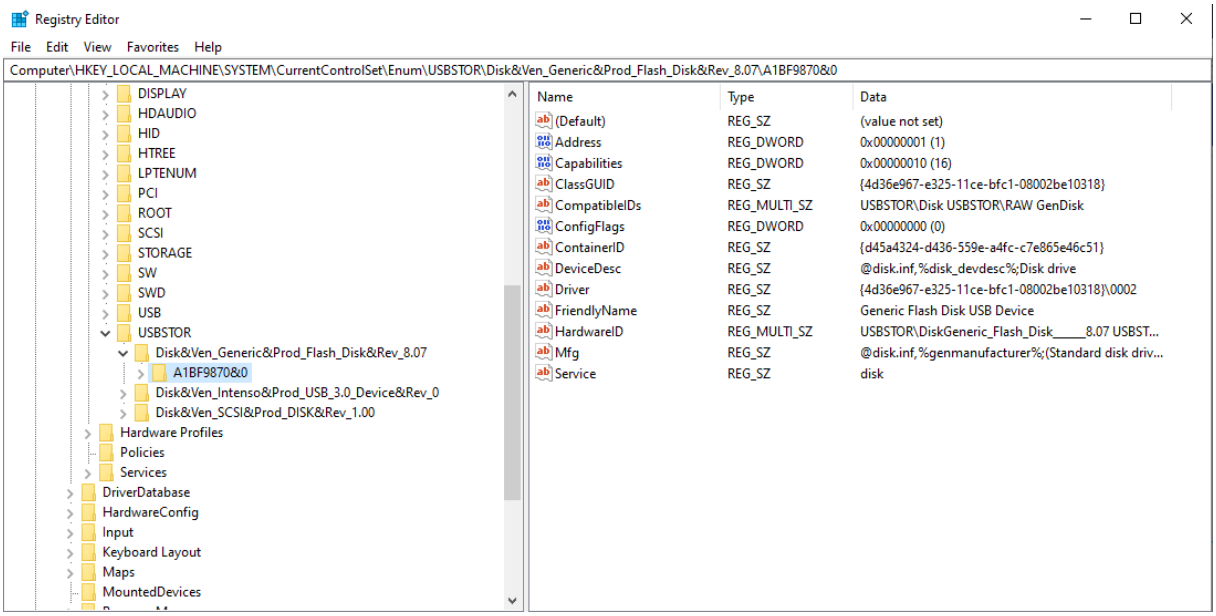
5.1 Σενάριο

Ο κύριος Ο.Ε., γραμματέας της φανταστικής εταιρείας τηλεφώνων ‘aPhone’, πρόσφατα ζήτησε την παραίτησή του από την, καθώς είχε μία καλύτερη επαγγελματική πρόταση. Ο Διευθύνον Σύμβουλος της εταιρείας ισχυρίζεται πως ο Ο.Ε. είχε πρόσβαση σε εταιρικό υπολογιστή με εμπιστευτικά αρχεία. Υποψιαζόμενος πως ο Ο.Ε. σκοπεύει να διαρρεύσει τα σχέδια για το νέο μοντέλο ‘aPhone Pro’ στην ανταγωνιστική εταιρεία ‘bPhone’, ζήτησε να διερευνηθεί η υπόθεση. Ο Ο.Ε. θεωρώντας πως δεν έχει να κρύψει κάτι συνεργάζεται και δέχεται να γίνει έλεγχος στο προσωπικό του laptop και τις συσκευές που διαθέτει.

Έτσι, στη διάθεσή μας έχουμε τον εταιρικό υπολογιστή με λειτουργικό σύστημα Windows 10 (64-bit) στον οποίο βρίσκονται τα αρχεία ενδιαφέροντος, ένα εικονικό αρχείο (image) του USB stick που είχε στην κατοχή του ο Ο.Ε., καθώς και το προσωπικό του laptop με λειτουργικό σύστημα Windows 7 (32-bit). Στόχος είναι να βρούμε πειστήρια τα οποία στηρίζουν ή απορρίπτουν τον ισχυρισμό πως ο Ο.Ε. έχει στην κατοχή του τα εμπιστευτικά αρχεία.

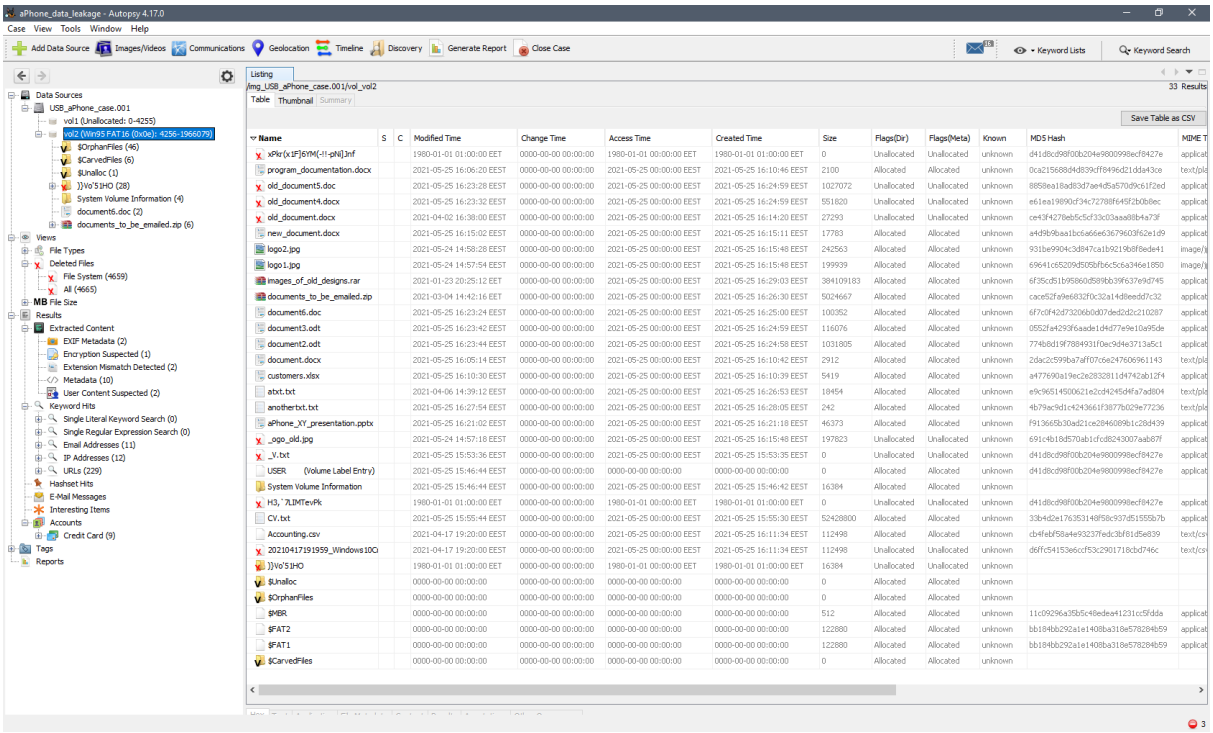
5.2 Εξέταση USB stick

Κατά τη διαδικασία δημιουργίας αρχείου εικόνας του USB stick, το εργαλείο FTK Imager παρέχει ορισμένες πληροφορίες για το αποθηκευτικό μέσο, μεταξύ των οποίων, και το σειριακό του αριθμό ο οποίος, στην προκειμένη περίπτωση, είναι ο ‘A1BF9870’. Αναζητώντας στο κλειδί μητρώου HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR συσκευές USB που έχουν συνδεθεί στον εταιρικό υπολογιστή , βλέπουμε πως έχει συνδεθεί συσκευή με σειριακό αριθμό ίδιο με αυτόν που είχε στην κατοχή του ο Ο.Ε. (σχήμα 5.1).



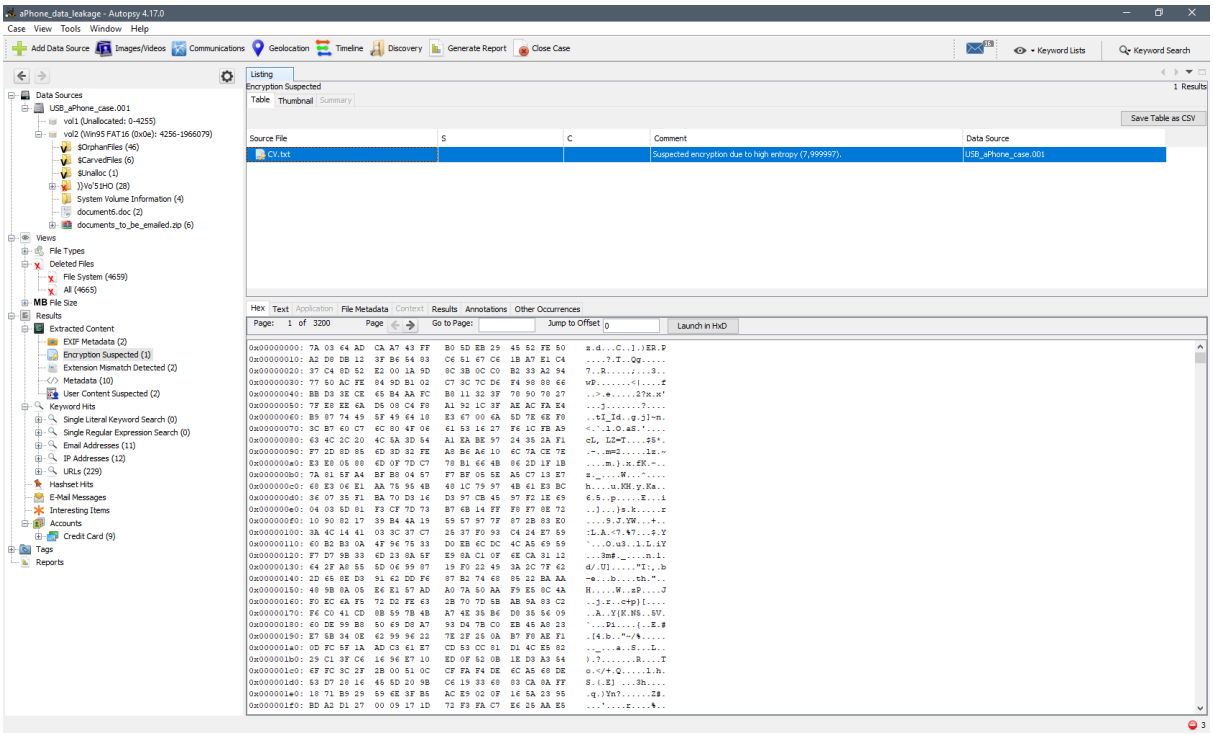
Σχήμα 5.1 Εντοπισμός του σειριακού αριθμού το USB stick προς ανάλυση στον εταιρικό υπολογιστή

Εξετάζοντας το αρχείο εικόνας του USB stick με το εργαλείο Autopsy, με μια πρώτη ματιά δεν διακρίνουμε τα αρχεία ενδιαφέροντος, αν και υπάρχουν αρχεία τα οποία φαίνεται πως έχουν διαγραφεί με πρόγραμμα ασφαλούς καταστροφής αρχείων (τα ονόματα αυτών έχουν αντικατασταθεί με τυχαίες συμβολοσειρές) σε αντίθεση με ορισμένα αρχεία που έχουν διαγραφεί μέσω του λειτουργικού συστήματος (και, επομένως, έχουν διατηρήσει το όνομά τους). Τα περιεχόμενα του USB stick απεικονίζονται στο σχήμα 5.2.



Σχήμα 5.2 Περιεχόμενα του USB stick προς ανάλυση

Εξετάζοντας τα αποτελέσματα από τις λειτουργίες που παρέχει το Autopsy, βλέπουμε πως εντόπισε, μεταξύ άλλων, πιθανή χρήση κρυπτογραφίας σε ένα αρχείο με όνομα 'CV.txt'. Προβάλλοντας το περιεχόμενο του αρχείου βλέπουμε ότι δεν ανταποκρίνεται στο περιεχόμενο ενός συνηθισμένου αρχείου κειμένου txt (καθαρό κείμενο), όπως διακρίνεται στο σχήμα 5.3. Επιπλέον, το μέγεθός του (50 MB) είναι ασυνήθιστα μεγάλο για αρχεία αυτού του είδους. Αφού εξάγουμε το αρχείο CV.txt αναζητούμε με την υπογραφή του, τον τύπο αρχείου στο οποίο αντιστοιχεί, χωρίς όμως να έχουμε κάποιο αποτέλεσμα (σχήμα 5.4).

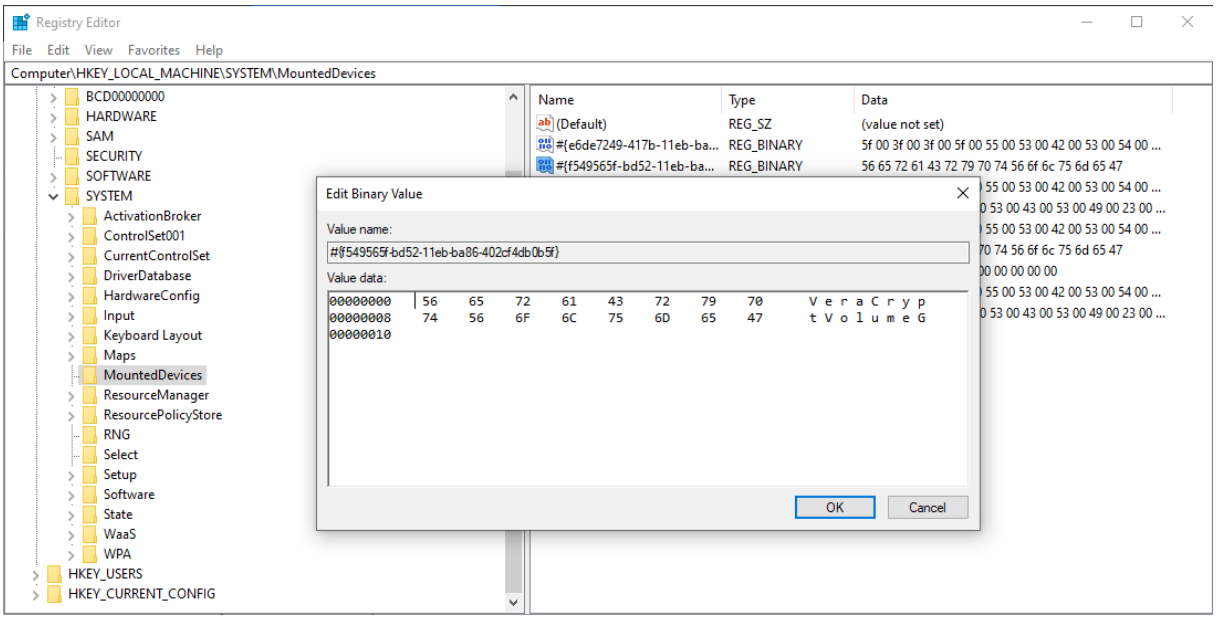


Σχήμα 5.3 Περιεχόμενο του αρχείου CV.txt

Σχήμα 5.4 Αναζήτηση πιθανού τύπου αρχείου χρησιμοποιώντας την υπογραφή του 'CV.txt'

5.3 Εξέταση εταιρικού υπολογιστή

Συνεχίζοντας την έρευνα στον εταιρικό υπολογιστή και εξετάζοντας το κλειδί HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices, βλέπουμε πως στο σύστημα έχει προσαρτιστεί κρυπτογραφημένος τόμος που δημιουργήθηκε με το εργαλείο VeraCrypt (σχήμα 5.5). Επομένως, το αρχείο CV.txt πιθανόν να είναι ένας κρυπτογραφημένος τόμος. Για να επιβεβαιωθεί αυτή η υπόθεση, μένει να δούμε αν υπάρχουν ίχνη του εργαλείου VeraCrypt στον προσωπικό υπολογιστή του Ο.Ε. αλλά και ίχνη των εμπιστευτικών αρχείων.

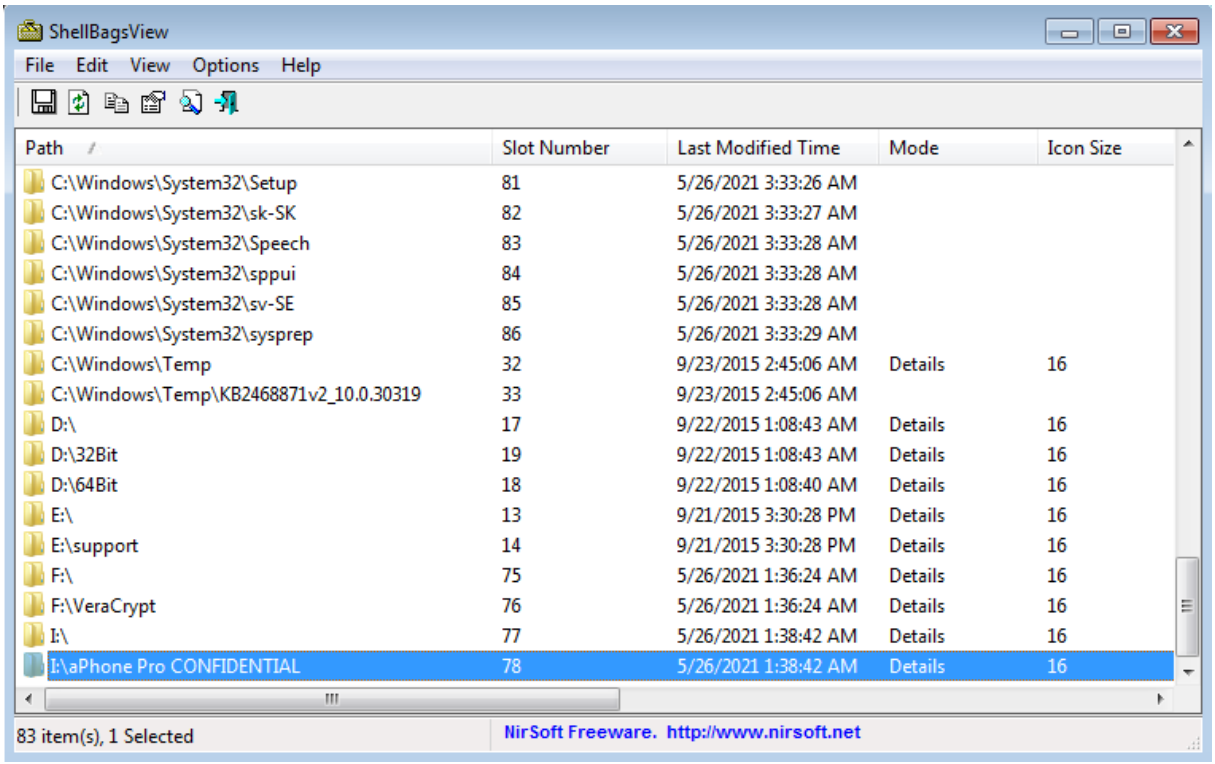


Σχήμα 5.5 Ίχνη κρυπτογραφημένου τόμου στα κλειδί μητρώου MountedDevices

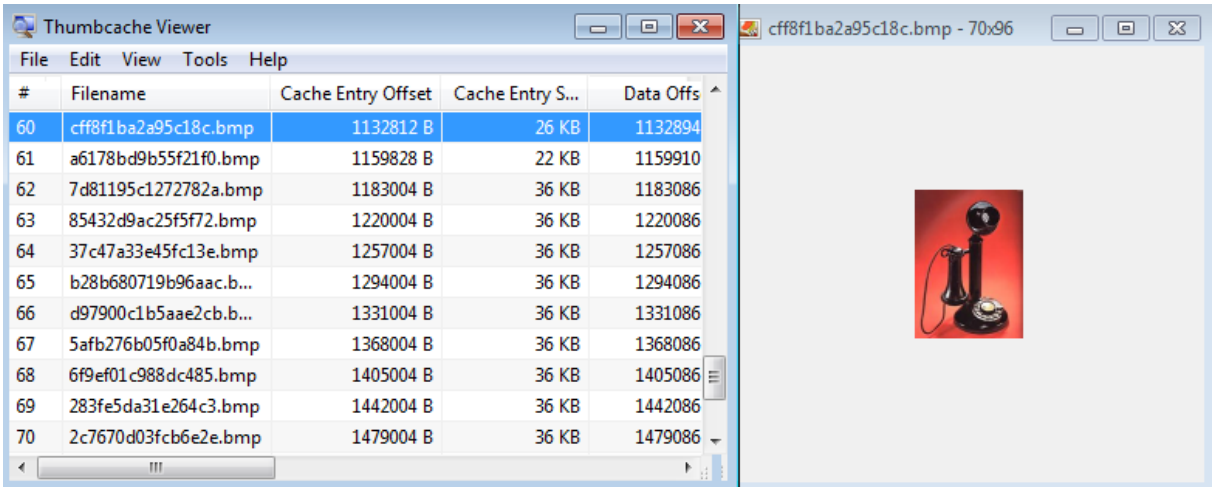
5.4 Εξέταση προσωπικού υπολογιστή

Στον προσωπικό υπολογιστή του Ο.Ε. εκτελούμε ορισμένα εργαλεία για την εξαγωγή πληροφοριών από τις λειτουργίες του συστήματος. Εκτελώντας το πρόγραμμα ShellBagsView, για την προβολή των shellbags, βλέπουμε πως έχει προβληθεί ένας φάκελος με όνομα VeraCrypt και ο φάκελος με τα εμπιστευτικά αρχεία από εξωτερικές συσκευές (σχήμα 5.6). Επομένως, μπορούμε να συμπεράνουμε πως ο Ο.Ε. εκτέλεσε το εργαλείο VeraCrypt από το USB stick για να προσαρτίσει στο σύστημα τον κρυφό τόμο, στον οποίο αποθήκευσε τα εμπιστευτικά αρχεία, αναθέτοντάς του το γράμμα 'I'.

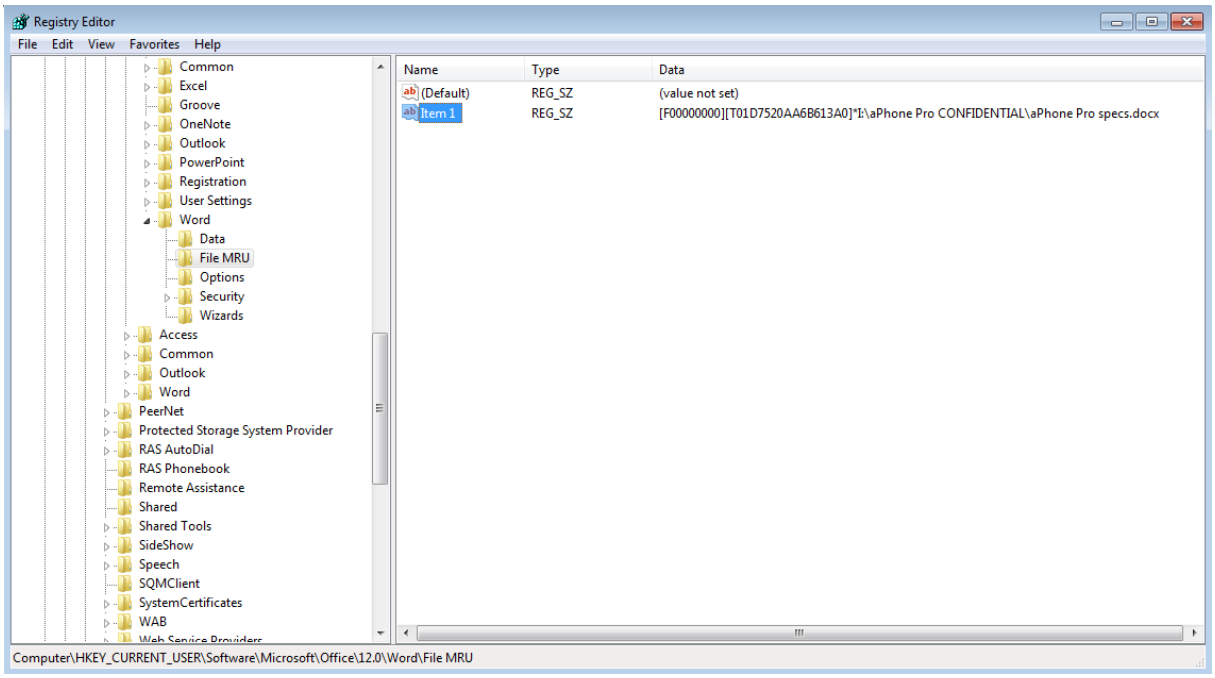
Ελέγχοντας τα αρχεία προσωρινής μνήμης με μικρογραφίες εικόνων (thumbnail cache) και τα αρχεία που έχουν προσπελαστεί πρόσφατα μπορούμε να δούμε ορισμένα από τα εμπιστευτικά αρχεία όπως φαίνεται στα σχήματα 5.7 και 5.8.



Σχήμα 5.6 Αποτελέσματα από την εξέταση των shellbags στον προσωπικό υπολογιστή του Ο.Ε.



Σχήμα 5.7 Εύρεση εμπισευτικών αρχείων στην προσωρινή μνήμη μικρογραφιών



Σχήμα 5.8 Εύρεση εμπιστευτικών αρχείων στα πρόσφατα αρχεία του Word.

Επομένως, μπορούμε να ισχυριστούμε πως τα στοιχεία που προέκυψαν από την έρευνα αποδεικνύουν τον ισχυρισμό πως ο Ο.Ε. είχε στην κατοχή του τα εμπιστευτικά αρχεία.

Κεφάλαιο 6 Συμπεράσματα – Συζήτηση – Μελλοντική Έρευνα

6.1 Συμπεράσματα

Στην παρούσα διπλωματική εργασία αναλύθηκαν οι τεχνικές anti-forensics οι οποίες ταξινομήθηκαν σε τέσσερις βασικές κατηγορίες που πρότεινε ο Mark Rogers. Ωστόσο, είδαμε πως δεν είναι εύκολη η αποκλειστική ταξινόμηση ορισμένων τεχνικών, αφού είναι δυνατό να ταξινομηθούν σε περισσότερες κατηγορίες ανάλογα με τον τρόπο προσέγγισης τους. Στη συνέχεια, έγινε πρακτική εφαρμογή τεχνικών anti-forensics μέσω της οποίας παρατηρήθηκαν τα αποτελέσματα αυτών στο σύστημα ή τα δεδομένα στα οποία εφαρμόζονται. Το βασικό συμπέρασμα που προέκυψε από την παρατήρηση είναι ότι σε πολλές περιπτώσεις ο εντοπισμός των τεχνικών anti-fortensics είναι αδύνατος εξετάζοντας μόνο τα δεδομένα στα οποία έχουν εφαρμοστεί.

Έπειτα, αναλύθηκαν τεχνικοί και μη-τεχνικοί μέθοδοι προσέγγισης των τεχνικών anti-forensics. Από αυτήν την ανάλυση προκύπτουν δύο κύρια συμπεράσματα. Αρχικό συμπέρασμα αποτελεί η σημασία της ανάλυσης συστημάτων σε λειτουργία. Η ανάλυση συστημάτων σε λειτουργία παρέχει στον ερευνητή μία σπουδαία πηγή πληροφοριών, όπως τα δεδομένα στο μητρώο του λειτουργικού συστήματος Windows, και τα δεδομένα που βρίσκονται αποθηκευμένα στη μνήμη RAM, όπως κωδικοί πρόσβασης και αποκρυπτογραφημένα δεδομένα. Το επόμενο βασικό συμπέρασμα είναι η ανάγκη της επέκτασης της έρευνας πέρα από το υπό ανάλυση ψηφιακό μέσο. Ο βασικός στόχος των τεχνικών anti-forensics είναι η παρεμπόδιση της ερευνητικής διαδικασίας η οποία βασίζεται κατά κύριο λόγο σε γνωστές διαδικασίες ανάλυσης των δεδομένων από αποθηκευτικά μέσα. Επομένως, η αντιμετώπισή τους με τεχνικά μέσα δεν είναι πάντα εφικτή. Αυτό σημαίνει πως η έρευνα πρέπει να στραφεί σε μη τεχνικές μεθόδους, οι οποίες θα κατέχουν συμπληρωματικό ρόλο στην αναζήτηση πληροφοριών.

6.2 Συζήτηση

Αφού έχει γίνει αναφορά σε τρόπους αντιμετώπισης των τεχνικών anti-forensics, οδηγούμαστε στο εξής ερώτημα: Υπάρχει δυνατότητα εφαρμογής μεθοδολογιών για την αντιμετώπιση των τεχνικών anti-forensics ή λήψης μέτρων για την πρόληψή τους; Ας εξετάσουμε κάθε μία από τις βασικές κατηγορίες των τεχνικών anti-forensics ξεκινώντας από την καταστροφή πειστηρίων. Η καταστροφή πειστηρίων είναι δύσκολο να αποτραπεί, πόσο μάλλον να αντιμετωπιστεί αφού έχει πραγματοποιηθεί. Για να αποτραπεί η καταστροφή δεδομένων θα πρέπει να μην γνωστοποιείται η επερχόμενη έρευνα στον ύποπτο, ώστε να μην διαθέτει το χρονικό περιθώριο να προβεί στην καταστροφή των πειστηρίων. Ωστόσο, πολλές διαδικτυακές υπηρεσίες ενημερώνουν τους χρήστες σε περίπτωση αιτήματος για πληροφορίες από τις αρχές, εκτός από περιπτώσεις στις οποίες απαγορεύεται από τον νόμο, κρίνεται ως έκτακτη περίπτωση ανάγκης ή θα είχε αρνητικές επιπτώσεις στην έρευνα.

Όσον αφορά την απόκρυψη πειστηρίων, η πρόληψή τους δεν είναι εφικτή. Η αντιμετώπισή τους όμως είναι δυνατή εφαρμόζοντας τους τρόπους προσέγγισης που παρουσιάστηκαν στο τέταρτο κεφάλαιο. Οι ερευνητές οφείλουν να είναι εξοικειωμένοι με τις τεχνικές anti-forensics και να λαμβάνουν πλήρη και συνεχή εκπαίδευση στην οποία θα συμπεριλαμβάνονται και τρόποι διαχείρισης των τεχνικών αυτών. Σε ορισμένες χώρες ισχύουν νομοθεσίες οι οποίες υποχρεώνουν τους παρόχους υπηρεσιών

κρυπτογραφίας ή τους χρήστες να συνεργάζονται με τις Αρχές παρέχοντας πρόσβαση στα κρυπτογραφημένα δεδομένα [139]. Παρομοίως, υπάρχουν και νομοθεσίες που απαγορεύουν τη χρήση υπηρεσιών VPN [140] ή προσπαθούν να παρεμποδίσουν την πρόσβαση σε δίκτυα και εφαρμογές ανωνυμίας, που εντάσσονται στην κατηγορία της απόκρυψης ιχνών. Ωστόσο, όταν η νομοθεσία εφαρμόζεται καθολικά και όχι σε εξαιρετικές περιπτώσεις, όπου κάτι τέτοιο κρίνεται αναγκαίο για τη δημόσια ασφάλεια ή την ασφάλεια ενός ατόμου, καταπατούνται τα δικαιώματα των ανθρώπων στην ελεύθερη έκφραση και την ιδιωτικότητα.

Τέλος, η επίθεση στα εργαλεία και τις διαδικασίες μπορεί να αντιμετωπιστεί και να προληφθεί με τις μεθόδους που αναφέρθηκαν στο τέταρτο κεφάλαιο. Η ερευνητική διαδικασία βασίζεται κατά κύριο λόγο στη χρήση προγραμμάτων τα οποία πρέπει να ελέγχονται πριν τη χρήση τους, αλλά και να είναι γνωστός ο τρόπος λειτουργίας τους από τον ερευνητή. Επίσης, η χρήση διαφορετικών εργαλείων για τον ίδιο σκοπό μπορεί σε ορισμένες περιπτώσεις να αποτελεί μία χρονοβόρα διαδικασία, ωστόσο παράγονται πιο σίγουρα αποτελέσματα.

Συνοψίζοντας, η εφαρμογή μεθοδολογιών για την αντιμετώπιση τεχνικών anti-forensics ή η λήψη μέτρων πρόληψης δεν είναι πάντοτε εφικτή ή απαιτεί την καταπάτηση ανθρωπίνων δικαιωμάτων. Αυτό οφείλεται στο ότι οι τεχνικές anti-forensics (όπως αναφέρθηκε στο πρώτο κεφάλαιο) ουσιαστικά αποτελούν τεχνικές που υπό άλλες συνθήκες εφαρμόζονται για εύλογους σκοπούς όπως η ανωνυμία και η προστασία των δεδομένων.

6.3 Μελλοντική Έρευνα

Στην παρούσα διπλωματική εργασία αναλύθηκαν οι πιο κοινοί τύποι τεχνικών anti-forensics. Για την τεχνική τους αντιμετώπιση μελετήθηκαν κατά κύριο λόγο λειτουργίες του λειτουργικού συστήματος Windows, καθώς κατέχει το μεγαλύτερο μερίδιο στην αγορά των λειτουργικών συστημάτων, παγκοσμίως. Ωστόσο, αυτό αφορά λειτουργικά συστήματα υπολογιστών. Πλέον, η χρήση κινητών τηλεφώνων έχει ξεπεράσει αυτή των υπολογιστών και, επομένως, είναι πολύ πιθανό τα ψηφιακά πειστήρια να συλλέγονται από κάποια κινητή συσκευή. Αυτό σημαίνει πως μελλοντικές έρευνες πρέπει να εστιάσουν σε λειτουργικά συστήματα, όπως το Android και το iOS, για την ανάλυση τεχνικών anti-forensics που εφαρμόζονται σε κινητά τηλέφωνα.

Περεταίρω μελέτη πάνω σε εργαλεία anti-forensics θα βοηθούσε στη δημιουργία εργαλείων για τον εντοπισμό τους. Κατά τη μελέτη τρόπων αντιμετώπισης των τεχνικών anti-forensics έγινε αναφορά σε λειτουργίες του συστήματος Windows, όπως το μητρώο, που μπορεί να εκμεταλλευτεί ο ερευνητής για τον εντοπισμό εργαλείων στεγανογραφίας, κρυπτογραφίας, καταστροφής δεδομένων, κ.α. Η αναζήτηση σε κλειδιά του μητρώου και αρχεία του συστήματος για τον εντοπισμό εργαλείων anti-forensics, αποτελεί μία διαδικασία η οποία μπορεί να αυτοματοποιηθεί με τη χρήση εργαλείων. Ωστόσο, θα πρέπει να προηγηθεί έρευνα πάνω στα υπάρχοντα εργαλεία anti-forensics. Επιπλέον, η έρευνα πάνω στα εργαλεία anti-forensics μπορεί να εστιάσει στα ιδιαίτερα χαρακτηριστικά του κάθε εργαλείου και της επίδρασής τους πάνω σε δεδομένα και στο σύστημα, δηλαδή στην υπογραφή του, όπως συμβαίνει και με την ανάλυση κακόβουλου λογισμικού.

Τέλος, μελλοντική έρευνα μπορεί να πραγματοποιηθεί ώστε να προταθούν μεθοδολογίες που εντάσσουν τις πληροφορίες OSINT στην εγκληματολογική έρευνα. Οι πληροφορίες αυτές χρησιμοποιούνται κατά τη διερεύνηση γενικότερων υποθέσεων, όμως δεν λαμβάνονται πάντα υπόψη

σε υποθέσεις της ψηφιακής εγκληματολογίας, η οποία συχνά περιορίζεται στα υπό εξέταση ψηφιακά μέσα. Επιπλέον, η μελέτη της ανθρώπινης φύσης και ψυχολογίας για τον εντοπισμό ιδιαίτερων χαρακτηριστικών και συμπεριφορών των κυβερνοεγκληματιών γενικότερα, αλλά και του εκάστοτε υπόπτου, μπορεί να αποβεί χρήσιμη στην έρευνα η οποία θα μπορεί να προσανατολίζεται ανάλογα με την αναμενόμενη συμπεριφορά του υπόπτου.

Βιβλιογραφία

[1] K. Zatyko, "Commentary: Defining Digital Forensics", *Forensic Magazine*, no. 1, p. 18, 2007.

[2] "5 Cases Cracked With Digital Forensics", *International Private Investigative Group*, 2020. [Online]. Available: https://www.iigpi.com/5-cases-cracked-with-digital-forensics/. [Accessed: 08- Nov- 2020].

[3] "Γνήσια ηλεκτρονικά εγκλήματα", *Sites.google.com*. [Online]. Available: https://sites.google.com/site/elektronikoenklema2012/morphes-tou-elektronikou-enklematos/gnesia-elektronika-enklemata. [Accessed: 04- May- 2021].

[4] "Εγκλήματα με την χρήση Η/Υ(ως βοηθητικό μέσο)", *Sites.google.com*. [Online]. Available: https://sites.google.com/site/elektronikoenklema2012/morphes-tou-elektronikou-enklematos/enklemata-me-ten-chrese-e-y-os-boethetiko-meso. [Accessed: 04- May- 2021].

[5] Y. Yusoff, R. Ismail and Z. Hassan, "Common Phases of Computer Forensics Investigation Models", *International Journal of Computer Science and Information Technology*, vol. 3, no. 3, pp. 17-31, 2011. doi: 10.5121/ijcsit.2011.3302.

[6] M. Lessing and B. Von Solms, "Live Forensic Acquisition as Alternative to Traditional Forensic Processes", in *4th International Conference on IT Incident Management & IT Forensics*, Mannheim, Germany, 2008.

[7] S. Selamat, R. Yusof and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework", *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 10, pp. 163-168, January 2008.

[8] D. Garrie, "Understanding a Digital Forensics Report", *Legal Executive Institute*, 2016. [Online]. Available: https://www.legalexecutiveinstitute.com/understanding-digital-forensics-report/. [Accessed: 09- Nov- 2020].

[9] N. Karie, V. Kebande, H. Venter and K. Choo, "On the importance of standardising the process of generating digital forensic reports", *Forensic Science International: Reports*, vol. 1, article 100008, November 2019. doi: 10.1016/j.fsir.2019.100008.

[10] J. Sachowski, *Digital forensics and investigations: People, Processes, and Technologies to Defend the Enterprise*, 1st ed. Boca Raton: CRC Press, 2018.

[11] M. Khanafseh, M. Qatawneh and W. Almobaideen, "A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics", *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, pp. 610-627, January 2019. doi: 10.14569/ijacsa.2019.0100880.

[12] "Desktop vs Mobile vs Tablet Market Share Worldwide - January 2021", *StatCounter Global Stats*. [Online]. Available: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide. [Accessed: 12- Nov- 2020].

[13] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues", *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191-1221, January 2020. doi: 10.1109/comst.2019.2962586.

[14] K. Conlan, I. Baggili and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy", *Digital Investigation*, vol. 18, pp. 66-75, August 2016. doi: 10.1016/j.diin.2016.04.006.

[15] D. M. Rogers, (2005). Anti-Forensic [slide 3]. Available: https://www.researchgate.net/profile/Marcus_Rogers/publication/268290676_Anti-Forensics_Anti-Forensics/links/575969a908aec91374a3656c.pdf.

[16] C. Thuen, "Understanding Counter-Forensics to Ensure a Successful Investigation", 2007, [online], Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.138.2196.

[17] "hephaest0s/usbkill", *GitHub*. [Online]. Available: https://github.com/hephaest0s/usbkill. [Accessed: 13- Feb- 2021].

[18] C. Boyd and P. Forster, "Time and date issues in forensic computing—a case study", *Digital Investigation*, vol. 1, no. 1, pp. 18-23, February 2004. doi: 10.1016/j.diin.2004.01.002.

[19] J. Van Belle, "Anti-Forensics: A Practitioner Perspective", *International Journal of Cyber-Security and Digital Forensics*, vol. 4, no. 2, pp. 390-403, January 2015. doi: 10.17781/p001593.

[20] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, *Special Publication (NIST SP) - 800-88 Rev 1*, doi: http://dx.doi.org/10.6028/NIST.SP.800-88r1.

[21] "DoD Information Security Program: Protection of Classified Information", no. 5200.01, Department of Defense, Feb. 24, 2012. Accessed on: Nov. 12, 2020. [Online]. Available: https://www.dodig.mil/Portals/48/Documents/Policy/520001_vol3.pdf.

[22] "Tor: Overview", *2019.torproject.org*. [Online]. Available: https://2019.www.torproject.org/about/overview.html.en. [Accessed: 14- Nov- 2020].

[23] N. Sunde and I. E. Dror, "Cognitive and human factors in digital forensics: Problems, challenges, and the way forward," *Digital Investigation*, vol. 29, pp. 101-108, June 2019. doi: 10.1016/j.diin.2019.03.011.

[24] K. Cherry, "What Is Cognitive Bias?", *Verywell Mind*. [Online]. Available: https://www.verywellmind.com/what-is-a-cognitive-bias-2794963. [Accessed: 17- Nov- 2020].

[25] I. Dror, "Biases in forensic experts", *Science*, vol. 360, no. 6386, pp. 243-243, April 2018. doi: 10.1126/science.aat8443.

[26] C. Wilson, "Digital Evidence Discrepancies - Casey Anthony Trial", *Digital Detective*, 2011. [Online]. Available: https://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/. [Accessed: 17- Nov- 2020].

[27] "Findings From The Forensic Focus 2018 Survey - Forensic Focus", *Forensic Focus*. [Online]. Available: https://www.forensicfocus.com/articles/findings-from-the-forensic-focus-2018-survey/. [Accessed: 19- Nov- 2020].

[28] D. Kovar, "The value of push button forensics", *Integriography: A Journal of Broken Locks, Ethics, and Computer Forensics*. November 17, 2009. [Blog]. Available: https://integriography.wordpress.com/2009/11/17/the-value-of-push-button-forensics/, Accessed on: Nov. 20, 2020.

[29] J. I. James and P. Gladyshev, “Challenges with Automation in Digital Forensic Investigations”, *ArXiv*, 2013. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.4498.pdf

[30] B. Cusack και A. Homewood, ‘Identifying Bugs In Digital Forensic Tools’, 11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013 at Edith Cowan University, Western Australia, 2013, doi: 10.4225/75/57B3C3BEFB86C.

[31] Y. Guo, J. Slay and J. Beckett, "Validation and verification of computer forensic software tools—Searching Function", *Digital Investigation*, vol. 6, pp. S12-S22, September 2009. doi: 10.1016/j.diin.2009.06.015.

[32] J. Gillum, "Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned", *ProPublica*, 2019. [Online]. Available: https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned. [Accessed: 20- Nov- 2020].

[33] R. Overill, M. Kwan, K.-P. Chow, P. Lai, και F. Law, ‘A Cost-Effective Model for Digital Forensic Investigations’, in Advances in Digital Forensics V, Springer Berlin Heidelberg, 2009, pp. 231–240.

[34] T. Moore, “The economics of digital forensics”, Fifth Workshop on the Economics of Information Security, 26–28 June, 2006, Cambridge, UK.

[35] J. Brunty, “Mobile device forensics: threats, challenges, and future trends,” in Digital Forensics Threatscape and Best Practices, J. Sammons, Ed., Waltham, MA, USA: Syngress, 2016, pp. 69–84.

[36] AP, "This Doctor's Drug Charges Were Dropped Because There Was Too Much Evidence", *Business Insider*, 2012. [Online]. Available: https://www.businessinsider.com/charges-dropped-against-armando-angulo-2012-8. [Accessed: 23- Nov- 2020].

[37] Council of Europe, *European Convention on Human Rights, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, Available: https://www.echr.coe.int/Documents/Convention_ENG.pdf

[38] Electronic Communications Privacy Act of 1986

[39] A. Xrysanthou and I. Apostolakis, "Network Forensics: Problems and Solutions", in *E-Democracy: Challenges of the Digital Era*, Athens, 2006, pp. 307-318.

[40] Νόμος 4620/2019 - ΦΕΚ 96/Α/11-6-2019 Κύρωση του Κώδικα Ποινικής Δικονομίας

[41] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, “Cloud forensics: An overview”, January 2011.

[42] A. Wayne, "TECHNOLOGY; Philippines to Drop Charges on E-Mail Virus", *Nytimes.com*, 2000. [Online]. Available: https://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html. [Accessed: 22- Nov- 2020].

[43] "Choose an AWS Region", *AWS*. [Online]. Available: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-region.html. [Accessed: 20- Apr- 2021].

[44] "Azure geographies", *Microsoft Azure*. [Online]. Available: https://azure.microsoft.com/en-us/global-infrastructure/geographies/. [Accessed: 20- Apr- 2021].

[45] Νόμος 4619/209 - ΦΕΚ 95/Α/11-6-2019 Κύρωση του Ποινικού Κώδικα

[46] M. Rogers, "Anti-Forensics," presented at Lockheed Martin, San Diego, California, US, September 15, 2005. Anailable: https://www.researchgate.net/profile/Marcus-Rogers-2/publication/268290676_Anti-Forensics_Anti-Forensics/links/575969a908aec91374a3656c/Anti-Forensics-Anti-Forensics.pdf.

[47] N. A. Hassan, "Antiforensics Techniques," in *Digital Forensics Basics: A Practical Guide Using Windows OS*, Berkeley, CA, US: Apress, 2019, pp. 291-310.

[48] "What Are the Different Types of Data Destruction and Which One Should You Use?", *DataSpan*, October 3, 2018. [Blog]. Available: https://www.dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/ , Accessed on: Nov. 27, 2020.

[49] W. Stallings, "Εξωτερική Μνήμη," στο *Οργάνωση & Αρχιτεκτονική Υπολογιστών*, Μ. Ρουμελιώτης, Επιμ., 10η έκδ. Θεσσαλονίκη, Ελλάδα: Τζιόλα, 2017, κεφ.6, τμ.1, σσ. 195–228.

[50] "What Is a Degausser and How Does It Work?", *Securis.com*, 2016. [Online]. Available: https://securis.com/what-is-a-degausser-and-how-does-it-work/. [Accessed: 27- Nov- 2020].

[51] A. Rubtsov, "HDD from inside: Tracks and Zones.", *HDDscan*. [Online]. Available: https://hddscan.com/doc/HDD_Tracks_and_Zones.html. [Accessed: 27- Nov- 2020].

[52] "Master File Table (Local File Systems)", *Docs.microsoft.com*, 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/fileio/master-file-table. [Accessed:29- Nov- 2020].

[53] D. McKay, "Everything You Ever Wanted to Know About inodes on Linux", *How-To Geek*, 2020. [Online]. Available: https://www.howtogeek.com/465350/everything-you-ever-wanted-to-know-about-inodes-on-linux/. [Accessed: 29- Nov- 2020].

[54] W. Bux and I. Iliadis, "Performance of greedy garbage collection in flash-based solid-state drives", *Performance Evaluation*, vol. 67, no. 11, pp. 1172-1186, 2010. Available: 10.1016/j.peva.2010.07.003 [Accessed 29 Nov 2020].

[55] R. Stiennon, "Everything You Need to Know About DoD 5220.22-M Wiping Standard & Its Applications Today", *Blancco*, 2019. [Online]. Available: https://www.blancco.com/blog-dod-5220-22-m-wiping-standard-method/. [Accessed: 30- Nov- 2020].

[56] "CryptoLocker Ransomware Information Guide and FAQ", *BleepingComputer*, 2013. [Online]. Available: https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information. [Accessed: 02- Dec- 2020].

[57] C. Boyd, "SamSam ransomware: what you need to know", *Malwarebytes Labs*, 2018. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/. [Accessed: 02- Dec- 2020].

[58] D. Edwards, *Computer Forensic TimelineAnalysis with Tapestry*, SANS Institute, November 12, 2011. Accessed on: December 6, 2020. [Online]. Available: https://www.sans.org/reading-room/whitepapers/forensics/computer-forensic-timeline-analysis-tapestry-33836

[59] Exchangeable image file format for digital still cameras:Exif Version 2.3, JEITA CP－3451C, 2010. [Online]. Available: https://www.exif.org/Exif2-2.PDF

[60] N. Kuncik and A. Harbison, “Counter forensics techniques - a brief overview”. Available: https://www.yumpu.com/en/document/read/47811787/counter-forensics-techniques-a-a-brief-overview-grant-thornton

[61] M. Hosenball, "FBI paid under $1 million to unlock San Bernardino iPhone: sources", *Reuters*, 2016. [Online]. Available: https://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032. [Accessed: 08- Dec- 2020].

[62] Παγουρτζής, Α., Ζάχος, Ε., *Υπολογιστική κρυπτογραφία*. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015. Διαθέσιμο: http://hdl.handle.net/11419/5439

[63] "How long does it take to crack encryption?", *Findanyanswer.com*. [Online]. Available: https://findanyanswer.com/how-long-does-it-take-to-crack-encryption. [Accessed: 10- Dec- 2020].

[64] "VeraCrypt - Free Open source disk encryption with strong security for the Paranoid", *Veracrypt.fr*. [Online]. Available: https://www.veracrypt.fr/en/Hidden%20Volume.html. [Accessed: 12- Apr- 2021].

[65] Z. AL-Ani, A. Zaidan, B. Zaidan and H. Al-Anaz, "Overview: Main Fundamentals for Steganography", *Journal of Computing*, vol. 2, no. 3, pp. 158-165, 2010. Available: https://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdf. [Accessed 13 December 2020].

[66] D. Molina, M. Zimmerman, G. Roberts, M. Eaddieand and G. Peterson, “Timely rootkit detection during live response” 2008, in IFIP International Federation for Information Processing, Volume 285; Advances in Digital Forensics IV; Indrajit Ray, Sujeet Shenoi; (Boston: Springer), pp. 139–148.

[67] R. L. Means, Alternate Data Streams: Out of the Shadows and into the Light, SANS Institute, 2003. Available: https://www.giac.org/paper/gcwn/230/alternate-data-streams-shadows-light/104234

[68] "[MS-FSCC]: NTFS Streams", *Docs.microsoft.com*, 2019. [Online]. Available: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/c54dec26-1551-4d3a-a0ea-4fa40f848eb3. [Accessed: 10- Dec- 2020].

[69] B. Brenner, "How BitPaymer ransomware covers its tracks", *Naked Security*, 2017. [Online]. Available: https://nakedsecurity.sophos.com/2017/09/21/how-bitpaymer-ransomware-covers-its-tracks/. [Accessed: 27- Dec- 2020].

[70] R. Parish, “Windows 2000 Streaming Virus”, November 20, 2000. Available: https://www.giac.org/paper/gsec/167/windows-2000-streaming-virus/100637

[71] K. Chiang and L. Lloyd, "A case study of the rustock rootkit and spam bot", in *Proceedings of the first Workshop on Hot Topics in Understanding Botnets*, 2007, p. 10.

[72] M. Gupta, M. Hoeschele and M. Rogers, "Hidden Disk Areas: HPA and DCO", *International Journal of Digital Evidence*, vol. 5, no. 1, 2006. [Accessed 29 Dec 2020].

[73] R. Leickly, Richard and D., David, Applications of Data Recovery Tools to Digital Forensics: Analyzing the Host Protected Area with the PC-3000.

[74] C. Hoffman, "Bad Sectors Explained: Why Hard Drives Get Bad Sectors and What You Can Do About It", *How-To Geek*, 2017. [Online]. Available: https://www.howtogeek.com/173463/bad-sectors-explained-why-hard-drives-get-bad-sectors-and-what-you-can-do-about-it/. [Accessed: 06- Jan- 2021].

[75] C. K. Wee, "Analysis of hidden data in the NTFS file system - Forensic Focus", *Forensic Focus*, 2006. [Online]. Available: https://www.forensicfocus.com/articles/analysis-of-hidden-data-in-the-ntfs-file-system/. [Accessed: 06- Jan- 2021].

[76] "Live CD - Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Live_CD. [Accessed: 10- Jan- 2021].

[77] "Tails", *Tails.boum.org*. [Online]. Available: https://tails.boum.org/. [Accessed: 10- Jan- 2021].

[78] W. Al Maawali, "Linux Kodachi 8.5 The Secure OS", *Digi77.com*, 2013. [Online]. Available: https://www.digi77.com/linux-kodachi/. [Accessed:10- Jan- 2021].

[79] Α. Γαρμπής, "Η χρήση των Εικονικών Μηχανών," σε *Λειτουργικά Συστήματα Θεωρητική & Πρακτική Προσέγγιση*, Αράκυνθος, 2010, κεφ. 4, σσ. 328–388.

[80] D. Balaban, "11 Types of Spoofing Attacks Every Security Professional Should Know About", *Securitymagazine.com*, 2020. [Online]. Available: https://www.securitymagazine.com/articles/91980-types-of-spoofing-attacks-every-security-professional-should-know-about. [Accessed: 4- Feb- 2021].

[81] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Proxies for Anonymous Routing," in 12th Annual Computer SecurityApplications Conference, San Diego, CA, December 9-13, 1996. doi:10.1109/CSAC.1996.569678

[82] "Freenet Project", *Freenetproject.org*. [Online]. Available: https://freenetproject.org [Accessed: 04- May- 2021].

[83] "I2P Anonymous Network", *Geti2p.net*. [Online]. Available: https://geti2p.net/en/. [Accessed: 04- May- 2021].

[84] Ι. Μαυρίδης, "Ιδεατά Προσωπικά Δίκτυα - VPN," στο *Ασφάλεια πληροφοριών στο διαδίκτυο*. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015, κεφ 10, σσ. 189-207. Διαθέσιμο: http://hdl.handle.net/11419/1034

[85] "Onion Over VPN NordVPN – your gate to ultimate privacy on the internet.", *NordVPN*. [Online]. Available: https://nordvpn.com/features/onion-over-vpn/. [Accessed: 05- Feb- 2021].

[86] A. Jain and G. Chhabra, "Anti-forensics techniques: An analytical review", *2014 Seventh International Conference on Contemporary Computing (IC3)*, 2014. doi: 10.1109/ic3.2014.6897209 [Accessed 8 Feb 2021].

[87] D. Skovli, "Killswitch", *Apps.danielskovli.com*, 2021. [Online]. Available: http://www.apps.danielskovli.com/killswitch/. [Accessed: 13- Feb- 2021].

[88] Xu Chen, J. Andersen, Z. M. Mao, M. Bailey, and J. Nazario, "Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware," presented at the 2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN), 2008, doi: 10.1109/dsn.2008.4630086.

[89] "Autopsy | Digital Forensics", *Autopsy*. [Online]. Available: https://www.autopsy.com/. [Accessed: 11- May- 2021].

[90] "FTK® Imager", *AccessData*. [Online]. Available: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager. [Accessed: 11- May- 2021].

[91] "Eraser – Secure Erase Files from Hard Drives", *Eraser*. [Online]. Available: https://eraser.heidi.ie/. [Accessed: 15- Feb- 2021].

[92] "Features | BleachBit", *Bleachbit.org*. [Online]. Available: https://www.bleachbit.org/features. [Accessed: 23- Feb- 2021].

[93] "Darik's Boot and Nuke", *En.wikipedia.org*. [Online]. Available: https://en.wikipedia.org/wiki/Darik%27s_Boot_and_Nuke. [Accessed: 24- Feb- 2021].

[94] "dd(1) - Linux manual page", *Man7.org*. [Online]. Available: https://man7.org/linux/man-pages/man1/dd.1.html. [Accessed: 24- Feb- 2021].

[95] M. Sanborn, "Wiping a Hard Drive with DD", *Marksanborn.net*, 2008. [Online]. Available: https://www.marksanborn.net/howto/wiping-a-hard-drive-with-dd/. [Accessed: 24- Feb- 2021].

[96] "shred(1) - Linux man page", *Linux.die.net*. [Online]. Available: https://linux.die.net/man/1/shred. [Accessed: 24- Feb- 2021].

[97]"scrub(1): patterns on disk/file - Linux man page", *Linux.die.net*. [Online]. Available: https://linux.die.net/man/1/scrub. [Accessed: 24- Feb- 2021].

[98] "BulkFileChanger: Change date/time/attributes of multiple files", *NirSoft*. [Online]. Available: https://www.nirsoft.net/utils/bulk_file_changer.html. [Accessed: 02- Mar- 2021].

[98] R, Russon and Y. Flede, "NTFS Documentation", Available: https://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf

[100] D. Palmbach and F. Breitinger, "Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability," Forensic Science International: Digital Investigation, vol. 32, p. 300920, Apr. 2020, doi: 10.1016/j.fsidi.2020.300920.

[101] R. Lee, "Windows 7 MFT Entry Timestamp Properties", *SANS*, April 12, 2010. [Blog]. Available: https://www.sans.org/blog/windows-7-mft-entry-timestamp-properties/, Accessed on: Mar. 4, 2021.

[102] O. Skulkin and I. Mikhaylov, "Windows 10 Time Rules – Cyber Forensicator", *Cyberforensicator.com*, 2018. [Online]. Available: https://cyberforensicator.com/2018/03/25/windows-10-time-rules/. [Accessed: 04- Mar- 2021].

[103] G. Kessler, "An overview of steganography for the computer forensics examiner", 2004 Available: https://www.garykessler.net/library/fsc_stego.html

[104] "b3dk7/StegExpose", *GitHub*. [Online]. Available: https://github.com/b3dk7/StegExpose. [Accessed: 09- Mar- 2021].

[105] A. Muñoz, "StegSecret. A simple steganalysis tool.", *Stegsecret.sourceforge.net*, 2021. [Online]. Available: http://stegsecret.sourceforge.net/. [Accessed: 09- Mar- 2021].

[106] "SpyHunter", *Spy-hunter.com*. [Online]. Available: http://www.spy-hunter.com/stegspydownload.htm. [Accessed: 09- Mar- 2021].

[107] C. Thuen, “Understanding Counter-Forensics to Ensure a Successful Investigation”, 2007. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.2196&rep=rep1&type=pdf

[108] J. Kruger and D. Dunning, “Unskilled and unaware of it: How difficulties in recognizing one’s own incompetence lead to inflated self-assessments.,” Journal of Personality and Social Psychology, vol. 77, no. 6, pp. 1121–1134, 1999, doi: 10.1037/0022-3514.77.6.1121.

[109] M. Russinovich, "Inside the Registry", *Docs.microsoft.com*, 2014. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions//cc750583(v=technet.10). [Accessed: 27- Mar- 2021].

[110] "Predefined Keys - Win32 apps", *Docs.microsoft.com*, 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/sysinfo/predefined-keys. [Accessed: 27- Mar- 2021].

[111] "USB_DEVICE_DESCRIPTOR (usbspec.h) - Windows drivers", *Docs.microsoft.com*, 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/usbspec/ns-usbspec-_usb_device_descriptor. [Accessed: 07- Apr- 2021].

[112] Y. Zhu, P. Gladyshev and J. James, "Using shellbag information to reconstruct user activities", *Digital Investigation*, vol. 6, pp. S69-S77, 2009. Available: 10.1016/j.diin.2009.06.009 [Accessed 12 Apr 2021].

[113] C. Tilbury, "OpenSaveMRU and LastVisitedMRU", *SANS*, April 2, 2010. [Blog]. Available: https://www.sans.org/blog/opensavemru-and-lastvisitedmru/, Accessed on: Apr. 14, 2021.

[114] Lifars, “Amcache and Shimcache Forensics”-When and how toleverageAmcache and Shimcache artifacts”. Available: https://lifars.com/wp-content/uploads/2017/03/Technical_tool_Amcache_Shimcache.pdf

[115] O. Skulkin, "Reconstructing User Activity for Forensics with FeatureUsage", *Group-ib.com*, 2021. [Online]. Available: https://blog.group-ib.com/featureusage. [Accessed: 15- Apr- 2021].

[116] J. Minton, "How to Employ FeatureUsage for Windows 10 Taskbar Forensics", *Crowdstrike.com*, 2020. [Online]. Available: https://www.crowdstrike.com/blog/how-to-employ-featureusage-for-windows-10-taskbar-forensics/. [Accessed: 15- Apr- 2021].

[117] S. McKeown, G. Russell and P. Leimich, "Fast Forensic Triage Using Centralised Thumbnail Caches on Windows Operating Systems", *The Journal of Digital Forensics, Security and Law*, vol. 14, 2019. Available: 10.15394/jdfsl.2019.1591 [Accessed 20 Apr 2021].

[118] "What is windows prefetch in windows 10? super-simplified", *windows ground*, 2020. [Online]. Available: https://windowsground.com/what-is-windows-prefetch-in-windows-10/. [Accessed: 21- Apr- 2021].

[119] B. Singh and U. Singh, "A forensic insight into Windows 10 Jump Lists", *Digital Investigation*, vol. 17, pp. 1-13, 2016. Available: 10.1016/j.diin.2016.02.001 [Accessed 21 Apr 2021].

[120] J. Sylve, V. Marziale and G. Richard, "Modern windows hibernation file analysis", *Digital Investigation*, vol. 20, pp. 16-22, 2017. Available: 10.1016/j.diin.2016.12.003 [Accessed 21 Apr 2021].

[121] K. Sreelakshmi and P. Sugathan, "Significance of Residual Artifacts from Random Access Memory", *International Journal of Science and Research (IJSR)*, vol. 5, no. 5, pp. 201-204, 2016. Available: 10.21275/v5i5.nov163234.

[122] C. Maartmann-Moe, S. Thorkildsen and André Årnes, "The persistence of memory: Forensic identification and extraction of cryptographic keys", *Digital Investigation*, vol. 6, pp. S132-S140, 2009. Available: 10.1016/j.diin.2009.06.002 [Accessed 24 Apr 2021].

[123] Case 1:14-cr-00068-KBF, Document 200. Available: https://storage.courtlistener.com/recap/gov.uscourts.nysd.422823.200.0.pdf

[124] S. Garfinkel, "Anti-Forensics: Techniques, Detection and Countermeasures", The 2nd International Conference on i-Warfare and Security (ICIW), Monterey, CA, March, 2007.

[125] M. C. Amirani, M. Toorani, and A. Beheshti, "A new approach to content-based file type detection," presented at the 2008 IEEE Symposium on Computers and Communications (ISCC), Jul. 2008, doi: 10.1109/iscc.2008.4625611

[126] S. Berinato, "The Rise of Anti-Forensics", *CSO Online*, 2007. [Online]. Available: https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html?page=2. [Accessed: 27- Apr- 2021].

[127] T. Brewster, "Life360 Comes At You Fast—Cops Convince Arson Suspect's Kid To Give Up Dad's Location On Family Tracking App", *Forbes*, 2020. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2020/02/12/life360-comes-at-you-fast--cops-use-family-surveillance-app-to-trace-arson-suspect/?sh=73574773380a. [Accessed: 27- Apr- 2021].

[128] N. Popper, "The Tax Sleuth Who Took Down a Drug Lord", *Nytimes.com*, 2015. [Online]. Available: https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html. [Accessed: 28- Apr- 2021].

[129] A. Kanta, I. Coisel and M. Scanlon, "A survey exploring open source Intelligence for smarter password cracking", *Forensic Science International: Digital Investigation*, vol. 35, p. 301075, 2020. doi: 10.1016/j.fsidi.2020.301075

[130] "Online Security Survey", Google / Harris Poll, 2019. Available: https://services.google.com/fh/files/blogs/google_security_infographic.pdf

[131] "The FBI's most wanted cyber-criminal used his cat's name as a password - Panda Security Mediacenter", *Panda Security Mediacenter*, 2014. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/security/fbis-wanted-cyber-criminal-used-cats-name-password/. [Accessed: 28- Apr- 2021].

[132] R.L Atkinson, R. C. Atkinson, E. E. Smith, D.J. Bem, and S. Nolen-Hoeksema, "Μνήμη," στο *Εισαγωγή στην Ψυχολογία του Hilgard*, Τόμος Α', 13th ed. Αθήνα, Ελλάδα: Παπαζήση, 2003, κεφ.8, σσ. 505-582.

[133] "Psychology of Passwords: The Online Behavior That's Putting You at Risk," LastPass, 2020. Accessed: May. 5, 2014. [Online] Available: https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf

[134] "Password security survey reveals accounts are at risk", *Specops*, April 28, 2020. [Blog]. Available: https://specopssoft.com/blog/password-security-survey-reveals-accounts-at-risk/, Accessed on: May. 5, 2021.

[135] N. Lord, "Uncovering Password Habits: Are Users' Password Security Habits Improving? (Infographic)", *Digital Guardian*, 2020. [Online]. Available: https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic. [Accessed: 05- May- 2021].

[136] S. A. McLeod, "Maslow's hierarchy of needs", *Simply Psychology*, 2020. [Online]. Available: https://www.simplypsychology.org/maslow.html. [Accessed: 23- May- 2021].

[137] M. Schwartz, "Suspected NASA Hacker Busted After Boasting About Exploits", *Bank Info Security*, October 10, 2018. [Blog]. Available: https://www.bankinfosecurity.com/blogs/suspected-nasa-hacker-busted-after-boasting-about-exploits-p-2672, Accessed on: May 23, 2021.

[138] M. Sheetz, "Meet Paige Thompson, who is accused of hacking Capital One and stealing the data of 100 million people", *cnbc.com*, 2019. [Online]. Available: https://www.cnbc.com/2019/07/30/paige-thompson-alleged-capital-one-hacker-stole-100-million-peoples-data.html. [Accessed: 23- May- 2021].

[139] "Encryption laws and policies:Human rights assessment tool", Global Partners Digital, 2020. Available: https://www.gp-digital.org/wp-content/uploads/2020/12/encryption-human-rights-assessment-tool.pdf

[140] M. Gargiulo, "Which Countries Block VPNs, and Why? | VPN.com", *VPN.com*, 2021. [Online]. Available: https://www.vpn.com/guide/which-countries-block-vpn/. [Accessed: 31- May- 2021].