Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Δικανική Υπολογιστών (Computer Forensics)

Επιμέλεια:
Καρρά Τανισκίδου Ευθυμία

Επιβλέπων:
Αντώνιος Συμβώνης

28 Αυγούστου 2014

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Σήμερα, με την ραγδαία ανάπτυξη της τεχνολογίας, ζούμε σε έναν ψηφιακό κόσμο που έχει εισβάλλει σε κάθε πτυχή της ζωής μας. Οι ηλεκτρονικοί υπολογιστές και τα κινητά τηλέφωνα έχουν καταστεί απαραίτητα εργαλεία σχεδόν σε κάθε επαγγελματική μας δραστηριότητα. Παράλληλα, η ανάπτυξη του Διαδικτύου έχει επιφέρει αλλαγές στις εργασιακές σχέσεις και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Ταυτόχρονα με τη βελτίωση της ποιότητας της ζωής μας, οι νέες τεχνολογίες και το Διαδίκτυο δημιούργησαν ιδανικές συνθήκες για την ανάπτυξη ηλεκτρονικών εγκλημάτων όπως η διακίνηση παιδικής πορνογραφίας και η αφαίρεση χρηματικών ποσών από τραπεζικούς λογαριασμούς. Διευκόλυναν όμως και τις υπόλοιπες μορφές εγκλημάτων προσφέροντας για παράδειγμα ευκολότερη μετακίνηση πληροφορίας και επικοινωνία μεταξύ των κακοποιών.

Τα εγκλήματα στον ψηφιακό κόσμο μοιάζουν με αυτά του φυσικού κόσμου. Στον φυσικό τόπο που λαμβάνει χώρα ένα έγκλημα, σχεδόν πάντα, θα έχουν μείνει ίχνη, στοιχεία, ανθρώπινο γενετικό υλικό που θα αποδεικνύουν το πώς, το γιατί και από ποιον διαπράχθηκε το έγκλημα. Αντίστοιχα ένα ψηφιακό έγκλημα αφήνει, ηλεκτρονικά αυτή τη φορά, ίχνη που μπορούν να μας οδηγήσουν στο δράστη. Εδώ υπεισέρχεται λοιπόν η επιστήμη της ανάκτησης και ανάλυσης ψηφιακών πειστηρίων ή αλλιώς ψηφιακής δικανικής (digital forensics), για να μας βοηθήσει να καταδείξουμε το δράστη και να τον οδηγήσουμε ενώπιον της δικαιοσύνης.

1.1 Ψηφιακή Δικανική

Ως ψηφιακή δικανική (digital forensics) ορίζεται:
Η χρήση επιστημονικά αποδεκτών μεθόδων που αποσκοπούν στη διατήρηση, την αναγνώριση και καταγραφή,την ανάλυση, την ερμηνεία και την παρουσίαση ψη-

φιακών πειστηρίων προερχόμενων από ψηφιακά μέσα με στόχο την ανακατασκευή-αναπαράσταση εγκληματικών ενεργειών ή την έγκαιρη πρόληψη και αντιμετώπιση μη εξουσιοδοτημένων ενεργειών οι οποίες αποτελούν κίνδυνο για σχεδιαζόμενες διαδικασίες [1].

Λέγοντας **ψηφιακά πειστήρια** εννοούμε οποιοδήποτε πληροφορία αποθηκευμένο ή μεταδιδόμενο σε δυαδική μορφή, το οποίο περιλαμβάνει αξιόπιστη πληροφορία που υποστηρίζει ή καταρρίπτει μία υπόθεση.

Λέγοντας **ψηφιακό μέσο** εννοούμε οποιαδήποτε συσκευή μπορεί να αποθηκεύσει, επεξεργαστεί,στείλει ή λάβει ψηφιακή πληροφορία. Δεν αναφέρεται μόνο με φορητούς και επιτραπέζιους υπολογιστές. Οι κινητές συσκευές, τα δίκτυα, οι βάσεις δεδομένων, τα συστήματα ”νέφους” (”cloud” systems), οι προσωπικοί ψηφιακοί βοηθοί (PDAs) και άλλες ηχητικές συσκευές και συσκευές βίντεο αποτελούν επίσης ψηφιακά μέσα και βρίσκονται και αυτά εντός του πεδίου της ψηφιακής δικανικής.

Στόχος της ψηφιακής δικανικής, είναι η διαμόρφωση μιας υπόθεσης και η αποκάλυψη ψηφιακών στοιχείων που την υποδεικνύουν ως έγκυρη ή λανθασμένη. Η διαμόρφωση υπόθεσης είναι απαραίτητη διότι τα ψηφιακά γεγονότα και καταστάσεις δεν μπορούν να εντοπιστούν άμεσα και άρα τα γεγονότα δεν είναι γνωστά. Πρέπει να χρησιμοποιηθούν εργαλεία για να προσδιοριστεί η κατάσταση των ψηφιακών δεδομένων, πράγμα που τα καθιστά έμμεσες παρατηρήσεις. Επιπλέον, άλλα χαρακτηριστικά των ψηφιακών στοιχείων είναι η ευθραυστότητα, η μεταβλητότητα και η μη απτή φύση τους που επιβάλλουν ειδική μεταχείριση. Επομένως, χρειάζεται ιδιαίτερη προσοχή στο λογισμικό και υλικό που θα χρησιμοποιηθούν για την εξαγωγή και ανάλυση ψηφιακών πειστηρίων, καθώς και στις διαδικασίες που θα ακολουθηθούν, ώστε να υπάρχει εμπιστοσύνη στην εγκυρότητά τους και να μην απορριφθούν από κάποιο πιθανό δικαστήριο.

Η ψηφιακή δικανική έχει μεγάλη ποικιλία εφαρμογών. Πρώτα από όλα εφαρμόζεται στα πλαίσια εγκληματικών ερευνών που περιλαμβάνουν ψηφιακά στοιχεία, για να επιβεβαιώσει ή να απορρίψει μια υπόθεση πριν τη δίκη. Τέτοιες έρευνες, αν και αμέσως φέρνουν στο μυαλό παιδική πορνογραφία και κλοπή ταυτότητας, δεν περιορίζονται μόνο σε τέτοιου είδους εγκλήματα. Στο σημερινό ψηφιακό κόσμο, ηλεκτρονικά αποδεικτικά στοιχεία μπορούν να βρεθούν σε οποιουδήποτε είδους εγκληματική έρευνα. Για παράδειγμα, σε μία ληστεία μπορεί να βρεθούν στοιχεία στα κινητά των κακοποιών (κλίσεις,e-mail) που να υποδεικνύουν και άλλους συνεργούς τους.

Επιπλέον, αυτός ο κλάδος της εγκληματολογίας εφαρμόζεται και σε περιπτώσεις που δεν εμπλέκεται παραβίαση της νομοθεσίας. Παραβιάσεις πολιτικών και διαδικασιών μπορεί να περιλαμβάνουν κάποιου είδους ηλεκτρονικά αποθηκευμένης πληροφορίας. Για παράδειγμα, ένας υπάλληλος, την ώρα που δουλεύει σε

μια εταιρεία, λειτουργεί και μια δεύτερη προσωπική επιχείρηση χρησιμοποιώντας τους υπολογιστές της εταιρείας. Αυτό μπορεί να μην αποτελεί παραβίαση του νόμου, όμως μπορεί να δικαιολογεί τη διεξαγωγή έρευνας από την επιχείρηση.

1.2 Μεθοδολογία Ψηφιακής Δικανικής

- **Απόκτηση (Acquisition)** είναι η συλλογή των ψηφιακών μέσων που πρόκειται να εξετασθούν. Ανάλογα με το είδος της έρευνας, αυτά μπορεί να είναι σκληροί δίσκοι, οπτικά μέσα, κάρτες αποθήκευσης από ψηφιακές φωτογραφικές μηχανές, κινητά τηλέφωνα, chips από φορητές συσκευές, ή ακόμα και μεμονωμένα αρχεία. Αφού τα μέσα αυτά συλλεχθούν, δημιουργείται ένα ακριβές αντίγραφο τους (forensic duplicate) με κατάλληλα εργαλεία υλικού ή λογισμικού και συνήθως χρησιμοποιείται και μία συσκευή write-blocking η οποία αποτρέπει τυχόν τροποποιήσεις στα αρχικά δεδομένα. Η διαδικασία αυτή συχνά ονομάζεται και imaging. Να σημειωθεί ότι οποιαδήποτε εξέταση πραγματοποιείται επί του αντιγράφου και όχι επί του πρωτότυπου πειστηρίου, έτσι ώστε να αποφευχθεί οποιαδήποτε μεταβολή στα αυθεντικά ψηφιακά δεδομένα, η οποία θα καθιστούσε την όλη έρευνα αναξιόπιστη ώστε να σταθεί ως αποδεικτικό στοιχείο σε μια δικαστική διαμάχη.

  Στη συνέχεια, το αρχικό ψηφιακό μέσο τοποθετείται σε ένα ασφαλές μέρος ώστε να αποφευχθούν αλλοιώσεις. Τέλος, για το αποκτηθέν αντίγραφο καθώς και για το αρχικό ψηφιακό μέσο, πρέπει να υπολογιστεί μία κτυπτογραφική σύνοψη (με χρήση για παράδειγμα των συναρτήσεων MD5, SHA-1 και SHA-256). Οι δύο τιμές που θα προκύψουν συγκρίνονται ώστε να πιστοποιηθεί ότι το αντίγραφο είναι ακριβές. Σε κρίσιμα σημεία της ανάλυσης, υπολογίζεται πάλι η σύνοψη του ψηφιακού μέσου έτσι ώστε να επιβεβαιωθεί ότι τα δεδομένα δεν έχουν υποστεί αλλοιώσεις.

- **Ανάλυση (Analysis)** είναι η πραγματική εξέταση του ψηφιακού μέσου. Μετά την απόκτηση, το περιεχόμενο των ψηφιακών αντιγράφων αναλύεται με σκοπό την εύρεση αποδείξεων που είτε υποστηρίζουν είτε αντικρούουν μία υπόθεση, ή στοιχείων που υποδεικνύουν αλλοιώσεις (με σκοπό την απόκρυψη δεδομένων). Το 2002, το International Journal of Digital Evidence αναφέρθηκε στο συγκεκριμένο στάδιο σαν ” μία σε βάθος συστηματική αναζήτηση στοιχείων που να σχετίζονται με το υποπτευόμενο έγκλημα”. Αντίθετα, ο Brian Carrier το 2005, περιέγραψε μία πιο διαισθη-

τική διαδικασία κατά την οποία προφανή δεδομένα προσδιορίζονται πρώτα και στη συνέχεια πραγματοποιούνται πιο διεξοδικές αναζητήσεις για να καλυφθούν τα διάφορα κενά [4].

Κατά τη διάρκεια της ανάλυσης,ένας ερευνητής συνήθως ανακτά αποδεικτικό υλικό χρησιμοποιώντας πολλές διαφορετικές μεθοδολογίες (και εργαλεία), συνήθως ξεκινώντας από τις πιο συνηθισμένες τοποθεσίες ανάλογα με το είδος της έρευνας. Για παράδειγμα, αν μελετώνται περιηγήσεις ιστού ενός χρήστη, η έρευνα ξεκινά από το ιστορικό, τους σελιδοδείκτες και την προσωρινή μνήμη του περιηγητή (web browser cache.) Οι εξεταστές χρησιμοποιούν ειδικά εργαλεία για να βοηθήσουν την προβολή και ανάκτηση δεδομένων. Το είδος των δεδομένων που ανακτάται ποικίλει ανάλογα με την έρευνα και παραδείγματα αποτελούν e-mail, logs συνομιλιών, εικόνες, ιστορικό διαδικτύου ή αρχεία κειμένου. Οι αποδείξεις μπορούν να ανακτηθούν όχι μόνο από τον προσβάσιμο χώρο ενός ψηφιακού μέσου αλλά και από τον ελεύθερο χώρο του ή από αρχεία λανθάνουσας μνήμης ενός λειτουργικού συστήματος (cache files).
Αφού ανακτηθούν τα στοιχεία, οι πληροφορίες αναλύονται με σκοπό την αναπαράσταση γεγονότων ή ενεργειών και την κατάληξη σε συμπεράσματα.

- **Παρουσίαση (presentation)** είναι η διαδικασία κατά την οποία ο εξεταστής μοιράζεται τα αποτελέσματα της ανάλυσής του με τους ενδιαφερόμενους. Αυτό περιλαμβάνει την δημιουργία αναφοράς με τα βήματα που ακολούθησε, τα στοιχεία που σύλλεξε καθώς και την ερμηνεία τους. Πολλές φορές η φάση της παρουσίασης περιλαμβάνει επίσης την υπεράσπιση των ευρημάτων από τον εξεταστή.

1.3 Κλάδοι Ψηφιακής Δικανικής

Η ψηφιακή δικανική χωρίζεται σε διάφορους κλάδους ανάλογα με το είδος της συσκευής που εμπλέκεται κάθε φορά. Οι κλάδοι αυτοί είναι η δικανική υπολογιστών, η δικανική δικτύων, η δικανική κινητών συσκευών, η δικανική βάσεων δεδομένων.

1.3.1 Δικανική δικτύων

Η δικανική δικτύων ορίζεται ως η διαδικασία ανάκτησης και ανάλυσης πληροφοριών από ένα ή περισσότερα δίκτυα υπολογιστών, για τα οποία υπάρχει η υποψία ότι εκτέθηκαν ή προσπελάστηκαν από μη εξουσιοδοτημένους χρήστες.

Οι πληροφορίες αυτές περιλαμβάνουν την κίνηση του δικτύου και τα φορτία δεδομένων. Η δικανική δικτύων επιτρέπει στους αναλυτές να επεξεργαστούν την εγκυρότητα των υποθέσεων προσπαθώντας να εξηγήσουν τις συνθήκες και τα αίτια της ενέργειας που ερευνούν και αν είναι δυνατόν να παρέχουν αποδεικτικά στοιχεία που θα υποστηρίξουν είτε ποινική είτε αστική ευθύνη.

Αν και η δικανική δικτύων χρησιμοποιείται για να προσδιορίσει το πως έγινε κάποια παραβίαση ασφάλειας, είναι απαραίτητο να ληφθούν μέτρα ώστε να ισχυροποιηθεί η ασφάλεια του δικτύου και να αποφευχθούν εισβολές. Τέτοια μέτρα αποτελούν η διαρκής ενημέρωση του λογισμικού, η ισχυροποίηση μεμονωμένων υπολογιστών, η προστασία του δικτύου (περιμετρικά) και η ενημέρωση και εκπαίδευση του προσωπικού. Πρόκληση επίσης αποτελεί η ανίχνευση συμβάντων ασφάλειας, καθώς οι σημερινές εξελιγμένες επιθέσεις μπορούν να μασκαρευτούν ώστε να δείχνουν φυσιολογικές δραστηριότητες του δικτύου. Για να εντοπιστεί πιο αποτελεσματικά ύποπτη δραστηριότητα σε ένα συγκεκριμένο δίκτυο, είναι σημαντικό να αποκτηθεί μια εικόνα για το τι αποτελεί φυσιολογική κίνηση ή δραστηριότητα στο δίκτυο αυτό, εικόνα που μπορεί να αποκτηθεί μέσα από τα logs του δικτύου. Στα πιθανά σημάδια επιθέσεων συμπεριλαμβάνονται ειδοποιήσεις του λογισμικού προστασίας από υιούς, μη φυσιολογική διαδικτυακή συνδεσιμότητα και ανωμαλίες στην δικτυακή κίνηση.

Στη συνέχεια, αξίζει να αναφερθούν οι απροσδόκητες προκλήσεις που παρουσιάζονται κατά τη διαχείριση ψηφιακών αποδεικτικών στοιχείων σε ένα δίκτυο, σε αντίθεση με την ανάκτηση στοιχείων από την επεξεργασία σκληρών δίσκων η οποία είναι μία καλά ορισμένη διαδικασία. Τα δεδομένα στα δικτυωμένα συστήματα είναι δυναμικά και ευμετάβλητα κάνοντας δύσκολη τη λήψη στιγμιότυπου στο δίκτυο για μία δεδομένη χρονική στιγμή. Επιπλέον, σε αντίθεση για παράδειγμα με τους προσωπικούς υπολογιστές, δεν είναι εφικτό να κλείσει ένα δίκτυο διότι όχι μόνο τα περισσότερα αποδεικτικά στοιχεία που περιέχονται σε αυτό θα καταστραφούν αλλά και, τις περισσότερες φορές, οι ερευνητές έχουν την ευθύνη να εξασφαλίσουν τα στοιχεία χωρίς να αποδιοργανώσουν τις επιχειρηματικές δραστηριότητες που βασίζονται στο δίκτυο.

Επιπρόσθετα, αντίθετα με τα εγκλήματα στο φυσικό περιβάλλον, τα ψηφιακά εγκλήματα μπορούν να πραγματοποιηθούν σε διαφορετικά σημεία ενός δικτύου σε οποιαδήποτε χρονική στιγμή. Επομένως αποδεικτικά στοιχεία μπορεί να είναι διεσπαρμένα σε διάφορα μηχανήματα ή συσκευές και σε διαφορετικές γεωγραφικές περιοχές, δυσκολεύοντας έτσι την απομόνωση ενός εγκλήματος. Βέβαια, ένα πλεονέκτημα που προκύπτει από αυτή τη διασπορά, είναι η δυσκολία στην καταστροφή των αποδεικτικών στοιχείων. Εάν καταστραφούν τα στοιχεία σε ένα υπολογιστικό σύστημα, συχνά μπορεί να βρεθεί ένα αντίγραφό τους σε διάφορους υπολογιστές στο διαδίκτυο.

1.3.2 Δικανική κινητών συσκευών

Η δικανική κινητών συσκευών είναι ένας κλάδος της ψηφιακής δικανικής που σχετίζεται με την ανάκτηση ψηφιακών αποδεικτικών στοιχείων ή δεδομένων από μία κινητή συσκευή. Ο όρος κινητή συσκευή δεν αναφέρεται μόνο στα κινητά τηλέφωνα αλλά σχετίζεται και με κάθε ψηφιακή συσκευή η οποία διαθέτει ταυτόχρονα εσωτερική μνήμη και δυνατότητα επικοινωνίας. Παραδείγματα αποτελούν οι συσκευές PDA, τα GPS και τα tablet.

Τα δεδομένα των κινητών συσκευών δε διαφέρουν από άλλα ψηφιακά δεδομένα με αποτέλεσμα οι βασικές αρχές διαχείρισης ψηφιακών αποδεικτικών στοιχείων να εφαρμόζονται και σε αυτόν τον κλάδο. Υπάρχουν όμως μερικές ιδιαιτερότητες που αξίζει να αναφερθούν.

Πρώτον, αν η συσκευή βρεθεί ανοικτή, πρέπει να εξασφαλισθεί ότι η θα παραμείνει συνδεδεμένη σε κάποια πηγή ενέργειας μέχρις ότου συλλεχθούν τα δεδομένα της προσωρινής της μνήμης. Σε περίπτωση που η συσκευή είναι συνδεδεμένη σε υπολογιστή θα πρέπει να αποσυνδέεται αμέσως έτσι ώστε να αποφευχθεί πιθανός συγχρονισμός ο οποίος θα μπορούσε να αντικαταστήσει δεδομένα της συσκευής.

Επίσης, είναι απαραίτητη η απομόνωση της συσκευής με χρήση, για παράδειγμα, μίας σακούλας Faraday, διότι πέρα από τον κίνδυνο της απομακρυσμένης διαγραφής δεδομένων (από τον ύποπτο), υπάρχει και η πιθανότητα διαγραφής πιθανών αποδεικτικών στοιχείων από εισερχόμενες κλήσεις, μηνύματα ή e-mails. Όμως, αν η απομόνωση γίνει με τη συσκευή ανοικτή, η μπαταρία αδειάζει πιο γρήγορα διότι η συσκευή προσπαθεί συνεχώς να συνδεθεί στο διαδίκτυο. Η NIST προτείνει να χρησιμοποιηθεί μία φορητή πηγή ενέργειας για να αντιμετωπιστεί ο κίνδυνος αυτός.

Τέλος, μία ακόμα δυσκολία που αντιμετωπίζουν οι ερευνητές είναι η τεράστια ποικιλία μοντέλων και λειτουργικών συστημάτων κινητών συσκευών που κυκλοφορεί. Κάθε μία συσκευή υποστηρίζει πολλές διαφορετικές υπηρεσίες και εφαρμογές κι επιπλέον, απαιτεί διαφορετικά καλώδια κι εξαρτήματα καθώς δεν υπάρχει ένα ενιαίο hardware διεπαφών.

1.3.3 Δικανική Βάσεων Δεδομένων

Η δικανική βάσεων δεδομένων είναι η εφαρμογή τεχνικών ανάλυσης και έρευνας υπολογιστών με σκοπό τη συλλογή αποδεικτικών στοιχείων από βάσεις δεδομένων ώστε να μπορούν να παρουσιαστούν στο δικαστήριο.

1.3.4 Δικανική Υπολογιστών

Η Δικανική Υπολογιστών (computer forensics) είναι ένας κλάδος της επιστήμης της ψηφιακής εγκληματολογίας, ο οποίος σχετίζεται με την εύρεση αποδεικτικών στοιχείων σε υπολογιστές και συνήθως εμπλέκει και άλλα ψηφιακά μέσα αποθήκευσης όπως μνήμες USB, CD-ROM, DVD-ROM και δισκέτες. Πιο συγκεκριμένα, είναι η εφαρμογή τεχνικών έρευνας και ανάλυσης με σκοπό τη συλλογή και διατήρηση δεδομένων από μία συγκεκριμένη υπολογιστική συσκευή, με τρόπο κατάλληλο για μετέπειτα παρουσίαση των στοιχείων στο δικαστήριο. Στόχος της δικανικής υπολογιστών είναι η διεξαγωγή μίας δομημένης έρευνας και η παράλληλη διατήρηση γραπτής αλυσίδας στοιχείων έτσι ώστε να προσδιοριστεί με ακρίβεια τι συνέβη σε μία υπολογιστική συσκευή καθώς και ο υπεύθυνος για το κάθε συμβάν.

Στη δικανική υπολογιστών συνήθως ακολουθείται μία συγκεκριμένη σειρά διαδικασιών: Αφού απομονώσουν τη συσκευή την οποία ερευνούν έτσι ώστε να προστατευτεί από πιθανές βλάβες, οι ερευνητές φτιάχνουν ένα ψηφιακό αντίγραφο του περιεχομένου της συσκευής η οποία στη συνέχεια κλειδώνεται σε ασφαλές μέρος έτσι ώστε να διατηρηθεί η αρχική της κατάσταση. Όλες οι έρευνες πραγματοποιούνται στο ψηφιακό αντίγραφο και όχι στα αυθεντικά δεδομένα, με χρήση ποικιλίας τεχνικών και εφαρμογών λογισμικού. Οποιοδήποτε στοιχείο βρεθεί κατά την εξέταση του αντιγράφου καταγράφεται σε μία αναφορά.

Στα κεφάλαια που ακολουθούν, θα εστιάσουμε σε θέματα που αφορούν την δικανική υπολογιστών. Αρχικά θα περιγράψουμε τις βασικές αρχές της απόκτησης ψηφιακών δεδομένων σε μία έρευνα της δικανικής υπολογιστών και στη συνέχεια θα αναπτύξουμε στοιχεία ανάλυσης αποδεικτικών στοιχείων, με έμφαση στο λειτουργικό σύστημα Windows και σε διάφορους τύπους αρχείων. Τέλος θα περιγραφούν κάποια εργαστήρια όπου θα φαίνεται πρακτικά, πώς γίνεται η αναζήτηση στοιχείων σε έναν υπολογιστή με λειτουργικό Windows.

Κεφάλαιο 2

Απόκτηση Ψηφιακών Δεδομένων

Στον κλάδο της δικανικής υπολογιστών, απόκτηση ψηφιακών δεδομένων είναι η συλλογή ψηφιακών στοιχείων από ψηφιακά μέσα αποθήκευσης. Για να συλλέξει κάθε δυνατό στοιχείο, ο ερευνητής πρέπει να λάβει ένα ακριβές αντίγραφο των ψηφιακών δεδομένων. Οποιουδήποτε είδους εξέταση θα πραγματοποιηθεί πάνω στο αντίγραφο και όχι στα πρωτότυπα στοιχεία. Υπάρχουν δύο τεχνικές απόκτησης ψηφιακών δεδομένων που θα αναλυθούν στη συνέχεια, η στατική και η ”ζωντανή”. Συνήθης τακτική, όταν ένα σύστημα βρεθεί ενεργοποιημένο, είναι πρώτα να εκτελείται μία ”ζωντανή” απόκτηση των δεδομένων που θα χαθούν με την απενεργοποίηση του συστήματος και στη συνέχεια το σύστημα να απενεργοποιείται καταλλήλως και να εκτελείται μία στατική απόκτηση των δεδομένων ολόκληρου του δίσκου.

2.1 Στατική Απόκτηση (Static Acquisition)

Η στατική απόκτηση ψηφιακών δεδομένων πραγματοποιείται σε έναν απενεργοποιημένο υπολογιστή. Αν ο υπό εξέταση υπολογιστής βρεθεί σε λειτουργία, απενεργοποιείται είτε τραβώντας από την πρίζα το καλώδιο τροφοδοσίας είτε ακολουθώντας την φυσιολογική διαδικασία απενεργοποίησης. Μετά την απενεργοποίηση, ο σκληρός δίσκος αφαιρείται από το σύστημα, συνδέεται ως εξωτερικός δίσκος σε έναν σταθμό forensic και αντιγράφονται τα περιεχόμενά του. Αντιγραφή των περιεχομένων του δίσκου ΔΕ σημαίνει απλή αντιγραφή αρχείων. Σημαίνει ότι αντιγράφεται κάθε byte του δίσκου, συμπεριλαμβανομένου του ελεύθερου χώρου (unallocated space), του χώρου slack (slack space)[1] και των μεταδεδο-

[1]Ένα αρχείο αποθηκεύεται σε μπλοκ στο δίσκο. Αν το μέγεθος του δεν είναι πολλαπλάσιο του μεγέθους των μπλοκ που καταλαμβάνει, τότε ένα μέρος του τελευταίου μπλοκ μένει αχρησιμοποί-

μένων. Τα κατάλληλα μέτρα λαμβάνονται ώστε να μην υπάρξουν τροποποιήσεις δεδομένων στον υπό εξέταση δίσκο. Ανάλογα με την κάθε περίπτωση, ο δίσκος επιστρέφεται στο αρχικό σύστημα ή παραμένει στην κατοχή του ερευνητή και φυλάσσεται ως στοιχείο.

Απενεργοποίηση

Στην επιλογή της διαδικασίας απενεργοποίησης παίζουν ρόλο οι διαδικασίες και τα προγράμματα που τρέχουν τη συγκεκριμένη στιγμή στον υπολογιστή καθώς αυτά, μετά από μία φυσιολογική απενεργοποίηση, μπορεί να σβήσουν πιθανά στοιχεία. Για παράδειγμα, προσωρινά αρχεία κειμένου μπορεί να διαγραφούν αν η εφαρμογή που τα δημιούργησε σβήσει φυσιολογικά. Επίσης, πρέπει να αναφερθεί ότι υπάρχουν προγράμματα τα οποία εκτελούνται κατά την φυσιολογική απενεργοποίηση και διαγράφουν στοιχεία χρησιμοποιώντας, για παράδειγμα, μία wipe utility.

Επιπλέον, η διαδικασία απενεργοποίησης εξαρτάται από τι είδους λειτουργικό σύστημα εκτελείται στον υπολογιστή αλλά και ποια έκδοση. Για παράδειγμα, τα περισσότερα συστήματα με Microsoft Windows μπορούν με ασφάλεια να απενεργοποιηθούν απλά τραβώντας από την πρίζα το καλώδιο τροφοδοσίας. Αντίθετα, είναι προτιμότερο να ακολουθείται η ομαλή λειτουργία απενεργοποίησης, στα συστήματα που είναι διακομιστές (servers) και εκτελούνται σε αυτά εφαρμογές βάσεων δεδομένων, οι οποίες είναι ευαίσθητες σε μη ομαλή απενεργοποίηση.

Για να αναγνωρίσει το λειτουργικό σύστημα ενός υπολογιστή, ο ερευνητής μπορεί είτε να απευθυνθεί στον διαχειριστή του συστήματος είτε να αναγνωρίσει το λειτουργικό από κάποια χαρακτηριστικά του (π.χ για Windows XP, πράσινο κουμπί εκκίνησης με το σύμβολο του Windows). Εναλλακτικά μπορεί να αλληλεπιδράσει με το σύστημα για να ποσδιορίσει τον ακιβή τύπο και έκδοση του λειτουργικού συστήματος.Στην περίπτωση αυτή όμως, η αλληλεπίδραση θα πρέπει να γίνει με πολύ μεγάλη προσοχή καταγράφοντας ακριβώς τις ενέργειες που γίνανε. Τέτοιες περιπτώσεις βέβαια είναι εξαιρετικά σπάνιες καθώς, λόγω εμπειρίας, τις πιο πολλές φορές ένα λειτουργικό σύστημα μπορεί να αναγνωριστεί αμέσως.

Αν η μέθοδος που θα ακολουθηθεί είναι η αφαίρεση της παροχής ρεύματος, θα πρέπει να βεβαιωθεί ο ερευνητής ότι δεν υπάρχει συσκευή αδιάλειπτης παροχής ενέργειας (UPS) αλλιώς θα πρέπει να διακόψει τη λειτουργία αυτής προκειμένου να σβήσει ο ηλεκτρονικός υπολογιστής ή να αφαιρεθεί το καλώδιο από το πίσω μέρος του υπολογιστή και όχι από τον τοίχο. Αυτό είναι σημαντικό, γιατί

ητο. Αυτό ονομάζεται slack ή file space και μπορεί να περιέχει υπολείμματα παλιών διεγραμμένων αρχείων.

πολλές φορές αυτές οι συσκευές συνοδεύονται από λογισμικό το οποίο κατά τη διακοπή ρεύματος αποστέλλει ειδοποιήσεις (e-mail, snmp κτλ) οι οποίες ενδεχομένως δε θέλουμε να αποσταλούν και επίσης δημιουργούν συμβάντα στο αρχείο καταγραφής του συστήματος με αποτέλεσμα αντί να διατηρούνται αναλλοίωτα τα δεδομένα του υπολογιστή, να προκαλείται η δημιουργία νέων.

Επιπλέον, όταν επιχειρείται η διακοπή παροχής ρεύματος σε έναν φορητό υπολογιστή πρέπει να αφαιρείται και η μπαταρία του η οποία συνήθως συνεχίζει να παρέχει ρεύμα στον υπολογιστή, ακόμα και αφότου το καλώδιο έχει τραβηχτεί από την πρίζα.

Τέλος όποια μέθοδος κι αν ακολουθηθεί, θα πρέπει να καταγραφούν τα βήματά της και να αιτιολογηθούν σε περίπτωση που ο ερευνητής χρειαστεί να δώσει λόγο σε ενδεχόμενη δίκη.

Περιορισμοί

Ένα βασικό πρόβλημα που αντιμετωπίζεται με την στατική απόκτηση είναι η **κρυπτογράφηση** δίσκου ή αρχείων. Στην κρυπτογράφιση δίσκου κρυπτογραφείται ολόκληρος ο δίσκος ή το περιεχόμενο ενός τόμου του δίσκου (disk volume). Όταν ο υπολογιστής απενεργοποιηθεί, ο δίσκος φαινομενικά είναι γεμάτος με τυχαία δεδομένα, αδύνατο να διαβαστούν χωρίς το κλειδί αποκρυπτογράφησης. Η κρυπτογραφία δίσκου όχι μόνο χρησιμοποιείται από κακοποιούς για να αντιμετωπιστεί η αποτελεσματικότητα της στατικής ανάλυσης αλλά είναι και προεπιλεγμένο χαρακτηριστικό κάποιων καινούριων λειτουργικών συστημάτων. Στην κρυπτογράφηση αρχείων, αντί για ολόκληρους δίσκους ή τόμους, κρυπτογραφούνται μεμονωμένα αρχεία εντός το λειτουργικό συστημάτων (π.χ ένα αρχείου σε Word ή ένας ολόκληρος φάκελος).

Στην περίπτωση ενός κρυπτογραφημένου δίσκου ή αρχείου, ακόμα κι αν ο ερευνητής έχει στη διάθεσή του ένα ακριβές αντίγραφο των bit του, αν αυτό έχει ληφθεί ενόσω ο υπολογιστής είναι απενεργοποιημένος, του είναι άχρηστο εκτός αν το αποκρυπτογραφήσει με το μοναδικό κλειδί αποκρυπτογράφησης. Επομένως ο ερευνητής, για να βρει το κλειδί αποκρυπτογράφησης, πρέπει να στηριχθεί στη συνεργασία του υπόπτου ή να χρησιμοποιήσει κάποιο εργαλείο ανάκτησης κλειδιών όπως το Password Recovery Toolkit.

Άλλο σημαντικό ζήτημα είναι ότι υπάρχουν δεδομένα σε έναν υπολογιστή σε λειτουργία, τα οποία είναι δυναμικά και προσωρινά και χάνονται με την απενεργοποίηση του υπολογιστή. Σημαντικά τέτοια δεδομένα, που μπορούν να δώσουν μία πιο πλήρη εικόνα για το πως έχει χρησιμοποιηθεί το σύστημα, είναι τα περιεχόμενα της RAM, οι δικτυακές συνδέσεις που είναι σε εξέλιξη εκείνη τη στιγμή (network connections), οι διεργασίες που εκτελούνται, οι συνδεδεμένοι χρήστες,

ανοιχτά αρχεία και κλειδιά του Registry στα πλαίσια της εκτέλεσης κάποιας διεργασίας και πολλά άλλα. Για παράδειγμα, σε μια υπόθεση όπου ο κατηγορούμενος ισχυρίζεται ότι κακόβουλο λογισμικό είναι υπεύθυνο για παράνομη δραστηριότητα στο σύστημά του (Trojan Defence), είναι σημαντικό να έχουμε πληροφορίες για ενεργές συνδέσεις και διεργασίες για να εντοπιστεί αν κάποια ασυνήθιστη διεργασία έτρεχε τη στιγμή εκείνη και αν κάποιος ήταν συνδεδεμένος στο σύστημα για να ανεβάσει αρχεία για παράδειγμα.

2.2 Ζωντανή Απόκτηση (Live Acquisition)

Για να αντιμετωπιστούν οι αδυναμίες της στατικής απόκτησης απέναντι στην κρυπτογραφία και το χάσιμο των ευμετάβλητων δεδομένων, αναπτύχθηκε η τεχνική της ζωντανής (live) απόκτησης. Η ζωντανή απόκτηση περιλαμβάνει την συλλογή δεδομένων από ένα σύστημα ενώ αυτό είναι ενεργοποιημένο. Μπορεί να πραγματοποιηθεί είτε τοπικά εκτελώντας εντολές από το πληκτρολόγιο και σώζοντας δεδομένα σε κάποιον εξωτερικό δίσκο ή σε κάποια δικτυακή πηγή (network share) είτε απομακρυσμένα με σύνδεση στο σύστημα μέσω δικτύου και εκτελώντας εντολές στο σύστημα μέσα από τη σύνδεση αυτή. Η ”ζωντανή” απόκτηση περιλαμβάνει την συλλογή πτητικών (volatile) ψηφιακών δεδομένων ή/και την απόκτηση αντιγράφου ολόκληρου του σκληρού δίσκου ενώ το σύστημα είναι σε λειτουργία.

Στην απόκτηση των πτητικών δεδομένων, πρέπει να δοθεί προσοχή στο πόσο ευμετάβλητο είναι το κάθε στοιχείο. Υπάρχουν πληροφορίες με πολύ μικρότερη διάρκεια ζωής μέσα στο σύστημα από ότι άλλες. Για παράδειγμα, ο χρόνος για συνδέσεις δικτύου που δε χρησιμοποιούνται, λήγει συχνά μέσα σε μερικά λεπτά. Κάποιες διεργασίες όπως οι υπηρεσίες (services) τρέχουν για μεγάλο διάστημα ενώ άλλες εκτελούν τις ”υποχρεώσεις” τους γρήγορα και εξαφανίζονται από τη μνήμη. Με βάση αυτές τις πληροφορίες, πρέπει να δοθεί προτεραιότητα στην απόκτηση κάποιων πτητικών δεδομένων. Για παράδειγμα, καλό είναι να λαμβάνονται πρώτα τα περιεχόμενα ολόκληρης της RAM καθώς οποιοδήποτε εργαλείο χρησιμοποιηθεί μετά για συλλογή άλλων πτητικών δεδομένων,θα φορτωθεί στη μνήμη τροποποιώντας έτσι τα περιεχόμενά της.

Επιπλέον, κατά τη διάρκεια μιας ζωντανής απόκτησης, είναι απαραίτητο να προσδιοριστεί αν ο τρέχων λογαριασμός χρήστη είναι συνδεδεμένος σε ένα πραγματικό ή εικονικό περιβάλλον [11]. Στην ουσία, και τα δύο περιβάλλοντα απαιτούν τις ίδιες τεχνικές διερεύνησης, όμως αν ο τρέχων λογαριασμός είναι συνδεδεμένος σε μία εικονική μηχανή, εκτενέστερη ανάλυση απαιτείται για να αποκτηθεί και το αντίγραφο του πραγματικού μηχανήματος καθώς και άλλα εικο-

νικά μηχανήματα που πιθανότατα βρίσκονται στο πραγματικό σύστημα. Υπάρχουν διάφορες τεχνικές για να ξεχωρίσει ένας ερευνητής αν ένα σύστημα είναι πραγματικό ή εικονικό όπως να ψάξει για ειδικούς hardware οδηγούς ή εγκατεστημένα εργαλεία. Βέβαια αυτά τα ίχνη δεν είναι ιδιαίτερα αξιόπιστα καθώς εύκολα τροποποιούνται. Πιο αξιόπιστη τεχνική αποτελεί η εγκατάσταση λογισμικού εντοπισμού εικονικών μηχανών αν και αυτό μπορεί να επιδράσει αρνητικά στην ακεραιότητα των δεδομένων.

Περιορισμοί

Οι δύο κυριότερες ανησυχίες σχετικά με την ζωντανή απόκτηση είναι η τροποποίηση δεδομένων κατά τη διάρκεια της απόκτησης και η εξάρτηση της διαδικασίας από το λειτουργικό σύστημα του υπό εξέταση υπολογιστή.

Η ζωντανή απόκτηση πραγματοποιείται με προγράμματα που εκτελούνται στο λειτουργικό σύστημα του υπό εξέταση υπολογιστή. Αν και υπάρχουν κάποια κοινά χαρακτηριστικά, οι χρήστες υπολογιστών διαμορφώνουν τα συστήματά τους με βάση τις προτιμήσεις τους. Επομένως, ένας εξεταστής θα πρέπει να γνωρίζει να χειρίζεται μια ποικιλία υλικού, λογισμικού και λειτουργικών συστημάτων. Επίσης πολλοί κακοποιοί μπορούν να ρυθμίσουν (με κατάλληλα προγράμματα) το λειτουργικό τους σύστημα ώστε να παρουσιάζει καμουφλαρισμένα δεδομένα στους ερευνητές [9]. Είναι σα να ζητάει ο ερευνητής από το ”κακό” λειτουργικό να του επιστρέψει τα αποδεικτικά στοιχεία της ενοχής του.

Επιπρόσθετα, τα δεδομένα ενός υπολογιστή μπορεί να τροποποιηθούν από οποιαδήποτε διεργασία που τρέχει κατά τη διάρκεια της απόκτησης. Ο ερευνητής, όταν βρίσκει έναν υπολογιστή ανοιχτό, δεν έχει έλεγχο πάνω στις διεργασίες που τρέχουν σε αυτόν εκείνη τη στιγμή. Αυτές μπορεί να είναι εφαρμογές χρήστη ή εξυπηρετητών και μπορούν να αλλάξουν δεδομένα κατά τη διάρκεια τη απόκτησης. Επίσης, λάθη του ερευνητή κατά την απόκτηση οδηγεί σε αλλαγές δεδομένων. Για παράδειγμα αν εκτελέσει μια εφαρμογή θα αλλάξει η χρονική στιγμή τελευταίας εκτέλεσης και άλλες λίστες πρόσφατων ενεργειών.

Επιπλέον, όταν το σύστημα αρχείων τροποποιείται κατά τη διάρκεια της απόκτησης, το αντίγραφο που θα αποκτηθεί μπορεί να παρουσιάζει μία ασαφή εικόνα των δεδομένων του συστήματος (slurred images) [9] [11]. Οποιαδήποτε τροποποίηση, αλλάζει το τμήμα των μεταδεδομένων του δίσκου το οποίο όμως διαβάζεται πρώτο κατά την απόκτηση. Αν τομείς του δίσκου, οι οποίοι αναφέρεται από τα μεταδεδομένα ότι φυλάνε αρχεία, αλλάξουν πριν αποκτηθούν, η ανάλυση θα εμπεριέχει προβλήματα καθώς μεταδεδομένα και τομείς του δίσκου δεν θα ταιριάζουν. Επίσης, λόγω των τροποποιήσεων, τιμές κατακερματισμού (hash values) του δίσκου ή των partitions που υπολογίστηκαν πριν την απόκτηση δεν μπορούν

να πιστοποιήσουν την ακεραιότητα των συλλεχθέντων δεδομένων. Κατά τη διάρκεια της απόκτησης δεδομένα τροποποιούνται επομένως η τιμή κατακερματισμού τους πριν και μετά θα διαφέρει.

Τέλος μία ζωντανή απόκτηση δεν μπορεί να επαναληφθεί δίνοντας τα ίδια ακριβώς αποτελέσματα [7]. Στην την στατική απόκτηση, αν έχει διατηρηθεί το αρχικό μέσο αποθήκευσης, επανάληψη της διαδικασίας θα επιφέρει τα ίδια αποτελέσματα. Τα δεδομένα στον δίσκο δεν αλλάζουν όσες αποκτήσεις και να πραγματοποιηθούν. Αντίθετα, εκτελώντας μία δεύτερη ζωντανή απόκτηση ενώ ο υπολογιστείς είναι σε λειτουργία θα οδηγήσει στη συλλογή νέων δεδομένων λόγω των δυναμικών αλλαγών στο λειτουργικό σύστημα.

2.3 Μέθοδοι Απόκτησης

Ανεξάρτητα με τον τύπο απόκτησης (ζωντανή ή στατική), υπάρχουν τέσσερις [7] μέθοδοι συλλογής των δεδομένων από τον σκληρό δίσκο: Αντιγραφή του δίσκου σε ένα αρχείο (disk-to-image file), αντιγραφή του δίσκου σε άλλον δίσκο (disk-to-disk copy), λογική απόκτηση (logical acquisition) και αραιή απόκτηση (sparse acquisition) .

Η πιο συνηθισμένη και ευέλικτη μέθοδος είναι η αντιγραφή του δίσκου σε ένα αρχείο **(disk-to-image)** το οποίο αποθηκεύεται σε κάποιον άλλο σκληρό δίσκο ή σε CD-ROM. Το αρχείο αυτό συχνά ονομάζεται εικόνα (image) του δίσκου και πολλά εργαλεία επιτρέπουν την διάσπαση του αρχείου εικόνας σε μικρότερα μέρη έτσι ώστε να χωράνε σε CDs ή DVDs. Στη μέθοδο αυτή, δημιουργούνται ένα ή περισσότερα sector-by-sector ακριβή αντίγραφα όλων των δυαδικών δεδομένων του δίσκου συμπεριλαμβανομένου του ελεύθερου χώρου και του slack space. Δεν θα πρέπει να υπάρχει οποιαδήποτε πληροφορία που να παρουσιάζεται στο αυθεντικό μέσο αλλά όχι στο αρχείο-εικόνα που δημιουργήθηκε! Για να διαβαστούν οι πιο κοινοί τύποι αρχείων εικόνας μπορούν να χρησιμοποιηθούν πολλά διαφορετικά εργαλεία forensics όπως τα Prodiscover, Encase, FTK, SMART, Sleuth Kit, X-Ways Forensics και ILook τα οποία διαβάζουν το αρχείο σαν να ήταν ο πραγματικός δίσκος.

Κάποιες φορές, συνήθως όταν πρόκειται για παλαιότερους δίσκους, η δημιουργία ενός αρχείου-εικόνα δεν είναι δυνατή λόγω σφαλμάτων λογισμικού ή υλικού (hardware) ή λόγω ασυμβατοτήτων [7]. Σε τέτοιες περιπτώσεις ίσως πρέπει να αντιγραφούν τα περιεχόμενα του δίσκου σε έναν άλλο δίσκο **(disk-to-disk copy)**. Με άλλα λόγια, το πρώτο sector του αυθεντικού δίσκου θα είναι πανομοιότυπο με το πρώτο sector του δίσκου-προορισμού. Στη μέθοδο αυτή, προτείνεται ο δίσκος-προορισμός να γραφτεί με μηδενικά (wipe with zeros) πριν την

αντιγραφή έτσι ώστε να μην υπάρξει μπέρδεμα με άσχετα δεδομένα, πιθανότατα από προηγούμενη έρευνα. Προβλήματα μπορεί να παρουσιαστούν όταν ο δίσκος-προορισμός είναι μεγαλύτερος από τον δίσκο-πηγή, καθώς θα είναι δύσκολο να προσδιοριστεί που ακριβώς τελειώνει το αντίγραφο του δίσκου-πηγή. Επίσης μπορεί να προκύψουν δυσκολίες αν οι δύο δίσκοι έχουν διαφορετική γεωμετρία διότι πολλές δομές δεδομένων χρησιμοποιούν γεωμετρία για να περιγράψουν τοποθεσίες.

Η συλλογή δεδομένων από ένα μεγάλο δίσκο μπορεί να διαρκέσει πολλές ώρες οπότε αν ο διαθέσιμος χρόνος είναι περιορισμένος μπορεί να χρησιμοποιηθεί μία λογική ή αραιή απόκτηση αντιγράφου δεδομένων. Η **λογική απόκτηση** συλλέγει μόνο συγκεκριμένα αρχεία ή τύπους αρχείων. Η **αραιή απόκτηση** είναι παρόμοια με την λογική αλλά επιπλέον συλλέγει τμήματα του ελεύθερου χώρου. Ένα παράδειγμα λογικής απόκτησης είναι μια υπόθεση που αφορά e-mail και στην οποία απαιτείται η συλλογή αρχείων Outlook .pst ή .ost.

Για να επιλεγεί η καταλληλότερη μέθοδος απόκτησης για μία έρευνα πρέπει να ληφθούν υπόψιν το μέγεθος του υπό εξέταση δίσκου, το αν ο δίσκος πρέπει να επιστραφεί άμεσα στον ιδιοκτήτη και πόσος χρόνος μπορεί να διατεθεί για την απόκτηση. Αν ο δίσκος πρέπει να επιστραφεί καλό είναι να χρησιμοποιηθεί ένα αξιόπιστο εργαλείο που ο ερευνητής ξέρει να χειρίζεται καλά ώστε να ληφθεί ένα πολύ καλό αντίγραφο μιας και δεν θα υπάρχει δεύτερη ευκαιρία απόκτησης των δεδομένων. Επιπλέον, αν ο δίσκος-πηγή είναι πολύ μεγάλος (π.χ 500GB ή παραπάνω) πρέπει ο ερευνητής να έχει στη διάθεσή του έναν δίσκο που να χωράει το αρχείο-εικόνα που θα δημιουργήσει. Αν δε διαθέτει τέτοιο δίσκο μπορεί να καταφύγει σε εναλλακτικές όπως η συμπίεση του αρχείου-εικόνα.

Συμπίεση Αρχείου-Εικόνα

Στην περίπτωση τα ψηφιακά δεδομένα γράφονται σε αρχείο, πολλές φορές δίνεται η δυνατότητα συμπίεσης του αρχείου ώστε να καταλαμβάνει λιγότερο χώρο. Υπάρχουν δύο μέθοδοι συμπίεσης, η συμπίεση με απώλειες και η χωρίς απώλειες (lossy και lossless compresion).

1. Η συμπίεση με απώλειες συμπιέζει τα δεδομένα ξεσκαρτάροντας μόνιμα, bits πληροφορίας του αρχείου με αποτέλεσμα μετά την αποσυμπίεση να παράγεται ένα τροποποιημένο αντίγραφο των δεδομένων. Επειδή λοιπόν αυτή η μέθοδος αλλάζει αρχικά δεδομένα, δε χρησιμοποιείται για forensics acquisitions. Αντίθετα, χρησιμοποιείται η συμπίεση χωρίς απώλειες η οποία μειώνει το μέγεθος του αρχείου χωρίς να αλλάζει δεδομένα με αποτέλεσμα, μετά την αποσυμπίεση, να παράγεται ένα ακριβές αντίγραφο των αρχικών δεδομένων.

2. Η συμπίεση χωρίς απώλειες λειτουργεί αποθηκεύοντας επαναλαμβανόμενα δεδομένα πιο αποδοτικά. Για παράδειγμα, αν τα δεδομένα έχουν 10000 συνεχόμενες μονάδες, ένας συμπιεσμένος τύπος αρχείου θα μπορούσε να το περιγράψει σε μερικά εκατοντάδες bits αντί για 10000 bits. Αν τα δεδομένα είναι τυχαία θα υπάρχει μικρή επανάληψη και η συμπίεση δε θα είναι τόσο αποδοτική. Αν συμπιεστούν δεδομένα τα οποία έχουν ήδη συμπιεστεί το αποτέλεσμα δε θα είναι ιδιαίτερα μικρότερο.

Όταν ένα μία εικόνα δίσκου είναι συμπιεσμένη, κάθε εργαλείο που χρησιμοποιείται για να την επεξεργασία της θα πρέπει να υποστηρίζει τον τύπο της συμπίεσης. Οι πιο συνηθισμένοι τύποι συμπίεσης απαιτούν την αποσυμπίεση ολόκληρου του αρχείου πριν αυτό χρησιμοποιηθεί όπως για παράδειγμα το Winzip για το Windows και το gzip για Unix. Υπάρχουν όμως και ειδικοί αλγόριθμοι συμπίεσης οι οποίοι επιτρέπουν την αποσυμπίεση του αρχείου και οι οποίοι πρέπει να χρησιμοποιούνται από κάθε εργαλείο απόκτησης ώστε να μην είναι απαραίτητη η αποσυμπίεσης ολόκληρης της εικόνας.

Τα πλεονεκτήματα της συμπίεσης είναι ότι τα περιεχόμενα ενός μέσου αποθήκευσης μπορούν να αντιγραφούν σε μικρότερο αρχείο αν και το μέγεθος του χώρου που τελικά εξοικονομείται εξαρτάται από τα αρχικά δεδομένα. Μειονεκτήματα της συμπίεσης είναι ότι ο τύπος της μπορεί να υποστηρίζεται από περιορισμένο αριθμό εργαλείων καθώς και ότι η απόκτηση και η ανάλυση μπορεί να χρειαστούν παραπάνω χρόνο καθώς απαιτούν συμπίεση και αποσυμπίεση του αρχείου αντίστοιχα.

2.4 Τύποι αρχείου-εικόνας

Στην περίπτωση που επιλεγεί ένα αρχείο για την αποθήκευση των δεδομένων που συλλέχθηκαν από κάποιο δίσκο (disk-to-image) , δίνεται η δυνατότητα επιλογής του τύπου του αρχείου αυτού. Υπάρχουν τρεις τύποι τέτοιων αρχείων.

Ακατέργαστος Τύπος (Raw format)

Τα αρχεία του τύπου αυτού, περιέχουν ένα απλό αντίγραφο sector-by-sector όλων των ανεπεξέργαστων δεδομένων του δίσκου χωρίς προσθήκες ή διαγραφές.

Τα πλεονεκτήματα του ακατέργαστου τύπου είναι οι γρήγορες μεταφορές δεδομένων και η δυνατότητα να αγνοηθούν αμελητέα σφάλματα ανάγνωσης του δίσκου. Επιπλέον τα περισσότερα εργαλεία δικανικής υπολογιστών μπορούν να το διαβάσουν.

Ένα μειονέκτημα του είναι ότι απαιτεί χώρο ίσο με το μέγεθος του δίσκου που αντιγράφεται. Άλλο πρόβλημα αποτελεί η αδυναμία του αρχείου να αποθηκεύσει μεταδεδομένα όπως για παράδειγμα ο σειριακός αριθμός του δίσκου. Βέβαια μεταδεδομένα μπορούν να αποθηκευτούν σε ξεχωριστά επιπλέον αρχεία, πρακτική όμως που ελοχεύει κινδύνους καθώς αυτά μπορεί να χαθούν ή ακόμα και να μπερδευτούν με μεταδεδομένα άλλων δίσκων.

Ιδιοκτησιακός Τύπος (Proprietary format)

Τα περισσότερα εμπορικά εργαλεία της δικανικής υπολογιστών έχουν τον δικό τους τύπο αρχείων εικόνας δίσκου και γι αυτό υπάρχουν και πολλά διαφορετικά format στην κατηγορία αυτή. Οι ιδιοκτησιακοί τύποι συνήθως παρέχουν διάφορες δυνατότητες οι οποίες δεν παρέχονται με την ακατέργαστη μορφή όπως η δυνατότητα συμπίεσης των αρχείων εικόνας του δίσκου με σκοπό την εξοικονόμηση χώρου και η δυνατότητα της ενσωμάτωσης μεταδεδομένων στο αρχείο εικόνας όπως για παράδειγμα την ημερομηνία της απόκτησης, την τιμή κατακερματισμού (hash value) του αυθεντικού δίσκου, το όνομα του εξεταστή και σχόλια ή λεπτομέρειες για την υπόθεση που ερευνάται. Ένα βασικό μειονέκτημα είναι ότι δεν είναι πάντα δυνατή η ανάλυση ενός τέτοιου αρχείου από ένα εργαλείο διαφορετικού κατασκευαστή. Για παράδειγμα, το εργαλείο IXimager παράγει τρεις ιδιοκτησιακούς τύπους - IDIF, IRBF και IEIF- που μπορούν να διαβαστούν μόνο από το εργαλείο ILook [7].

Ο πιο συχνά χρησιμοποιούμενος ιδιοκτησιακός τύπος είναι το Expert Witness Format (EWF) που συχνά καλείται και τύπος E01 λόγω της επέκτασής του (.E01). Είναι η προεπιλεγμένη επέκταση για το εργαλείο EnCase και υποστηρίζει συμπίεση, διάσπαση αρχείου-εικόνας και αποθήκευση μεταδεδομένων (συμπεριλαμβανομένου κρυπτογραφικών τιμών του αποκτηθέντος αντιγράφου) σε μια δομή επικεφαλίδας στο πρώτο τμήμα του αρχείου-εικόνας. Πολλά εργαλεία ψηφιακής δικανικής μπορούν να παράγουν και αναλύσουν EWF αρχεία, όπως το X-Ways Forensics, το FTK και το SMART.

Τύπος AFF

Το Advanced Forensic Format (AFF) είναι ένας τύπος αρχείων εικόνας δίσκου με τα παρακάτω βασικά χαρακτηριστικά:

- Δημιουργία συμπιεσμένου ή μη αρχείου.
- Δυνατότητα της αποθήκευσης της εικόνας του δίσκου δε αρχείο οποιουδήποτε μεγέθους ή της διάσπασης της σε πολλαπλά αρχεία.

- Αποθήκευση των μεταδεδομένων στο ίδιο το αρχείο ή σε ξεχωριστά αρχεία.
- Απλός σχεδιασμός και δυνατότητες επεκτασημότητας.
- Ανοιχτού κώδικα, διαθέσιμο για διάφορες πλατφόρμες και λειτουργικά συστήματα.
- Εσωτερικοί έλεγχοι συνέπειας έτσι ώστε μέρη της εικόνας μπορούν να ανακτηθούν ακόμα κι αν άλλα μέρη αλλοιωθούν.
- Επεκτασημότητα των αποθηκευμένων μεταδεδομένων - οποιαδήποτε πληροφορία για την υπόθεση μπορεί να αποθηκευτεί άμεσα στο αρχείο εικόνας.

Το AFF φαίνεται ότι στο μέλλον θα αποτελέσει το τυπική μορφή ενός forensic image οπότε σύντομα θα πρέπει να συμπεριληφθεί στα περισσότερα εμπορικά εργαλεία. Περισσότερες πληροφορίες γι αυτό υπάρχουν στις ιστοσελίδες www.afflib.org και www.basistech.com/digital-forensics/aff.html.

2.5 Εργαλεία Απόκτησης

Εδώ θα παρουσιαστούν εργαλεία δημοφιλή για τη δημιουργία αντιγράφων δίσκων. Υπάρχει πληθώρα τέτοιων εργαλείων, δωρεάν και μη, κάτι που καθιστά αδύνατη την παρουσία όλων τους.

2.5.1 dd/dcfldd

Το εργαλείο dd είναι εγκατεστημένο από προεπιλογή σχεδόν σε όλες τις διανομές Linux, διατίθεται όμως και για Windows. Είναι ένα πολύ απλό εργαλείο γραμμής εντολών αλλά παράλληλα πολύ ισχυρό και η λάθος χρήση του μπορεί πολύ εύκολα να οδηγήσει σε απώλεια δεδομένων. Δε διαθέτει χρήσιμα χαρακτηριστικά που έχουν άλλα πιο μοντέρνα εργαλεία όπως συλλογή μεταδεδομένων για το αρχείο-εικόνα που δημιουργεί και διόρθωση λαθών. Τα αρχεία-εικόνες που παράγει είναι σε ακατέργαστη μορφή (raw image file). διαγραφές.

Μία έκδοση της dd ειδικά σχεδιασμένη για χρήση στην επιστήμη της ψηφιακής δικανικής, είναι η **dcfldd**. Η βασική της λειτουργία είναι ίδια με της dd αλλά παρέχει κι επιπλέον δυνατότητες όπως ταυτόχρονο υπολογισμό τιμών κατακερματισμού των δεδομένων που αντιγράφει, μπάρα προόδου πόσων δεδομένων έχουν ήδη αντιγραφεί, πιστοποίηση ότι το αρχείο-εικόνα είναι ίδιο με τον αρχικό δίσκο, ταυτόχρονη αντιγραφή σε παραπάνω από ένα αρχεία/δίσκους και καταγραφή γεγονότων.

2.5.2 FTK Imager

Ο FTK Imager από την AccessData, είναι ένα εμπορικό (commercial) εργαλείο για απόκτηση αντιγράφων ψηφιακών δεδομένων. Οι τύποι αρχείων που υποστηρίζει είναι ο ακατέργαστος τύπος (raw), ο AFF, ο EWF και ο SMART [2]. Μπορεί να δημιουργήσει αρχεία-εικόνες σκληρών δίσκων και άλλων μέσων αποθήκευσης ή μεμονωμένων αρχείων και φακέλων. Επιτρέπει την προβολή του περιεχομένου ενός αρχείου-εικόνας όπως ακριβώς το έβλεπε και ο χρήστης, και την εξαγωγή αρχείων ή φακέλων από αυτό. Επίσης δημιουργεί τιμές κατακερματισμού για αρχεία είτε με τη συνάρτηση MD5 είτε με την SHA-1. Ο FTK Imager μπορεί να εγκατασταθεί στον υπολογιστή που θα χρησιμοποιηθεί ή μέσω κάποιας φορητής συσκευής (π.χ USB μνήμη) και άρα δεν είναι απαραίτητο να εγκατασταθεί στον υπό εξέταση υπολογιστή. Διατίθεται στην ιστοσελίδα `http://www.accessdata.com/support/product-downloads`.

2.6 Μπλοκάρισμα Εγγραφής

Κατά τη διάρκεια της απόκτησης ψηφιακών δεδομένων από ένα δίσκο, υπάρχει πιθανότητα να γραφούν δεδομένα στον αρχικό δίσκο. Αυτό θα οδηγούσε σε απόρριψη των αποδεικτικών στοιχείων από το δικαστήριο, επομένως ο ερευνητής πρέπει να λάβει μέτρα ώστε να μην τροποποιήσει τα στοιχεία. Ο πιο εύκολος τρόπος να επιτευχθεί αυτό είναι χρησιμοποιώντας write blockers.

Ένας write blocker επιτρέπει σε ένα σύστημα να διαβάζει δεδομένα από έναν δίσκο συνδεδεμένο εξωτερικά σε αυτό και ταυτόχρονα μπλοκάρει κάθε εντολή γραψίματος στον εξωτερικό αυτό δίσκο. Φυσιολογικά, ένας υπολογιστής γράφει δεδομένα ή διαβάζει δεδομένα από μια συσκευή αποθήκευσης μέσω συγκεκριμένων εντολών και μεταφέροντας τις εντολές αυτές από τη διεπαφή σύνδεσης του ίδιου του υπολογιστή, στη διεπαφή σύνδεσης της συσκευής αποθήκευσης. Χρησιμοποιώντας έναν write blocker, ο εξεταστής αποτρέπει τον υπολογιστή που εκτελεί την απόκτηση από το να γράψει δεδομένα στον υπό εξέταση σκληρό δίσκο.

Υπάρχουν δύο είδη write blocker, οι write blockers υλικού και οι λογισμικού (hardware/software write blockers). Ένας write blocker υλικού είναι μία συσκευή που παρεμβάλλεται ανάμεσα σε έναν υπολογιστή και μία εξωτερική συσκευή αποθήκευσης και φιλτράρει τις εντολές που δίνονται στη διεπαφή του μέσου

[2] Είναι ο τύπος αρχείου που παράγεται από το εργαλείο SMART που προσφέρει μια σειρά από δυνατότητες σε ερευνητές της ψηφιακής δικανικής και είναι σχεδιασμένο για Λίνουξ. Περισσότερες πληροφορίες στην `http://www.asrdata.com/forensic-software/smart-for-linux/`)

αποθήκευσης, αποτρέποντας έτσι την εγγραφή δεδομένων σε αυτό. Ένας write blocker λογισμικού αντικαθιστά τη διεπαφή πρόσβασης του υπολογιστή προς εξωτερικές συσκευές αποθήκευσης. Έτσι όταν δίνεται εντολή εγγραφής ή γραψίματος στον εξωτερικό δίσκο, αντί να εκτελεστεί ο κώδικας που θα πραγματοποιήσει την εγγραφή/γράψιμο, εκτελείτε ο κώδικας του write blocker λογισμικού ο οποίος εξετάζει την εντολή που έχει δοθεί.

Ένας άλλος τρόπος μπλοκαρίσματος εγγραφής στα αποθηκευτικά μέσα είναι η εκκίνηση του υπολογιστή μέσω CD/DVD/FLOPPY κτλ, σε ειδικά διαμορφωμένο λειτουργικό σύστημα, συνήθως Linux ή BSD ή και DOS το οποίο κατά την εκκίνηση προσαρτεί (mount) τα αποθηκευτικά μέσα μόνο προς ανάγνωση και δεν αφήνει την εγγραφή σε αυτά [7]. Φυσικά τέτοιου είδους δίσκοι θα έχουν πρώτα δοκιμαστεί στο εργαστήριο ότι όντως δεν επιτρέπουν οποιαδήποτε εγγραφή στο μέσο. Τέτοιο λειτουργικά είναι το Caine, ένα live CD βασισμένο στο Ubuntu (`http://www.caine-live.net/`).

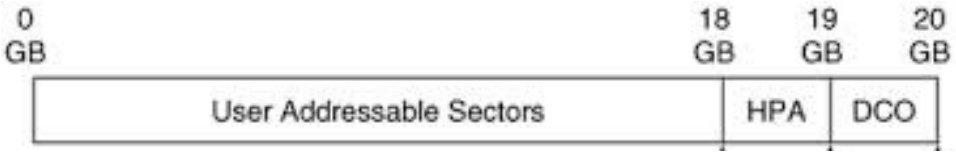
2.7 HPA και DCO

Οι HPA (Host Protected Area) και DCO (Device Configuration Overlay) είναι τμήματα στο τέλους του δίσκου που μπορούν να αποθηκεύσουν δεδομένα τα οποία όμως δεν είναι προσβάσιμα από το λειτουργικό σύστημα ή το BIOS και άρα και από το χρήστη. Αυτό τα κάνει ιδανικά για κάποιον που θέλει να κρύψει δεδομένα και άρα ο ερευνητής δεν πρέπει να παραλείπει να ψάχνει κι εκεί για δεδομένα. Όμως, αν το εργαλείο απόκτησης που χρησιμοποιεί ο ερευνητής δεν εξετάζει την ύπαρξη τμημάτων HPA/DCO, αυτά δε θα αποκτηθούν. Υπάρχουν εργαλεία απόκτησης που αυτόματα ψάχνουν για HPA/DCO και τις αποκτούν. Αν ο ερευνητής δεν έχει πρόσβαση σε ένα τέτοιο εργαλείο πρέπει να καταφύγει σε άλλες τεχνικές ανίχνευσης.

Ένας τρόπος για να εντοπιστούν τμήματα HPA/DCO είναι να συγκριθούν οι τομείς (LBA sectors) που βλέπει το BIOS με αυτούς που αναγράφει η ετικέτα πάνω στον σκληρό δίσκο. Όταν το BIOS βλέπει λιγότερους από αυτούς που αναγράφει η ετικέτα, τότε κατά πάσα πιθανότητα στο συγκεκριμένο δίσκο υπάρχει τμήμα HPA ή DCO. Αυτή η τακτική δεν είναι πάντα αξιόπιστη [8], γι αυτό ενδείκνυται ο ερευνητής να συμβουλεύεται την σελίδα του κατασκευαστή για περισσότερες τεχνικές λεπτομέριες. Αξίζει να σημειωθεί ότι σε ένα δίσκο μπορεί να συνυπάρχει χώρος HPA με DCO αρκεί το τμήμα DCO να έχει δημιουργηθεί πριν το HPA (ασχέτως αν το DCO βρίσκεται ”χωροταξικά” στο δίσκο μετά το HPA). Επίσης,τμήματα HPA και DCO ανιχνεύονται με την εφαρμογή hdparm (`http://hdparm.sourceforge.net/`) για Linux, με τις εντολές ”hdparm -N

/dev/sda" και "hdparm –dco-identify /dev/sda" αντίστοιχα, όπου sda ο υπό εξέταση δίσκος.

Αν ανιχνευθεί τμήμα HPA ή/και DCO, πρέπει να αφαιρεθεί ώστε να αποκτηθεί και αυτό το κρυμμένο κομμάτι του δίσκου. Αυτό γίνεται αλλάζοντας ρυθμίσεις του δίσκου και συγκεκριμένα θέτοντας το μέγιστο αριθμό των τομέων (sectors) που είναι ορατοί από το χρήστη, ίσο με τον πραγματικό αριθμό των τομέων που περιλαμβάνει ο δίσκος. Αυτό γίνεται με εργαλεία όπως το hdparm ή το setmax (`http://www.win.tue.nl/~aeb/linux/setmax.c`)[4].



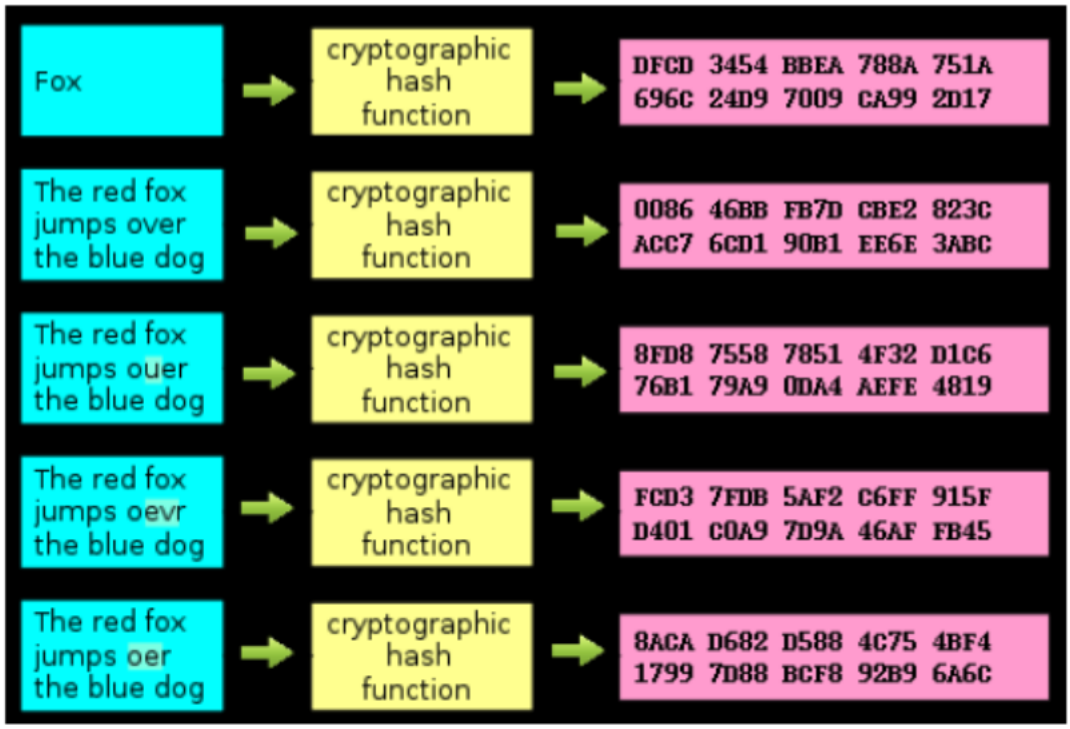
Σχήμα 2.1: Σκληρός δίσκος χωριτικότητας 20 GB με HPA 1GB και DCO 1GB

2.8 Πιστοποίηση

Ένα από τα πιο σημαντικά ζητήματα της δικανικής υπολογιστών είναι η πιστοποίηση ψηφιακών δεδομένων. Για να μπορεί μία έρευνα να ευσταθεί σε ένα δικαστήριο, θα πρέπει να αποδειχθεί ότι τα πειστήρια δεν έχουν αλλοιωθεί με οποιονδήποτε τρόπο.

Για την πιστοποίηση των δεδομένων χρησιμοποιείται μία κρυπτογραφική συνάρτηση κατακερματισμού η οποία είναι μία ντετερμινιστική διαδικασία που παίρνει ως είσοδο ένα μπλοκ δεδομένων τυχαίου μεγέθους, όπως για παράδειγμα αρχεία του δίσκου, κι επιστρέφει ένα αλφαριθμητικό ίδιου πάντα μεγέθους. Η παραμικρή μεταβολή στα αρχικά δεδομένα- ακόμα και η αλλαγή ενός γράμματος από μικρό σε κεφαλαίο- παράγει μία εντελώς διαφορετική τιμή κατακερματισμού (hash value). Στους αλγόριθμους κατακερματισμού που συχνά χρησιμοποιούνται σε μία forensic έρευνα περιλαμβάνονται οι MD5 και SHA1. Ο MD5 παράγει μία τιμή των 128 bit ενώ ο SHA1 των 160 bit. Και για τους δύο αυτούς αλγορίθμους έχουν εντοπιστεί συγκρούσεις που σημαίνει ότι δύο διαφορετικά μπλοκ δεδομένων έχουν την ίδια τιμή κατακερματισμού. Αυτό στη συγκεκριμένη περίπτωση δεν αποτελεί ιδιαίτερο πρόβλημα καθώς αν υπάρχει υποψία σύγκρουσης, μπορεί να γίνε μία σύγκριση byte-by-byte για να επιβεβαιωθεί ότι όλα τα bytes είναι ίδια. Τέτοιες συγκρίσεις γίνονται με την MS-DOS Comp εντολή ή την Linux/Unix diff εντολή.

Είναι φανερό λοιπόν από τις ιδιότητες των συναρτήσεων κατακερματισμού, το πως αυτές χρησιμοποιούνται στη δικανική υπολογιστών για την πιστοποίηση ψηφιακών δεδομένων. Δημιουργείται μία τιμή κατακερματισμού για τα αρχικά δεδομένα η οποία στη συνέχεια συγκρίνεται με την τιμή για το forensic αντίγραφο τους. Αν οι τιμές είναι ίδιες σημαίνει ότι δεν υπάρχει κάποια αλλοίωση στα δεδομένα. Επιπρόσθετα, υπολογίζοντας μία τιμή κατακερματισμού μετά την ολοκλήρωση της εξέτασης του foensic αντιγράφου, μπορεί να αποδειχθεί ότι ο εξεταστής δεν τροποποίησε δεδομένα. Άλλη χρήση μιας συνάρτησης κατακερματισμού είναι ο εντοπισμός γνωστών αρχείων που μπορούν να εξαιρεθούν από την έρευνα όπως για παράδειγμα αρχεία του λειτουργικού συστήματος και κοινά προγράμματα (π.χ Microsoft Word) ή ο εντοπισμός παράνομων αρχείων που ”κρύβονται” αλλάζοντας το όνομά τους. Η National Software Reference Library (NSRL) έχει δημιουργήσει μία λίστα από τιμές κατακερματισμού για διάφορα αρχεία λειτουργικών συστημάτων και εφαρμογές που μπορεί να βρεθεί στη διεύθυνση www.nsrl.nist.gov.



Σχήμα 2.2: Μικρή αλλαγή στην είσοδο της συνάρτησης κατακερματισμού επιφέρει τεράστια αλλαγή στην τιμή κατακερματισμού.

Κεφάλαιο 3

Στοιχεία Ανάλυσης

Κατά τη διάρκεια της ανάλυσης του αντιγράφου μιας συσκευής αποθήκευσης ο ερευνητής καλείται να προσδιορίσει πιθανές πηγές πληροφοριών (όπως ενεργά ή σβησμένα αρχεία), να τις εξάγει από το αντίγραφο και να τις ερμηνεύσει. Για να το επιτύχει αυτό θα πρέπει να γνωρίζει πως λειτουργούν τα λειτουργικά συστήματα που χρησιμοποιούνται πιο συχνά καθώς και πώς αποθηκεύουν τα αρχεία τους, το οποίο καθορίζεται από το σύστημα αρχείων (file system) που χρησιμοποιούν. Επιπλέον απαραίτητη γνώση αποτελεί η φύση των αρχείων που εξάγει και επεξεργάζεται ώστε να εκμεταλλευτεί κάθε δυνατή πληροφορία που βρίσκεται σ αυτά.

3.1 Windows artifacts

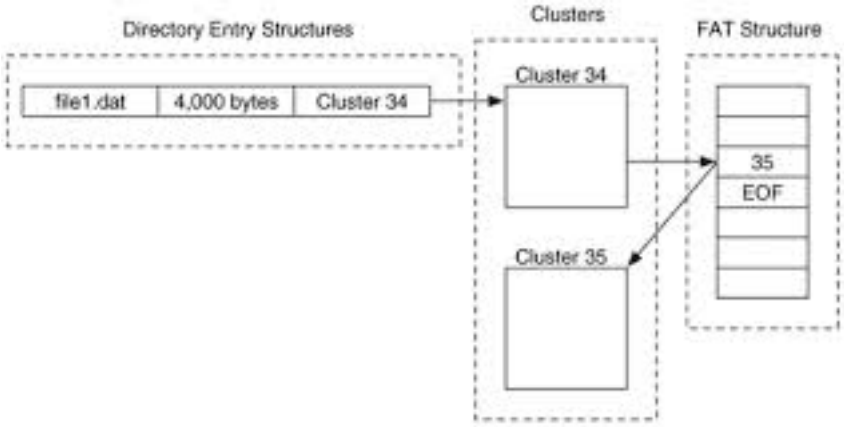
3.1.1 Συστήματα Αρχείων

FAT

Το FAT (File Allocation Table) σύστημα αρχείων (file system) είναι από τα πιο απλά συστήματα που συναντάται στα συνηθισμένα λειτουργικά συστήματα και είναι το κύριο σύστημα αρχείων των Microsoft DOS και Windows 9x. Το FAT υποστηρίζεται από όλα τα Windows και από τα περισσότερα Unix λειτουργικά συστήματα και θα συναντάται από ερευνητές για χρόνια ακόμα, παρ' όλο που δεν είναι η προεπιλογή των υπολογιστών με Windows. Συνήθως χρησιμοποιείται σε USB μνήμες και σε κάρτες μνήμης ψηφιακών φωτογραφικών μηχανών. Το FAT βγαίνει σε τέσσερις διαφορετικές εκδόσεις: FAT12, FAT16, FAT32 και exFAT.

Η βασική ιδέα ενός συστήματος αρχείων FAT είναι ότι για κάθε αρχείο και κατάλογο (directory), εκχωρείται μία δομή δεδομένων που καλείται εγγραφή κα-

ταλόγου (directory entry) η οποία περιλαμβάνει το όνομα του αρχείου, το μέγεθος και άλλα μεταδεδομένα. Τα περιεχόμενα των αρχείων και των καταλόγων αποθηκεύονται σε μονάδες δεδομένων (data units)[1] που για το σύστημα FAT ονομάζονται συστάδες (clusters). Η συστάδα απ την οποία ξεκινάει το περιεχόμενο του αρχείου ή καταλόγου καταγράφεται στην εγγραφή καταλόγου του. Αν το αρχείο καταλαμβάνει παραπάνω από μία συστάδες, οι υπόλοιπες συστάδες προσδιορίζονται μέσω μιας δομής που καλείται FAT. Η δομή FAT χρησιμοποιείται για τον εντοπισμό της επόμενης συστάδας ενός αρχείου αλλά και για τον προσδιορισμό του αν είναι κατανεμημένη σε κάποιο αρχείο ή όχι (allocation status). Η βασική διαφορά των εκδόσεων του FAT που αναφέρθηκαν παραπάνω είναι το μέγεθος των εγγραφών στην FAT δομή.



Σχήμα 3.1: Σχέση FAT δομής με εγγραφή καταλόγου και με συστάδες

Η διάταξη (layout) του συστήματος αρχείων FAT περιλαμβάνει τρία βασικά μέρη που φαίνονται στο σχήμα 3.2.

Το πρώτο μέρος, που ξεκινάει στον τομέα (sector) 0 του δίσκου, είναι η reserved περιοχή όπου βρίσκεται ο τομέας εκκίνησης (boot sector). Ο τομέας εκκίνησης είναι πάντα στον τομέα 0, περιέχει γενικές πληροφορίες για το ίδιο το σύστημα αρχείων και καθορίζει το μέγεθος της reserved περιοχής. Στις εκδόσεις FAT12/16 η reserved περιοχή καταλαμβάνει μόνο τον τομέα 0, ενώ στην FAT32 συνήθως και επιπλέον τομείς που περιέχουν ένα αντίγραφο ασφαλείας του τομέα εκκίνησης και τη δομή δεδομένων FSINFO που έχει πληροφορίες για την τοποθεσία της αμέσως επόμενης ελεύθερης συστάδας και για τον συνολικό αριθμό ελεύθερων συστάδων .

[1] Τα δεδομένα στον δίσκο χωρίζονται σε τομείς (sectors) συνήθως των 512 bytes. Μονάδα δεδομένων (data unit) είναι ένα σύνολο συνεχόμενων τομέων του δίσκου. Για λόγους απόδοσης στα αρχεία δεν κατανέμονται ξεχωριστοί τομείς αλλά μονάδες δεδομένων.

Σχήμα 3.2: Διάταξη ενός FAT συστήματος αρχείων

Το δεύτερο μέρος είναι η περιοχή FAT που ξεκινά στον τομέα αμέσως μετά την reserved περιοχή και περιέχει μία ή περισσότερες δομές FAT (αντίγραφα ασφαλείας της πρώτης δομής FAT). Το μέγεθος της βρίσκεται πολλαπλασιάζοντας το πλήθος των δομών FAT με το μέγεθος τους, τιμές που υπάρχουν στον τομέα εκκίνησης.

Το τρίτο μέρος είναι η περιοχή δεδομένων (data area) και περιέχει τις συστάδες όπου αποθηκεύονται περιεχόμενα αρχείων και καταλόγων. Διασκορπισμένες στην περιοχή δεδομένων βρίσκονται και οι εγγραφές καταλόγου των αρχείων και καταλόγων.

Κρυμμένα δεδομένα

Υπάρχουν πολλά μέρη που δεν χρησιμοποιούνται από το σύστημα αρχείων και μπορεί να περιέχουν δεδομένα κρυμμένα από το χρήστη. Για παράδειγμα, υπάρχουν πάνω από 450 bytes ανάμεσα στο τέλος των δεδομένων του τομέα εκκίνησης που βρίσκεται στον τομέα 0 και το τέλος του τομέα 0 [4]. Το Windows συνήθως αξιοποιεί το χώρο αυτό βάζοντας κώδικα εκκίνησης του συστήματος αλλά αυτό δεν είναι απαραίτητο για συστήματα αρχείων χωρίς δυνατότητες εκκίνησης (non-bootable). Επίσης τα FAT32 κατανέμουν πολλούς τομείς για την reserved περιοχή αλλά μόνο λίγοι χρησιμοποιούνται για τον τομέα εκκίνησης, το αντίγραφο ασφαλείας του και την δομή FSINFO. Επομένως οι υπόλοιποι μπορούν να έχουν κρυμμένα δεδομένα.

Κρυμμένα δεδομένα μπορεί να υπάρχουν και μεταξύ του τέλους του συστήματος αρχείων και το τέλος του τόμου του δίσκου (disk volume)[2] όπου βρίσκεται το σύστημα αρχείων. Το κενό αυτό λέγεται volume slack και υπολογίζεται συγκρίνοντας τον αριθμών των τομέων του συστήματος αρχείων (υπάρχει στον τομέα εκκίνησης) με τον αριθμών των τομέων του του τόμου του δίσκου. Να σημειωθεί ότι εύκολη η δημιουργία volume slack αφού απαιτείται μόνο η αλλαγή της τιμής του αριθμού των συνολικών τομέων, που βρίσκεται στον τομέα εκκίνησης.

[2]Τόμος δίσκου (volume) είναι ένας αριθμός τομέων (sectors) του δίσκου (όχι απαραίτητα συνεχόμενων στο δίσκο) που μπορούν να χρησιμοποιηθούν για αποθήκευση δεδομένων. Τα συστήματα αρχείων βρίσκονται πάνω σε τόμους.

Επιπλέον, το μέγεθος της περιοχής δεδομένων μπορεί να μην είναι πολλαπλάσιο του μεγέθους συστάδας του συστήματος αρχείων και άρα μπορεί να υπάρχουν μερικοί τόμοι στο τέλος της περιοχής δεδομένων που δεν αποτελούν μέρος κάποιας συστάδας. Αυτά χρησιμοποιούνται για κρυμμένα δεδομένα ή μπορεί να περιέχουν δεδομένα από προηγούμενα συστήματα αρχείων. Δεδομένα μπορούν να κρυφτούν και ανάμεσα στο τέλος της τελευταίας έγκυρης εγγραφής της κύριας δομής FAT και της αρχής του αντιγράφου ασφαλείας της δομής και μεταξύ της τελευταίας εγγραφής του αντιγράφου και της αρχής της περιοχής δεδομένων.

NTFS

Το NTFS (New Technologies File System) σχεδιάστηκε από την Microsoft και είναι το προεπιλεγμένο λειτουργικό σύστημα για Windows NT,2000, XP και νεότερες εκδόσεις. Το FAT θα συνεχίσει να υπάρχει σε μικρές συσκευές αποθήκευσης αλλά το NTFS θα είναι πιθανότατα το πιο συνηθισμένο σύστημα αρχείων για έρευνες σε συστήματα με Windows. Το NTFS είναι πολύ πιο πολύπλοκο από το FAT διότι έχει πολλά χαρακτηριστικά και δυνατότητες κλιμάκωσης.

Το βασικότερο χαρακτηριστικό του NTFS είναι ότι τα πάντα στο σύστημα είναι αρχεία, ακόμα και δεδομένα συστήματος και διαχείρισης! Δεν υπάρχει η ανάγκη φύλαξης συγκεκριμένων διευθύνσεων στο δίσκο για ειδικού τύπου δεδομένα όπως πίνακες εκχώρησης αρχείων (file allocation tables) αφού αυτά αποθηκεύονται σε συνηθισμένα αρχεία που μπορεί να βρίσκονται οπουδήποτε στο δίσκο.

Από αυτό το χαρακτηριστικό φαίνεται και η κυριότερη διαφορά του NTFS με το FAT. Αντίθετα με το FAT που έχει τρεις βασικές περιοχές στις ίδιες θέσεις κάθε φορά, το NTFS δεν έχει μία συγκεκριμένη διάταξη συνδεδεμένη με σταθερές διευθύνσεις του δίσκου. Όλο το σύστημα αρχείων θεωρείται μία περιοχή δεδομένων, οπότε κάθε αρχείο μπορεί να βρίσκεται οπουδήποτε στο δίσκο. Το μόνο σταθερό στοιχείο του NTFS, είναι ότι ο τομέας εκκίνησης και ο κώδικας εκκίνησης περιέχονται πάντα στους πρώτους τομείς.

MFT

Το MFT (Master File Table) είναι η βάση του NTFS καθώς περιέχει πληροφορίες για κάθε αρχείο και κατάλογο. Η τοποθεσία της αρχής του MFT είναι καταγεγραμμένη στον τομέα εκκίνησης και κάθε αρχείο και κατάλογος του NTFS έχει μια εγγραφή στο MFT. Κάθε εγγραφή έχει μήκος 1024 bytes, και περιέχει ένα σύνολο γνωρισμάτων που φυλάνε μεταδεδομένα για το αντίστοιχο αρχείο ή, καμιά φορά, το ίδιο το περιεχόμενο των αρχείων.

Τα πρώτα 42 bytes κάθε MFT εγγραφής αποτελούν την επικεφαλίδα της η οποία δίνει πληροφορίες μεταξύ άλλων, και για τον αριθμό των καταλόγων που έχουν εγγραφές για το συγκεκριμένο αρχείο (έτσι υπολογίζονται τα hard links [3]), για το αν η εγγραφή είναι αρχείου ή καταλόγου, για το αν το αρχείο ή ο κατάλογος έχει διαγραφεί. Μετά την επικεφαλίδα της MFT εγγραφής, ακολουθούν διάφορα γνωρίσματα. Θα επικεντρωθούμε στα γνωρίσματα **$ STANDARD _ INFOMATION ($SIA)** και **$FILE _ NAME ($FNA)** που υπάρχουν σε κάθε MFT εγγραφή, διότι περιέχουν χρονική πληροφορία που είναι πολύ σημαντική για μία έρευνα.

Το **$SIA** περιλαμβάνει (μεταξύ άλλων) ένα σύνολο χρονικών σημάνσεων (timestamps) οι οποίες είναι FILETIME αντικείμενα των 64 bit που αναπαριστούν τον αριθμό των διαστημάτων των 100 nanosecond που μεσολαβούν από την πρώτη Ιανουαρίου 1601. Τα timestamps αυτά είναι γραμμένα στην MFT εγγραφή σε UTC και περιλαμβάνουν:

- Χρονική στιγμή τελευταίας τροποποίησης (last modification time)
- Χρονική στιγμή τελευταίας πρόσβασης (last accessed time)
- Χρονική στιγμή τροποποίησης της MFT εγγραφής
- Χρονική στιγμή δημιουργίας (”γέννησης”) (last creation time).

Όλοι μαζί αναφέρονται ως χρόνοι ”MACB” και είναι οι χρόνοι που βλέπουμε με την εντολή dir της γραμμής εντολών ή μέσω του εξερευνητή του Windows (Windows Explorer). Οι χρόνοι αυτοί τροποποιούνται κατά τη διάρκεια φυσιολογικής δραστηριότητας του συστήματος. Όταν ένα αρχείο δημιουργείται, όλοι οι χρόνοι παίρνουν την τιμή της συγκεκριμένης ημερομηνίας και ώρας. Όταν γίνεται οποιαδήποτε αλλαγή στο αρχείο (προσθήκες, τροποποιήσεις ή αφαιρέσεις δεδομένων) η χρονική στιγμή τελευταίας τροποποίησης ενημερώνεται.

Όμως και άλλες ενέργειες του χρήστη (πέρα από το απλό γράψιμο ή διάβασμα) επηρεάζουν τους χρόνους του $SIA γνωρίσματος [3]. Για παράδειγμα, η αντιγραφή ή η μετακίνηση ενός αρχείου μέσα στο ίδιο διαμέρισμα (partition) του δίσκου διατηρεί τη χρονική στιγμή τελευταίας τροποποίησης αλλά, η αντιγραφή μετατρέπει την ημερομηνία δημιουργίας του αντιγράφου του αρχείου στην τρέχουσα ημερομηνία, ενώ η μετακίνηση διατηρεί την ημερομηνία του αρχικού αρχείου. Παράγοντες που επηρεάζουν αυτούς τους χρόνους περιγράφονται στο KnowledgeBase άρθρο της Microsoft `http://support.microsoft.com/kb/299648`.

[3] hard link είναι ένα αρχείο που αναπαριστά ένα άλλο αρχείο χωρίς στην πραγματικότητα να το διπλασιάζει. Χρησιμοποιεί την ίδια εγγραφή MFT με το πραγματικό αρχείο

Προσοχή!
Η πραγματική χρονική στιγμή τελευταίας πρόσβασης ενός αρχείου δεν είναι πάντα αυτή που αναγράφεται[3]! Παρ' όλα αυτά, οι πιο πολλοί αναλυτές πιστεύουν (λανθασμένα) ότι όταν ένα αρχείο ανοίγεται ή αποκτάται πρόσβαση σε αυτό με κάποιον άλλο τρόπο, η χρονική στιγμή τελευταίας πρόσβασης του τροποποιείται αμέσως ώστε να περιέχει τον κατάλληλο χρόνο. Το NTFS αργεί να κάνε την ανανέωση για λόγους απόδοσης. Διατηρεί τον σωστό χρόνο στη μνήμη και ανανεώσει το χρόνο στο δίσκο, όταν διαφέρει από αυτόν στην μνήμη κατά μία ώρα. Επίσης υπάρχει μία τιμή (value) του Registry (HKLM \CurrentControlSet \Control \FileSystem \NtfsDisableLastAccessUpdate) που αν πάρει τιμή ένα, απενεργοποιεί την ανανέωση του χρόνου τελευταίας πρόσβασης.

Το **$FNA** περιλαμβάνει (μεταξύ άλλων) τέσσερις σημάνσεις χρόνου, παρόμοια και της ίδιας μορφής με αυτά του $SIA. Η κυριότερη διαφορά τους είναι ότι το Windows δεν ενημερώνει τις τιμές τους με τον ίδιο τρόπο και συνήθως αντιστοιχούν στο πότε ΠΡΑΓΜΑΤΙΚΑ το αρχείο δημιουργήθηκε, μετακινήθηκε ή μετονομάστηκε. Επομένως, η επεξεργασία των MFT εγγραφών και η παρατήρηση ανωμαλιών μεταξύ των timestamps των γνωρισμάτων $SIA και $FNA, είναι μία τεχνική που χρησιμοποιούν οι αναλυτές ώστε να προσδιορίσουν εσκεμμένες τροποποιήσεις των timestamps του $SIA με σκοπό το "μασκάρεμα" αρχείων.

Εργαλεία

Υπάρχουν διάφορα εργαλεία για την επεξεργασία του MFT και άρα και την εξαγωγή των γνωρισμάτων $SIA και $FNA. Ένα από αυτά είναι το **analyzeMFT.py**, ένα script σε Python από τον David Kovar που διατίθεται στην ιστοσελίδα `https://github.com/dkovar/analyzeMFT` και λειτουργεί και σε Windows και σε Linux. Άλλο εργαλείο είναι το mft_ parser που διατίθεται για Windows στην ιστοσελίδα `http://redwolfcomputerforensics.com/index.php?option=com_content&task\=view&id=42&Itemid=55`.

Alternate Data Streams (ADS)

Τα ADS, ένα χαρακτηριστικό του NTFS συστήματος αρχείων, είναι μία επιπλέον σειρά (stream) δεδομένων σχετιζόμενη με κάποιο αρχείο. Με την εντολή dir /r του Windows μπορούν να προβληθούν τέτοιες σειρές δεδομένων σε ένα σύστημα σε λειτουργία. Τα ADS μπορούν να χρησιμοποιηθούν για κρύψιμο εκτε-

λέσιμου κώδικα ο οποίος μπορεί να τρέξει από εκεί αλλά και για κρύψιμο άλλων αρχείων όπως εικόνες! Πολλά εμπορικά εργαλεία με γραφικό περιβάλλον παρουσιάζουν τα ADSs με κόκκινο χρώμα.

3.1.2 Registry

Το Registry του Windows είναι μία κεντρική ιεραρχική βάση δεδομένων η οποία περιλαμβάνει απαραίτητες πληροφορίες για ρυθμίσεις παραμέτρων του συστήματος (system configuration) για έναν ή περισσότερους χρήστες, για εφαρμογές και συσκευές υλικού. Συνοπτικά, το Registry είναι μία δυαδική δομή δεδομένων με σκοπό να αντικαταστήσει τα αρχεία ρυθμίσεων και τα .ini αρχεία που χρησιμοποιούνταν από παλαιότερες εκδόσεις του Windows. Οι περισσότεροι χρήστες και διαχειριστές δεν αλληλεπιδρούν άμεσα με το Registry αλλά αντίθετα μέσα από εγκαταστάσεις εφαρμογών οι οποίες από μόνες τους τροποποιούν καταλλήλως το Registry χωρίς ο ίδιος ο χρήστης να αντιλαμβάνεται αυτές τις διαδικασίες ή χρησιμοποιώντας κάποιου είδους γραφικό περιβάλλον όπως ο Registry Editor. Ο Registry editor διανέμεται με τις περισσότερες εκδόσεις του Windows και παρουσιάζει το Registry σαν μία δομή από φακέλους η οποία είναι εύκολη και φιλική προς τον χρήστη.

Στην πραγματικότητα όμως το Registry δεν είναι ένα σύνολο φακέλων όπως παρουσιάζεται για ευκολία σε γραφικά περιβάλλοντα όπως ο Registry Editor. Αντίθεττα, το Registry αποτελείται από ένα σύνολο αρχείων αποθηκευμένων στο σκληρό δίσκο τα οποία ονομάζονται ”hive” αρχεία και μέσω αυτών των αρχείων αλληλεπιδρά ο αναλυτής με το Registry τις περισσότερες φορές. Τα hive αρχεία που περιλαμβάνουν ρυθμίσεις παραμέτρων του συστήματος όπως έκδοση και ρυθμίσεις του λειτουργικού συστήματος, πληροφορίες λογαριασμών χρηστών και εγκατεστημένο λογισμικό, ονομάζονται SAM, Security, Software και System και βρίσκονται στο φάκελο Windows\System32 \config. Για τις εκδόσεις από Window Vista και μετά, υπάρχει άλλο ένα hive αρχείο στο φάκελο αυτό που ονομάζεται ”Components” το οποίο δε φαίνεται να έχει ιδιαίτερη σημασία από μία forensics οπτική γωνία (τουλάχιστον για την ώρα).

Πληροφορίες ξεχωριστά για τον κάθε χρήστη διατηρούνται στο NTUSER.dat hive αρχείο που βρίσκεται στο προφίλ του κάθε χρήστη. Στο Windows 2000, XP και 2003 τα προφίλ των χρηστών βρίσκονται στον φάκελο Documents and Settings στον root φάκελο του συστήματος ενώ για Vista και νεότερες εκδόσεις βρίσκονται στον φάκελο Users του root. Υπάρχει επίσης ένα άλλο hive αρχείο χρήστη το οποίο συγχωνεύεται με το NTUSER.dat όταν ένας χρήστης συνδέεται, επιτρέποντας μία ενοποιημένη παρουσίαση των πληροφοριών και των δύο hive χρήστη. Αυτό το hive αρχείο ονομάζεται USRCLASS.dat και βρίσκε-

ται, για Windows 2000, XP και 2003 στο προφίλ του χρήστη στο φάκελο Local Settings\Application Data \Microsoft \Windows, και για Vista και νεότερες εκδόσεις στο προφίλ του χρήστη στο φάκελο AppData\Local \Microsoft \Windows.

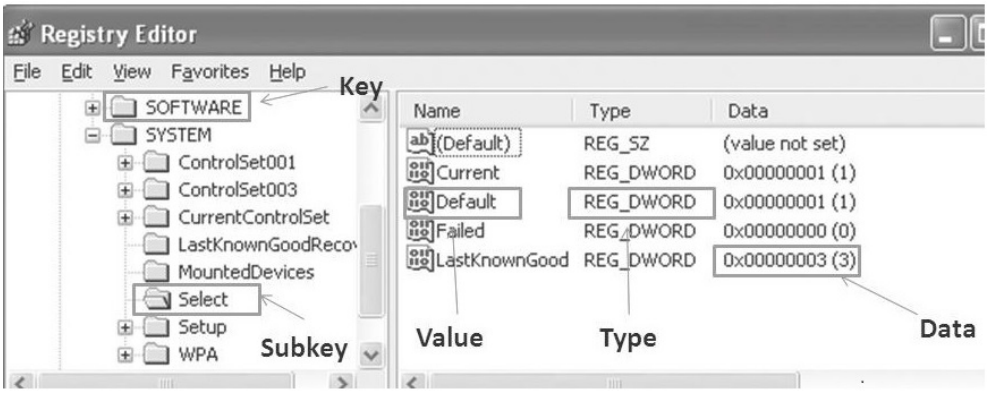
Η δυαδική δομή του Registry αποτελείται από δύο βασικά στοιχεία, τα κλειδιά (keys) και τις τιμές (values). Τα κλειδιά του Registry μοιάζουν με φακέλους καθώς δείχνουν ή περιέχουν επιπλέον κλειδιά που λέγονται υποκλειδιά (subkeys) καθώς και τιμές (values). Επιπλέον τα κλειδιά περιέχουν πολύ χρήσιμη πληροφορία για μία έρευνα καθώς η δομή τους περιλαμβάνει τη χρονική στιγμή LastWrite που είναι ένα FILETIME αντικείμενο των 64 bit [2]. Είναι ανάλογο της χρονική στιγμής της τελευταίας τροποποίησης ενός αρχείου (last modification time) και δείχνει πότε έγινε κάποια αλλαγή στο αντίστοιχο κλειδί. Στις αλλαγές περιλαμβάνονται η δημιουργία ή διαγραφή υποκλειδιών ή τιμών ή η τροποποίηση κάποιας τιμής.

Οι τιμές είναι ζευγάρια ονόματος-δεδομένων και μοιάζουν περισσότερο με αρχεία καθώς δεν περιέχουν άλλα κλειδιά. Η σημαντικότερη διαφορά τους από τα κλειδιά είναι ότι δεν περιέχουν πληροφορία timestamp όπως το LastWrite των κλειδιών. Παρ' όλα αυτά, οι τιμές είναι σημαντικές καθώς στα δεδομένα τους περιλαμβάνονται όλες οι πληροφορίες για τις ρυθμίσεις των παραμέτρων (configuration settings) του λειτουργικού συστήματος και των διαφόρων εφαρμογών οι οποίες είναι αποθηκευμένες στο Registry.

Στο σχήμα 3.1 φαίνονται τα στοιχεία του Registry όπως οπτικοποιούνται από τον Registry editor. Στο αριστερό τμήμα το editor βλέπουμε τα κλειδιά και υποκλειδιά που αναπαρίστανται σαν φάκελοι. Όταν επιλέξουμε με το ποντίκι κάποιο κλειδί, θα δούμε κάτι παρόμοιο με αυτό που παρουσιάζεται στο δεξί τμήμα και το οποίο αναπαριστά τις τιμές του Registry (values) και τα δεδομένα που αυτές περιλαμβάνουν. Δεν πρέπει όμως να ξεχνάμε ότι όλες αυτές οι πληροφορίες στην πραγματικότητα περιλαμβάνονται σε αρχεία μέσα στο σύστημα αρχείων (file system).

Από τη σκοπιά του ερευνητή

Όπως ήδη αναφέρθηκε, το Registry περιλαμβάνει πληροφορίες για τις ρυθμίσεις του συστήματος το οποίο για έναν forensic αναλυτή σημαίνει ότι περιλαμβάνει πληροφορίες που υποδεικνύουν στο λειτουργικό σύστημα και σε εφαρμογές τι να κάνουν, που να τοποθετήσουν "πράγματα" και πως να αντιδράσουν σε διάφορα ερεθίσματα. Για παράδειγμα, μία τιμή του Registry υποδεικνύει στο λειτουργικό σύστημα να αδειάσει το page file όταν το σύστημα απενεργοποιείται ενώ μία άλλη τιμή απενεργοποιεί την ανανέωση των χρόνων τελευταίας πρόσβασης (last acceess times) του συστήματος αρχείων[2]. Στη συνέχεια αναφέρονται



Σχήμα 3.3: Οπτικοποίηση κλειδιών και τιμών του Registry μέσω Registry Editor

ενδεικτικά σημαντικά δεδομένα που μπορεί να αντλήσει ένας ερευνητής από το Registry.

Στο System hive βρίσκονται πληροφορίες για ρυθμίσεις διάφορων παραμέτρων του συστήματος. Αποθηκεύονται στοιχεία για τα Windows services που είναι προγράμματα τα οποία τρέχουν αυτόματα όταν το σύστημα εκκινεί και ξεκινάνε από το ίδιο το σύστημα χωρίς να απαιτείται αλληλεπίδραση με το χρήστη. Λόγω της φύσης τους αποτελούν συνηθισμένο στόχο για κακόβουλο λογισμικό το οποίο τα χρησιμοποιεί κυρίως για να διατηρηθεί στο σύστημα. Επιπλέον εδώ καταγράφονται ρυθμίσεις του τοίχους προστασίας του Windows (Windows Firewall) που μπορεί να υποδείξουν για παράδειγμα την προσπάθεια κακόβουλου λογισμικού να το απενεργοποιήσει. Επίσης διατηρούνται πληροφορίες διεπαφές δικτύου που είναι διαθέσιμες στο σύστημα όπως IP διευθύνσεις που τους έχουν ανατεθεί και πότε έγιναν DHCP αναθέσεις και πότε τερματίστηκαν οι οποίες είναι χρήσιμες κυρίως για τον συσχετισμό ενός συγκεκριμένου συστήματος με εγγραφές που βρέθηκαν σε logs κάποιου router ή του FTP server.

Επιπλέον, συσκευές που έχουν συνδεθεί στο σύστημα μπορούν να ανιχνευθούν μέσω του Registry. Εκεί αποθηκεύονται πληροφορίες για τις συσκευές έτσι ώστε να αναγνωριστούν αμέσως μόλις ξανά συνδεθούν στο σύστημα. Έτσι ένας αναλυτής μπορεί, όχι μόνο να ανακαλύψει τι είδη συσκευών έχουν συνδεθεί στο σύστημα αλλά και να προσδιορίσει μοναδικά τις συσκευές αυτές και να εντοπίσει πότε συνδέθηκαν στο σύστημα. Για το σκοπό αυτό θα πρέπει να συλλέξει πληροφορίες από διαφορετικά μέρη του ίδου hive αρχείου αλλά και να συνδιάσει δεδομένα από πολλά διαφορετικά hive αρχεία (System, Software και NTUSER.dat). Είναι προφανές λοιπόν ότι ο αναλυτής έχει στη διάθεσή του πληροφορίες ανεκτίμητης αξίας όταν προσπαθεί να ανιχνεύσει για παράδειγμα τη χρήση ενός iPod, μιας ψηφιακής κάμερας ή μιας USB συσκευής σε ένα ή πολλά συστήματα.

Επίσης το Registry καταγράφει πληροφορίες για τις δραστηριότητες ενός χρήστη στα αρχεία NTUSER.dat και USRCLASS.dat. Αποθηκεύει αρχεία στα οποία ο χρήστης είχε πρόσβαση πρόσφατα και τη σειρά με την οποία είχε πρόσβαση σε αυτά, αρχεία τα οποία άνοιξε ή έσωσε πρόσφατα, αναζητήσεις τις οποίες εκτέλεσε χρησιμοποιώντας την ενσωματωμένη δυνατότητα αναζήτησης του Windows καθώς και τροποποιήσεις που έκανε στο μέγεθος και τη θέση του παραθύρου εφαρμογών που χρησιμοποίησε. Ακόμα υπάρχουν τιμές που ανιχνεύουν αλληλεπιδράσεις του χρήστη με τον Windows Explorer και κυρίως όταν ο χρήστης κάνει κλικ ή διπλό κλικ σε διάφορα εφαρμογές (φυλάσσεται η τελευταία φορά επιλογής της κάθε εφαρμογής και το πόσες φορές επιλέχθηκε).

Εργαλεία

Οι αναλυτές μπορεί να χρειαστεί να εξάγουν δεδομένα του Registry είτε από ένα σύστημα σε λειτουργία είτε από το αρχείο-εικόνα ενός συστήματος (image file).

Registry Editor

Για ένα σύστημα σε λειτουργία μπορούν να χρησιμοποιηθούν εργαλεία όπως ο Registry Editor (regedit.exe) που αναφέρθηκε προηγουμένως ο οποίος όμως παρουσιάζει το Registry μόνο του συστήματος στο οποίο είναι συνδεδεμένος ο τρέχων χρήστης κι επομένως σε περιπτώσεις όπου πολλαπλά συστήματα πρέπει να μελετηθούν ταυτόχρονα και γρήγορα ο regedit.exe δεν είναι η καταλληλότερη επιλογή. Επίσης αυτό το εργαλείο δεν επιτρέπει την πρόσβαση σε κάποια δεδομένα όπως το LastWrite time των κλειδιών.

Reg.exe

Είναι ένα εργαλείο γραμμής εντολών ενσωματωμένο στο Windows (από XP και μετά) και δίνει τη δυνατότητα όχι μόνο ανάγνωσης των στοιχείων του Registry αλλά και διαγραφής, τροποποίησης ή πρόσθεσης κλειδιών και τιμών. Για να ξεκινήσει ο reg.exe πρέπει να ανοίξουμε μία γραμμή εντολών (command prompt) και να πληκτρολογήσουμε reg /? όπου θα δούμε όλες τις δυνατές λειτουργίες του εργαλείου. Δε δίνει πρόσβαση στο LastWrite των κλειδιών αλλά επεξεργασίας του Registry ενός απομακρυσμένου συστήματος.

Mitec Windows Registry Recovery

Είναι ένα πρόγραμμα προβολής των hive αρχείων αφού αυτά έχουν εξαχθεί είτε για παράδειγμα από ένα αρχείο-εικόνα (image file) είτε από ένα σύστημα

μέσω απομακρυσμένης πρόσβασης. Με τον Windows Registry Recovery (WRR) ο αναλυτής μπορεί να περιηγηθεί σε ένα αρχείο του Registry όπως και με τον Registry Editor με τη διαφορά ότι το αρχείο αυτό δε θα είναι σε ένα ”ζωντανό” (live) σύστημα. Ο WRR δίνει πρόσβαση στην χρονική στιγμή Lastwrite των κλειδιών καθώς και δυνατότητα εκτέλεσης αναζήτησης με χρήση λέξεων κλειδιών. Το εργαλείο αυτό διατίθεται στην ιστοσελίδα `http://www.mitec.cz/wrr.html`.

RegRipper

Ο Regipper είναι ένα εργαλείο λογισμικού σε Perl ανοιχτού κώδικα που αναπτύχθηκε από τον Harlan Carvey για την εξαγωγή πληροφοριών από τα hive αρχεία του Registry και είναι διαθέσιμο στην ιστοσελίδα `https://code.google.com/p/regripper/downloads/list`. Το εργαλείο αυτό χρησιμοποιεί plugins που είναι αρχεία με κώδικα σε Perl και υποδεικνύουν στο εργαλείο σε ποιον hive εφαρμόζονται, τι κλειδιά και τιμές να ψάξει και τι πληροφορίες να εξάγει. Μπορεί να χρησιμοποιηθεί είτε μέσω ενός γραφικού περιβάλλοντος (rr.exe) είτε μέσω της γραμμής εντολών (rip.pl). Ο πρώτος τρόπος δίνει τη δυνατότητα της εφαρμογής μόνο ομάδων plugins σε αρχεία του Registry ενώ ο δεύτερος και της εφαρμογής μεμονωμένων plugis κι επομένως της εξαγωγής πιο στοχευμένης πληροφορίας.

RegSlack

Είναι ένα εργαλείο γραμμής εντολών σε Perl, το οποίο επεξεργάζεται τον ελεύθερο χώρο ενός hive του Registry και βρίσκει διαγραμμένα κλειδιά. Φτιάχτηκε από την Jolanta Thomassen και διατίθεται στην ιστοσελίδα `http://code.google.com/p/winforensicaanalysis/downloads/list`.

3.1.3 Αρχεία του Windows

Τα συστήματα με λειτουργικό σύστημα Windows διαθέτουν μεγάλο αριθμό αρχείων σε ποικιλία μορφών (π.χ event logs) τα οποία είναι χρήσιμα για έναν ερευνητή. Μπορεί να περιέχουν και μεταδεδομένα ενσωματωμένα σε διάφορες δομές, κάποιες από τις οποίες είναι λεπτομερώς καταγεγραμμένες ενώ άλλες έχουν ανακαλυφθεί μέσα από την ανάλυση. Οι αναλυτές, γνωρίζοντας πολλαπλές τοποθεσίες μέσα στο σύστημα στις οποίες φυλάσσεται πληροφορία, μπορούν να την συνδυάσουν μ πληροφορίες από άλλες πηγές και να μειώσουν την αβεβαιότητα των αποτελεσμάτων της ανάλυσής τους. Επομένως είναι σημαντική η κατανόηση της δομής των αρχείων που συναντώνται σε ένα σύστημα με Windows και η γνώση εργαλείων και τεχνικών για την επεξεργασία κι εξαγωγή πληροφοριών

από αυτά. Στη συνέχεια θα περιγραφούν κάποια από αυτά τα αρχεία καθώς και αντίστοιχα εργαλεία.

Event Logs

Στα συστήματα με Windows είναι πολλά και διαφορετικά αρχεία καταγραφής (Logs) που δημιουργούνται είτε από το ίδιο το λειτουργικό σύστημα είτε από εφαρμογές εγκατεστημένες σε αυτό. Τα αρχεία καταγραφής παίζουν σημαντικό ρόλο σε μία έρευνα διότι ενώ η ζωντανή κατάσταση ενός συστήματος είναι ευμετάβλητη, τα αρχεία αυτά (αν είναι διαθέσιμα) παρέχουν σημαντικά δεδομένα για προηγούμενες δραστηριότητες του συστήματος. Για παράδειγμα μπορεί να καταγραφούν επιτυχημένες και αποτυχημένες προσπάθειες σύνδεσης (login) σε ένα σύστημα.

Στο ποια γεγονότα είναι διαθέσιμα στα αρχεία καταγραφής ενός συστήματος παίζει ρόλο η πολιτική ελέγχου (audit policy) που δίνει δυνατότητα επιλογής της καταγραφής ή μη διαφόρων γεγονότων σχετικών με την ασφάλεια του συστήματος και η οποία είναι σημαντικό να ελέγχετε πριν από μία έρευνα ώστε να είναι γνωστό ποια γεγονότα θα έπρεπε να βρεθούν καταγεγραμμένα και ποια όχι. Για παράδειγμα, σε μια υπόθεση με παράνομες εικόνες, εάν επιτρέπεται η καταγραφή προσπαθειών σύνδεσης (login attempts) αλλά δεν υπάρχουν ενδείξεις απομακρυσμένης σύνδεσης στα Logs, μπορεί να ενισχυθεί η υποψία ότι ένας λογαριασμός χρήστη μπήκε στο σύστημα τοπικά (local access) και επεξεργάστηκε τις εικόνες. Σε ένα σύστημα σε λειτουργία, η πολιτική ελέγχου μπορεί να προσδιοριστεί είτε μέσω της συντόμευσης Local Security Policy στα εργαλεία διαχείρισης (Administrative tools) του πίνακα ελέγχου είτε με το εργαλείο auditpol που τρέχει στη γραμμή εργαλείων. Σε ένα αποκτηθέν αντίγραφο ενός συστήματος, εντοπίζεται από το κλειδί PolAdtEv του Security hive του Registry.

Οι παλαιότερες εκδόσεις του Windows (NT,2000,2003 και XP) χρησιμοποιούν ένα σύστημα καταγραφής αρχείων που ονομάζεται Event Logging και αποθηκεύουν τα αρχεία στο φάκελο %SystemRoot%\System32 \Config. Τα αρχεία καταγραφής των συστημάτων αυτών αποτελούνται από εγγραφές γεγονότων (event records) σε κάθε μία από τις οποίες δίνεται ένα μοναδικό αναγνωριστικό (Event ID) και οι οποίες αποθηκεύονται σε μία δυαδική μορφή η οποία είναι τόσο καλά ορισμένη έτσι ώστε είναι εύκολο να γραφούν εργαλεία για την εξαγωγή εγγραφών γεγονότων όχι μόνο από τα αρχεία καταγραφής αλλά και από σχετικά αδόμητα δεδομένα όπως ο ελεύθερος χώρος (unallocated space) ή το page file. Περισσότερες πληροφορίες για τη μορφή αυτή βρίσκονται στην MSDN ιστοσελίδα (`http://msdn.microsoft.com/en-US/`).

Οι νεώτερες εκδόσεις του Windows (Vista και μετά) χρησιμοποιούν ένα μη-

χανισμό που ονομάζεται ”Windows Event Log” και διαφέρει αρκετά από το Event Logging ως προς το πώς καταγράφονται τα γεγονότα, το είδος τους, την τοποθεσία τους και τη δομή τους. Τα Windows Event Logs αποθηκεύονται στο φάκελο %SystemRoot% \Windows \system32 \winevt \Logs και σε XML μορφή.

Στο σχήμα 3.2 βλέπουμε διάφορα αρχεία καταγραφής που συναντώνται σε ένα σύστημα με Windows Vista ή νεότερη έκδοση. Για παράδειγμα υπάρχουν τα Application, Security και System event logs τα οποία αντιστοιχούν στα ”appevent.evt”, ”secevent.evt” και ”sysevent.evt” αρχεία των παλαιότερων εκδόσεων του Windows. Το Security event log καταγράφει πολλά ίδια γεγονότα με αυτά που καταγράφονται σε Windows XP με τη διαφορά όμως ότι πολλές φορές το αναγνωριστικό για ίδια γεγονότα, διαφέρει. Για παράδειγμα, στο Windows 7 ένα γεγονός σύνδεσης έχει ID 4096 ενώ στο XP έχει 528. Μία μεγάλη λίστα των εγγραφών που υπάρχουν στο Security Event log για Windows 7 και XP μπορεί να βρεθεί στην ιστοσελίδα Ultimate Windows Security 9 (`http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx`). Το Setup log περιλαμβάνει γεγονότα σχετικά με την εγκατάσταση και τις ενημερώσεις εφαρμογών και το Forwarded event log αποθηκεύει γεγονότα που προωθούνται από άλλα συστήματα. Τέλος τα Applications και Services event logs αποθηκεύουν γεγονότα για μία συγκεκριμένη εφαρμογή ή συστατικό και όχι γεγονότα που επηρεάζουν όλο το σύστημα[3].

Προσοχή!

Ο χώρος κάθε αρχείου καταγραφής είναι περιορισμένος. Όταν ένα αρχείο καταγραφής γεμίσει, παλιές εγγραφές διαγράφονται για να προστεθούν οι καινούριες. Άρα υπάρχει περιορισμός στο πόσο πίσω στο χρόνο μπορούμε να ανατρέξουμε για στοιχεία. Όμως, πληρέστερο ιστορικό των γεγονότων μπορεί να αναζητηθεί σε VSCs (Volume Shadow Copy)[α΄] του συστήματος.

[α΄] VSCs είναι προηγούμενες εικόνες του συστήματος. Διατηρούν αντίγραφα ασφαλείας παλαιότερων εκδόσεων του συστήματος και των αρχείων του χρήστη σε ένα συγκεκριμένο τόμο του δίσκου (disk volume)

Εργαλεία

Event Viewer

Ο Event Viewer είναι ένα εργαλείο ενσωματωμένο σε κάθε έκδοση του Windows και χρησιμοποιείται για την προβολή των αρχείων καταγραφής του συστήματος. Στηρίζεται στις λειτουργίες του Windows API του συστήματος στο οποίο γίνεται η ανάλυση το οποίο μπορεί να φέρει αντιμέτωπο τον αναλυτή με το μήνυμα ότι

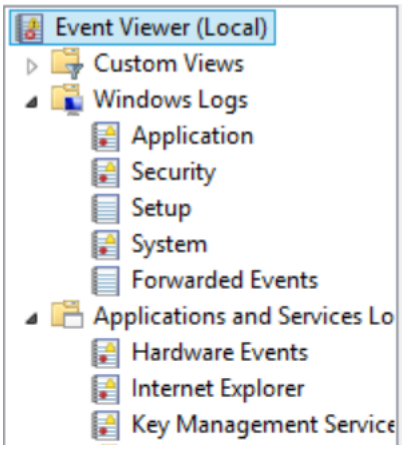
κάποιο αρχείο καταγραφής είναι κατεστραμμένο που όμως στην πραγματικότητα οφείλεται στο ότι κάποιο DLL αρχείο δεν υπάρχει στο σύστημα ανάλυσης.

Perl scripts

Το **evtrpt.pl** είναι ένα αρχείο δέσμης ενεργειών (script file) σε Perl, γραμμένο από τον Harlan Carvey και εξάγει πληροφορίες από τα αρχεία καταγραφής του Windows XP και παλαιότερων εκδόσεων. Πιο συγκεκριμένα, δίνει μια γρήγορη γενική εικόνα για τις πληροφορίες που είναι διαθέσιμες στο αρχείο καταγραφής που έχει δοθεί ως είσοδος, καθώς επιστρέφει για κάθε γεγονός, την πηγή του, το ID του και τον αριθμό των φορών που συνέβη. Επίσης παρέχει το χρονικό διάστημα στο οποίο συνέβησαν τα γεγονότα που είναι καταγεγραμμένα στο αρχείο πράγμα επίσης σημαντικό καθώς, συγκρίνοντας το με διαθέσιμες ημερομηνίες ενός γεγονότος, μας υποδεικνύει το αν έχει νόημα να μελετήσουμε περαιτέρω το αρχείο.

Το **evtparse.pl** διαβάζει τα αρχεία καταγραφής δεδομένων Windows XP και παλαιότερων εκδόσεων. Τα επεξεργάζεται σε δυαδικό επίπεδο και προσδιορίζει και επεξεργάζεται τις εγγραφές χωρίς χρήση των λειτουργιών του Windows API του συστήματος στο οποίο γίνεται η ανάλυση, πράγμα θετικό καθώς αποφεύγεται η ένδειξη ότι κάποιο αρχείο καταγραφής είναι κατεστραμμένο. Επίσης το εργαλείο αυτό μπορεί να χρησιμοποιηθεί σε οποιαδήποτε πλατφόρμα (Windows, Linux και Mac) και επιστρέφει τις εγγραφές σε μορφή csv ή σε μορφή κατάλληλη για timeline ανάλυση.

Τέλος το **evtxparse.pl** χρησιμοποιείται για την επεξεργασία αρχείων καταγραφής δεδομένων του Windows 7 και νεότερων εκδόσεων.



Σχήμα 3.4: Windows Event Logs μέσω του Event Viewer

LogParser

Ο Log Parser είναι ένα εργαλείο γραμμής εντολών το οποίο επιτρέπει την εφαρμογή ερωτήσεων (queries) σε αρχεία βασισμένα σε κείμενο όπως log αρχεία, xml αρχεία και csv αρχεία, καθώς και σε άλλα αρχεία του Windows όπως το Event Log, το Registry και το file system. Το εργαλείο αυτό παρέχεται από τη Microsoft και διατίθεται στην ιστοσελίδα `http://www.microsoft.com/en-us/download/details.aspx?id=24659`.

Προσοχή!

Ο Log Parser στηρίζεται στη διεπαφή προγραμματισμού εφαρμογής (API) του συστήματος στο οποίο εκτελείται. Έτσι για παράδειγμα δεν μπορεί να χρησιμοποιηθεί για την επεξεργασία αρχείων καταγραφής των Windows Vista ή 7 ενώ εκτελείται από σύστημα με Windows XP καθώς το API των αρχείων καταγραφής στο Windows XP είναι ασύμβατο με τον τύπο των αρχείων καταγραφής στα Vista/7/8 [3].

Prefetch αρχεία

Ξεκινώντας με το Windows XP, το λειτουργικό σύστημα απέκτησε τη δυνατότητα να εκτελεί ”Prefetching”. Όλες οι εκδόσεις Windows εκτελούν prefetching εκκίνησης (boot prefetching) αλλά μόνο το Windows XP, Vista και 7 εκτελούν αυτόματα prefetching εφαρμογών (Windows 8 και 2003 έχουν αυτή τη δυνατότητα αλλά αφού προηγηθεί κατάλληλη τροποποίηση του Registry) [3].

Το prefetching εφαρμογών έχει σκοπό να βελτιώσει την εμπειρία του χρήστη επιτρέποντας σε εφαρμογές που χρησιμοποιούνται συχνά να ξεκινάνε γρηγορότερα, αποθηκεύοντας σε συγκεκριμένη τοποθεσία DLLs και άλλα δεδομένα απαραίτητα για την εκκίνηση των εφαρμογών αυτών έτσι ώστε να μη χρειάζεται να τα ψάχνει κάθε φορά μέσα στο σύστημα αρχείων. Κάθε φορά που εκτελείται μία εφαρμογή για πρώτη φορά, ένα prefetch (με επέκταση .pf) αρχείο γι αυτήν την εφαρμογή δημιουργείται και αποθηκεύεται στο φάκελο % SystemRoot % \Windows \Prefetch. Τα ονόματα των αρχείων αυτών περιλαμβάνουν το όνομα της εφαρμογής και μία παύλα ακολουθούμενη από μία τιμή κατακερματισμού (hash value) κατασκευασμένη με χρήση, ανάμεσα στα άλλα, και του μονοπατιού (path) που οδηγεί στην εφαρμογή.

Από τη σκοπιά του αναλυτή, τα Prefetch αρχεία έχουν μεγάλη σημασία για μία έρευνα. Πρώτα απ’ όλα η ύπαρξη και μόνο ενός τέτοιου αρχείου αποτελεί ένδειξη ότι η αντίστοιχη εφαρμογή έχει εκτελεστεί στο σύστημα. Επιπλέον τα prefetch αρχεία περιέχουν χρήσιμα μεταδεδομένα. Η ημερομηνία δημιουργίας του αρχείου δείχνει την πρώτη φορά που έτρεξε η εφαρμογή, με δεδομένο βέβαια

ότι δεν υπήρχε κάποιο παλαιότερο prefetch αρχείο για τη συγκεκριμένη εφαρμογή το οποίο διαγράφηκε οπότε αργότερα κάποιο άλλο πήρε τη θέση του. Επιπλέον τα αρχεία περιλαμβάνουν την ημερομηνία όπου έτρεξε για τελευταία φορά μια εφαρμογή, πόσες φορές έχει εκτελεστεί, από ποιον τόμο (volume) έτρεξε καθώς και DLLs ή άλλα αρχεία που χρησιμοποίησε κατά την εκτέλεσή της.

Εργαλεία

pref.pl

Το pref.pl είναι ένα αρχείο δέσμης ενεργειών (script file) σε Perl που γράφτηκε από τον Harlan Carvey και το οποίο επεξεργάζεται χρήσιμα μεταδεδομένα των Prefetch αρχείων των Windows XP, 2003, Vista και 7. Πρέπει να σημειωθεί ότι υπάρχουν διαφορές στο μηχανισμό του prefetching και στην μορφή των prefetch αρχείων ανάμεσα στα Windows XP/2003 και στα Vista/7. Επομένως όταν χρησιμοποιείται το pref.pl για εξαγωγή μεταδεδομένων από Vista ή 7 πρέπει να δηλώνεται ξεκάθαρα μέσω του ορίσματος "-v".

PFDump.exe

Είναι ένα εργαλείο γραμμής εντολών που επεξεργάζεται τα μεταδεδομένα των Prefetch αρχείων και επιστρέφει αποτελέσματα σε TXT ή HTML ή XML μορφή. Είναι γραμμένο από τον Michael Spohn και διατίθεται στην ιστοσελίδα `http://malware-hunters.net/category/tools/`.

Prefetch Parser

Είναι ένα εργαλείο με γραφικό περιβάλλον κατασκευασμένο από τον Mark McKinnon και διατίθεται στην ιστοσελίδα του `http://redwolfcomputerforensics.com`.

Jump Lists

Οι Jump lists είναι ένα νέο χαρακτηριστικό του Windows 7. Είναι λίστες αρχείων που ο χρήστης έχει ανοίξει πρόσφατα και είναι οργανωμένες με βάση την εφαρμογή που άνοιξε τα αρχεία. Τα περιεχόμενά τους εμφανίζονται, μαζί με τις αντίστοιχες εφαρμογές, στη γραμμή εργασιών (task bar) και στο μενού Έναρξη. Οι λίστες αυτές δίνουν στοιχεία για τους σκοπούς ενός χρήστη διότι για να δημιουργηθούν πρέπει ο χρήστης να κάνει μία συγκεκριμένη ενέργεια (π.χ να ανοίξει ένα αρχείο). Επιπλέον τα περιεχόμενα των λιστών μπορεί να διατηρηθούν για

καιρό αφότου έχει ανοιχτεί ένα αρχείο και διατηρούνται ακόμα κι αν το αρχείο διαγραφεί ή μπορεί και αφού η αντίστοιχη εφαρμογή απεγκατασταθεί!

Από τη σκοπιά του αναλυτή οι Jump lists αποτελούνται από δύο είδη αρχείων. Τα αρχεία του πρώτου είδους βρίσκονται στο προφίλ του χρήστη, στο φάκελο AppData \Roaming \Microsoft \Windows \Recent \AutomaticDestinations και δημιουργούνται από το λειτουργικό σύστημα όταν ο χρήστης εκτελεί συγκεκριμένες ενέργειες όπως άνοιγμα αρχείων και χρήση του εργαλείου Remote Desktop Connection. Έχουν επέκταση .automaticDestinations-ms (autodest files) και οι πρώτοι 16 χαρακτήρες του ονόματος κάθε αρχείου αποτελούν το προσδιοριστικό εφαρμογής (AppID) [4], προσδιορίζουν την εφαρμογή που το δημιούργησε και δεν αλλάζουν από σύστημα σε σύστημα. Είναι δομημένα με βάση τον τύπο αρχείου OLE/compound document και περιλαμβάνουν μεμονωμένες σειρές δεδομένων (streams) δύο ειδών: σειρές σε μορφή LNK και μία σειρά DestList η οποία παίζει το ρόλο MRU[5] λίστας.

Τα αρχεία του δεύτερου τύπου με επέκταση .CustomDestinations-ms (customdest files), βρίσκονται στο προφίλ του χρήστη, στο φάκελο AppData \Roaming \Microsoft \Windows \Recent \CustomDestinations και δημιουργούνται όταν ο χρήστης καρφιτσώνει (pin) ένα αρχείο σε μια εφαρμογή (π.χ μέσω της γραμμής εργαλείων). Αποτελούνται από ενωμένες σειρές δεδομένων σε LNK τύπο αρχείου (όχι συσκευασμένες σε OLE). Και αυτών των αρχείων τα ονόματα ξεκινούν με αναγνωριστικό εφαρμογής 16 χαρακτήρων.

Εργαλεία

Τα αρχεία autodest, λόγω , μπορεί να προβληθούν με εργαλεία που επιτρέπουν τη διαχείριση της συσκευασίας OLE όπως ο Mitec Structured Storage Viewer (`http://www.mitec.cz/ssv.html`). Οι αριθμημένες σειρές δεδομένων μέσα στα αρχεία πρέπει στη συνέχεια να υποστούν επεξεργασία με κάποιον LNK Viewer όπως ο Mitec Windows File Analyzer (`http://www.mitec.cz/wfa.html`) που μεταξύ άλλων επεξεργάζεται και αρχεία σε LNK.

Άλλο εργαλείο για τα autodest είναι ο JumpLister του Mark Woan (`http://www.woanware.co.uk/forensics/jumplister.html`) που αυτόματα επεξεργάζεται τα streams δεδομένων και προβάλει τα περιεχόμενά τους. Επιπλέον το εργαλείο ProDiscover που θα περιγραφεί σε επόμενο κεφάλαιο, έχει ενσωματωμένο Jump List Viewer που αυτόματα επεξεργάζεται τα streams δεδο-

[4] Λίστα με τα AppIDs εφαρμογών υπάρχει στην ιστοσελίδα `http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs`

[5] MRU λίστα είναι μια λίστα που διατηρεί τη σειρά με την οποία διάφορες τιμές χρησιμοποιήθηκαν (ανάλογα με την εφαρμογή στην οποία αναφέρεται).

μένων.

3.1.4 Timelines

Ένα από τα πρώτα πράγματα που μπορεί να κάνει ένας αναλυτής για να διευκολύνει την έρευνά του, είναι να δημιουργήσει ένα timeline της δραστηριότητας του συστήματος που μελετά. Αυτό σημαίνει να τοποθετήσει σε χρονολογική σειρά, τα διάφορα γεγονότα που έχουν συμβεί στο σύστημα.

Πηγές για ένα timeline υπάρχουν άφθονες, και ειδικά σε ένα σύστημα με Windows, όπου υπάρχουν πάρα πολλές υπηρεσίες και εφαρμογές που, μαζί με τα δεδομένα που φυλάνε, διατηρούν και χρονική πληροφορία γι αυτά. Έχουμε δει ήδη τους χρόνους ”MACB” των MFT εγγραφών, τα αρχεία καταγραφής (Event Logs), τα Prefetch αρχεία και φυσικά το Registry με τους LastWrite χρόνους των κλειδιών του. Άλλες πηγές αποτελούν εφαρμογές πελάτη όπως το αρχείο bookmarks.html του περιηγητή ιστού FireFox, το οποίο με τους σελιδοδείκτες που έχουν προστεθεί, κρατάει την ημερομηνία της προσθήκης και την τελευταία φορά που τροποποιήθηκαν.

Πλεονεκτήματα

Με την κατασκευή timeline από πολλές διαφορετικές πηγές, επιτυγχάνονται τρία βασικά πράγματα: Προσθήκη ”πλαισίου” στα γεγονότα, αύξηση του βαθμού εμπιστοσύνης προς τα γεγονότα και εξοικονόμηση χώρου και χρόνου[3].

1. Προσθήκη πλαισίου στα γεγονότα σημαίνει ότι, συνδυάζοντας πολλές πηγές, αρχίζουν να φαίνονται περισσότερες πληροφορίες για δραστηριότητες που έχουν συμβεί κοντά σε ένα γεγονός και άρα πιθανόν σχετίζονται με αυτό. Για παράδειγμα, στην περίπτωση που ένα αρχείο έχει τροποποιηθεί μια συγκεκριμένη χρονική στιγμή, μπορεί να μας ενδιαφέρει τι προκάλεσε την μεταβολή αυτή (χρήστης; ενημέρωση λειτουργικού ή εφαρμογής; κακόβουλο λογισμικό;). Χρησιμοποιώντας χρονική πληροφορία από διάφορες πηγές και οργανώνοντας τη σε μία συνολική εικόνα, φαίνεται τι επιπλέον δραστηριότητα συνέβη στο σύστημα κοντά στο χρόνο που τροποποιήθηκε το υπό εξέταση αρχείο.

2. Αύξηση εμπιστοσύνης προς τα γεγονότα σημαίνει ότι αυξάνεται η σιγουριά του αναλυτή ότι η χρονική πληροφορία ενός γεγονότος είναι πράγματι ακριβής. Αυτό είναι σημαντικό, διότι για κάποιες πηγές γεγονότων οι χρόνοι είναι εύκολο να αλλοιωθούν (π.χ οι ”MACB” του $ SIA). Από την άλλη, για άλλες πηγές (όπως τα LastWrite του Registry) είναι πολύ πιο δύσκολο.

Έτσι, αν βρεθεί ένα γεγονός με χαμηλό βαθμό εμπιστοσύνης κοντά σε ένα σχετιζόμενο γεγονός που δεν μπορεί να αλλοιωθεί εύκολα, η εμπιστοσύνη για την ακρίβεια του πρώτου αυξάνεται σημαντικά!

3. Τα timelines είναι πληροφορίες σε μορφή κειμένου που μπορούν να εξαχθούν, συμπιεστούν και να μεταφερθούν σε άλλες αναλύσεις πολύ πιο εύκολα από το να μεταφερθούν ολόκληρες εικόνες δίσκων (μπορεί και με χωρητικότητα πολλών GB).

Μεθοδολαγία

Για τη δημιουργία timeline, δεν υπάρχει κάποιο εμπορικό εργαλείο που με το πάτημα ενός κουμπιού να επιστρέφει timeline από όλα τα διαθέσιμα δεδομένα. Συχνά πρέπει να χρησιμοποιηθεί μεγάλη ποικιλία ελεύθερων εργαλείων και εργαλείων ανοιχτού κώδικα.

Ο αναλυτής ξεκινάει με το αρχείο-εικόνα ενός δίσκου και εξάγει οποιαδήποτε πληροφορία τον ενδιαφέρει με όποιο εργαλείο είναι διαθέσιμο για το σκοπό αυτό και με τη μορφή που χρησιμοποιεί το εργαλείο αυτό. Μετά, είτε δημιουργώντας, είτε χρησιμοποιώντας υπάρχοντα εργαλεία, μετατρέπει τα διάφορα γεγονότα σε μία ενιαία μορφή και τα μεταφέρει όλα μαζί σε ένα ενδιάμεσο αρχείο. Η μορφή περιλαμβάνει πέντε πεδία και λέγεται TLN μορφή:

Time|*Source*|*System*|*User*|*Description*

Time είναι η χρονική στιγμή που συνέβη το γεγονός.
Source είναι η πηγή μέσα στο σύστημα από την οποία προήλθε η χρονική πληροφορία.
System είναι το σύστημα ή η συσκευή από την οποία προήλθαν τα δεδομένα με την χρονική πληροφορία.
User είναι ο χρήστης που σχετίζεται με το γεγονός (αν υπάρχει).
Description είναι μια μικρή περιγραφή του γεγονότος που συνέβη.

Τέλος, το ενδιάμεσο αρχείο, μετατρέπεται στην τελική χρονολογική σειρά των γεγονότων.

Απαραίτητα εργαλεία για την κατασκευή timeline σε Windows είναι η ActiveState ActivePerl (`http://www.activestate.com/activeperl`), κάποια timeline σκριπτάκια (tln_ tools.zip στην `http://code.google.com/p/\winforensicaanalysis/downloads/list`) και εργαλεία του sleuth kit (`http://www.sleuthkit.org/`)

3.2 Ανάλυση Αρχείων

Σε πολλές διαφορετικές έρευνες, είναι απαραίτητη η κατανόηση της φύσης μεμονωμένων αρχείων που εντοπίζονται και εξάγονται από μία συσκευή αποθήκευσης. Κατανοώντας τα αρχεία αυτά, γίνεται ευκολότερη η αποκάλυψη και αξιοποίηση άλλων στοιχείων μεγαλύτερης αξίας που πιθανόν υπάρχουν μέσα στα αρχεία. Για παράδειγμα, ένα κακόβουλο αρχείο (malicious document) μπορεί να αποτελέσει το σημείο εισόδου ενός επιτιθέμενου στο σύστημα. Ο εξεταστής μπορεί να πρέπει να βρει παράνομες εικόνες ή βίντεο στο σύστημα. Επίσης η παρουσία του ίδιου αρχείου σε δύο διαφορετικά μηχανήματα, συνδέει μεταξύ τους τα μηχανήματα αυτά και τους χρήστες τους. Μάλιστα το ότι τα αρχεία αυτά είναι αυτόνομα και μεταφέρονται εύκολα μεταξύ συστημάτων, τα μετατρέπει σε σημαντική πηγή στοιχείων.

Η ανάλυση αρχείων χωρίζεται σε δύο διακριτές αλλά και συμπληρωματικές δραστηριότητες: προσδιορισμός περιεχομένου και εξαγωγή μεταδεδομένων. Η πρώτη είναι ο προσδιορισμός ή η πιστοποίηση του τι ακριβώς είναι ένα συγκεκριμένο αρχείο (π.χ αν είναι αρχείο εικόνας) και η δεύτερη είναι η εξαγωγή οποιονδήποτε μεταδεδομένων, ενσωματωμένων στο αρχείο. Οι διάφοροι τύποι αρχείων που μπορεί να παίξουν ρόλο σε μία έρευνα χωρίζονται σε πέντε κατηγορίες οι οποίες θα αναλυθούν στη συνέχεια: εικόνες, αρχεία ήχου, βίντεο, έγγραφα (documents) και αρχεία αποθήκευσης (archives).

Προσδιορισμός περιεχομένου

Ο στόχος του προσδιορισμού του περιεχομένου, είναι η επιβεβαίωση είδους ενός συγκεκριμένου αρχείου. Πολλοί χρήστες υπολογιστών προσδιορίζουν τον τύπο ενός αρχείου (file type) από την επέκτασή του. Προφανώς, για έναν αναλυτή, η μέθοδος αυτή δεν είναι επαρκής για δύο κυρίως λόγους. Πρώτον, είναι εύκολο για ένα χρήστη να αλλάξει την επέκταση και την προεπιλεγμένη εφαρμογή που ανοίγει ένα αρχείο ώστε να κρύψει την φύση του αρχείου αυτού. Δεύτερον, σε μια έρευνα, είναι πιθανή η ανακάλυψη αρχείων χωρίς επέκταση. Γενικά αυτά θα είναι προσωρινά ή cache αρχεία που δεν προορίζονται για χρήση από τον τελικό χρήστη και μπορεί να περιέχουν σημαντικά δεδομένα.

Για τον προσδιορισμό των τύπων αρχείων, χρησιμοποιούνται δομές που είναι χαρακτηριστικές για συγκεκριμένους τύπους αρχείων. Αυτές ονομάζονται μαγικές τιμές ή μαγικοί αριθμοί (magic values or magic numbers) και γενικά είναι συγκεκριμένες δεκαεξαδικές τιμές που βρίσκονται σε συγκεκριμένες αποστάσεις από την αρχή του αρχείου.

Εργαλεία

HexDump-hex editor:

Για να παρουσιαστεί το δυαδικό περιεχόμενο ενός αρχείου, μπορεί να χρησιμοποιηθεί ένας hexadecimal dump όπως ο xxd του Linux και ο οποίος παρουσιάζει σε κείμενο το δυαδικό περιεχόμενο ενός αρχείου.
Για περισσότερη αλληλεπίδραση με το αρχείο και ανάλυση, μπορεί να χρησιμοποιηθεί ένας επεξεργαστής δεκαεξαδικής μορφής (hex editor) όπως ο HxD. Ο HxD είναι εφαρμογή γραφικού περιβάλλοντος και προσφέρει (μεταξύ άλλων) αναζήτηση και αντικατάσταση, εξαγωγή, τιμές κατακερματισμού, εισαγωγή μοτίβων σε bytes, ένωση ή διαχωρισμό αρχείων και στατιστικά. Διατίθεται στην ιστοσελίδα `http://mh-nexus.de/en/hxd/`.

Hachoir:

Hachoir είναι μία βιβλιοθήκη σε Python που μπορεί να εγκατασταθεί και σε Windows και σε Linux και η οποία επεξεργάζεται και ερμηνεύει δυαδικά αρχεία bit προς bit. Σύμφωνα με τον συγγραφέα, η βιβλιοθήκη αυτή επιτρέπει την "περιήγηση" κάθε σειράς δυαδικών δεδομένων ακριβώς όπως είναι και η περιήγηση φακέλων και αρχείων. Κάποια από τα προγράμματα που χρησιμοποιούν τη βιβλιοθήκη αυτή, είναι:

- hachoir-metadata, ένα εργαλείο που εξάγει και παρουσιάζει μεταδεδομένα από τύπους αρχείων που αναγνωρίζονται από τον hachoir-parser.
- hachoir-urwid, ένα περιβάλλον χρήστη για διερεύνηση δυαδικών αρχείων
- hachoir-subfile, ένα εργαλείο για προσδιορισμό και εξαγωγή αρχείων μέσα από δυαδικές σειρές δεδομένων (binary streams).

Εξαγωγή Μεταδεδομένων

Τα μεταδεδομένα είναι δεδομένα που σχετίζονται με άλλα δεδομένα. Στο πλαίσιο του συστήματος αρχείων, μεταδεδομένα είναι επιπλέον πληροφορίες για περιεχόμενα του συστήματος και είναι αποθηκευμένα σε blocks. Στο πλαίσιο της ανάλυσης αρχείων, μεταδεδομένα είναι πληροφορίες αποθηκευμένες στο ίδιο το αρχείο οι οποίες παρέχουν επιπλέον πληροφορίες για το αρχείο. Ο στόχος τους είναι να παρέχουν ένα πλαίσιο ή πληροφορίες που είναι έξω από τον στόχο των ίδιων των δεδομένων και η αξία τους εξαρτάται από τη φύση της κάθε έρευνας.

Εργαλεία

Το Hachoir-metadata που αναφέρθηκε παραπάνω, χρησιμοποιείται για εξαγωγή μεταδεδομένων από πολλούς τύπους δεδομένων με έμφαση σε μουσική, εικόνες και βίντεο και δίνει περισσότερες πληροφορίες από άλλα παρόμοια εργαλεία.

Η βιβλιοθήκη libextractor διαθέτει την εντολή extract με την οποία αποσπώνται μεταδεδομένα από αρχεία. Μπορεί να εγκατασταθεί και σε Windows και σε Linux και βρίσκεται στην ιστοσελίδα `http://www.gnu.org/software/libextractor/`.

3.2.1 Αρχεία Εικόνας

Τα αρχεία αυτά έχουν σκοπό την παρουσίαση δεδομένων εικόνας στον χρήστη. Μεταφέρουν μεγάλη ποικιλία μεταδεδομένων, από απλά σχόλια κειμένου μέχρι τις γεωγραφικές συντεταγμένες όπου δημιουργήθηκε το αρχείο. Ανάλογα με την έρευνα, ο αναλυτής μπορεί να ενδιαφέρεται για το περιεχόμενο της εικόνας (π.χ η φωτογραφία συγκεκριμένου προσώπου) ή για μεταδεδομένα. Για την εξαγωγή πληροφοριών από μια μεγάλη ποικιλία τύπων αρχείου εικόνας χρησιμοποιείται το πακέτο imagemagick και συγκεκριμένα η εντολή του identify. Διατίθεται για Windows και Linux στην ιστοσελίδα `http://www.imagemagick.org/`.

Υπάρχουν τρία βασικά είδη μεταδεδομένων αρχείων εικόνας:

- **EXIF** αποθηκεύει, μέσα στην ίδια την εικόνα, πληροφορίες για τη συσκευή που τη δημιούργησε (συνήθως φωτογραφική μηχανή). Αυτές περιλαμβάνουν τη μάρκα και το μοντέλο της κάμερας, την ημέρα και ώρα της δημιουργίας και τη γεωγραφική τοποθεσία της κάμερας.

- **IPTC** είναι το πρότυπο που δημιουργήθηκε από το IPTC (International Press Telecommunications) ώστε να ενσωματώνει πληροφορίες σε εικόνες που χρησιμοποιούνται από εφημερίδες και πρακτορεία νέων. Από τη στιγμή που το εργαλείο Adobe Photoshop επέτρεψε στους χρήστες τροποποιήσουν και να εισάγουν IPTC μεταδεδομένα σε ψηφιακές εικόνες, η χρήση τους διαδόθηκε σε ένα πιο ευρύ κοινό.

- **XMP** είναι ένα πρότυπο τύπου μεταδεδομένων που βασίζεται στη γλώσσα XML και αναπτύχθηκε από την Adobe το 2001. Περισσότερο χρησιμοποιείται για μεταδεδομένα εικόνων αλλά και για άλλους τύπους αρχείων λόγω της επεκτασιμότητας του.

JPEG

JPEG (Joint Photographic Experts Group) είναι ο πιο διαδεδομένος τύπος αρχείων εικόνας σήμερα και συναντάται κυρίως με τις επεκτάσεις αρχείων .jpg και .jpeg. Χρησιμοποιεί συμπίεση με απώλειες και είναι πλούσιο σε μεταδεδομένα. Το JFIF (JPEG File Interchange Format) επέκτεινε το JPEG ώστε να συμπεριλάβει μεταδεδομένα συμπεριλαμβανομένου πυκνότητα των pixel, αναλογίες εικόνας και προαιρετικά ένα thumbnail της εικόνας. Εκτός από αυτά τα μεταδεδομένα, τα JPEG αρχεία μπορούν να περιέχουν επίσης EXIF,IPTC ή XMP μεταδεδομένα. Εκτός απο το hachoir-metadata που αναφέρθηκε παραπάνω, άλλα εργαλεία γραμμής εντολών γι αυτούς τους τύπους μεταδεδομένων με περισσότερες δυνατότητες, είναι τα exiftool και exiv2.

Το exiftool κατασκευάστηκε από τον Phil Harvey και υποστηρίζει μεγάλη ποικιλία τύπων μεταδεδομένων συμπεριλαμβανομένου JFIF,EXIF,IPTC και XMP. Μια πλήρη λίστα βρίσκεται στην ιστοσελίδα `http://www.sno.phy.queensu.ca/~phil/exiftool/` όπου διατίθεται και το εργαλείο και για Windows και για Linux. Το exiv2 προσφέρει γρήγορη ανάγνωση και γραφή μεταδεδομένων της μορφής EXIF,IPTC και XMP και διατίθεται στην ιστοσελίδα `http://www.exiv2.org/` και για Windows και για Linux. Το exiv2 είναι πολύ γρηγορότερο από το exiftool και άρα πιο αποτελεσματικό για την επεξεργασία πολύ μεγάλων ποσοτήτων εικόνων.

GIF

Ο τύπος GIF (Graphics Interchange Format) χρησιμοποιείται κυρίως για εικονίδια και απλά γραφικά και παρέχει δυνατότητα για διαφάνεια (transparency) και κινούμενα σχέδια. Δεν δημιουργούνται από κάποια συσκευή οπότε δεν υπήρξε η ανάγκη για ενσωματωμένα μεταδεδομένα. Επομένως τα μεταδεδομένα των GIF αρχείων είναι πολύ λίγα, σχεδόν δεν υπάρχουν καθόλου! Γενικά περιορίζονται σε πληροφορίες για το αρχείο της εικόνας και ίσως και ένα πεδίο με κάποιο σχόλιο. Σπάνια μπορεί να περιέχουν και ετικέτες XMP. Τα hachoir-metadata και exiftool μπορούν να επεξεργαστούν GIF αρχεία.

TFF

Το TFF (Tagged Image File Format) χρησιμοποιείται κυρίως για το σχεδιασμό γραφικών και είναι ο προεπιλεγμένος τύπος για πολλές εφαρμογές του OS X. Όπως φαίνεται από το όνομά του, υποστηρίζει εσωτερικές ετικέτες μεταδεδομένων.Επιπλέον, υπάρχουν επεκτάσεις του όπως το GeoTIFF για αποθήκευση

γεωγραφικών δεδομένων εικόνας και το Microsoft Document Imaging για αποθήκευση σαρωμένων ή αρχείων σταλμένων με φαξ. το exiftool επεξεργάζεται μεταδεδομένα από TIFF αρχεία.

3.2.2 Αρχεία Ήχου

Τα αρχεία ήχου περιλαμβάνουν δεδομένα που παράγουν ήχο (μουσική, μηνύματα φωνής κτλ) αν αποκωδικοποιηθούν καταλλήλως. Με τα αρχεία ήχου, το πιο πιθανό είναι το ενδιαφέρον του ερευνητή να εστιάζεται στο περιεχόμενο τους. Παρόλα αυτά, οι τύποι αρχείων ήχου μπορεί να περιέχουν μεταδεδομένα που πθα προσφέρουν επιπλέον πληροφορίες σε μία έρευνα.

WAV

Το WAV είναι ένα πρότυπο για αποθήκευση μιας σειράς bit ήχου (audio bitstream) που αναπτύχθηκε από την Microsoft και IBM για χρήση σε επιτραπέζιους υπολογιστές. Τα αρχεία ήχου WAV αποθηκεύονται σε κομμάτια (chunks) μέσα σε έναν RIFF κοντέινερ. Ο RIFF κοντέινερ μπορεί να περιέχει ένα κομμάτι INFO το οποίο επιτρέπει την προσθήκη διαφόρων πληροφοριών με ετικέτες στα RIFF αρχεία. Εκτός από αυτά τα ειδικά μεταδεδομένα, αρχεία σε RIFF κοντέινερ μπορούν να περιέχουν XMP μεταδεδομένα. Χρήσιμα μεταδεδομένα όπως το όνομα της εφαρμογής που τα δημιούργησε και την ημερομηνία δημιουργίας, εξάγουμε με το εργαλείο hachoir-metadata.

MPEG-3/MP3

Το MP3 είναι ο πιο διάσημος τύπος αρχείου για μουσική σήμερα και είναι ο προτεινόμενος τύπος για δίκτυα διαμοιρασμού αρχείων όπως τα Napster και Gnutella. Τα MP3 αρχεία περιλαμβάνουν μεταδεδομένα σε δύο δυνατούς τύπους: ID3v1 και ID3v2. Οι ετικέτες ID3v1 είναι περιορισμένες σε ένα διάνυσμα των 128 bytes που προστίθεται στο τέλος του MP3 αρχείου. Οι επεκτεταμένες ID3v1 ετικέτες προσθέτουν για χρήση 227 επιπλέον bytes αμέσως πριν τις ετικέτες ID3v1. Ο τύπος ID3v2 δημιουργήθηκε για να αυξήσει τον χώρο των μεταδεδομένων. Οι ετικέτες ID3v2 δεν έχουν σταθερό μέγεθος και μπορούν να συμπεριλάβουν πολύ μεγαλύτερη ποικιλία μεταδεδομένων σε σχέση με τις ID3v1.

Τα hachoir-metadata και exiftool εξάγουν μεταδεδομένα και των δύο παραπάνω τύπων. Επίσης το εργαλείο γραμμής εντολών id3v2 χρησιμοποιείται και για τους δύο τύπους και διατίθεται (μόνο για Linux) στην ιστοσελίδα `http://id3v2.sourceforge.net`.

3.2.3 Έγγραφα

Έγγραφο είναι ένας πολύ γενικός όρος, όμως στην δικανική υπολογιστών, έγγραφο είναι ένας τύπος αρχείου που περιέχει κείμενο και εικόνα. Παραδείγματα εγγράφων είναι τύποι αρχείων του Office της Microsoft ή αρχεία PDF. Σχεδόν κάθε έγγραφο φέρει μεταδεδομένα όπως ο δημιουργός, εσωτερικές σημάνσεις χρόνου (timestamps), πληροφορίες για το σύστημα όπου έγινε η επεξεργασία του και άλλα πολλά που μπορεί να χρησιμεύσουν σε μία έρευνα.

OLE Compound Files(Office Documents)

Ο τύπος αυτός χρησιμοποιείται από πολλά γνωστά αρχεία όπως τα έγγραφα του Microsoft Office (π.χ παρουσιάσεις PowerPoint, έγγραφα του Word και φύλλα του Excel). Τα αρχεία OLE, είναι μικροσκοπικά, φορητά συστήματα αρχείων. Όπως τα παραδοσιακά συστήματα αρχείων, φέρουν δεδομένα σε μία δομημένη μορφή και διαθέτουν και μεταδεδομένα. Έχουν δύο κύριους μηχανισμούς αποθήκευσης: αντικείμενα αποθήκευσης και αντικείμενα ροής (stream objects). Το αντικείμενο αποθήκευσης λειτουργεί όπως ένας κατάλογος (directory) σε ένα συνηθισμένο σύστημα αρχείων, οπότε περιέχει επιπλέον αντικείμενα αποθήκευσης που δρουν ως υποκατάλογοι (subdirectories). Το αντικείμενο ροής είναι ακολουθίες τομέων του δίσκου κατανεμημένες για ένα τμήμα δεδομένων και παίζει το ρόλο του αρχείου.

Ένα αρχείο OLE αποτελείται από έναν αντικείμενο αποθήκευσης ρίζα (όπως ο κατάλογος ρίζα στα απλά συστήματα αρχείων) και τουλάχιστον ένα αντικείμενο ροής που αναπαριστά τα προεπιλεγμένα δεδομένα για το αρχείο. Επιπλέον, το αντικείμενο αποθήκευσης μπορεί να περιέχει οποιονδήποτε αριθμό άλλων αντικειμένων αποθήκευσης, το κάθε ένα από τα οποία μπορεί να περιέχει οποιονδήποτε αριθμό επιπλέον ροών αποθήκευσης.

Τα OLE αρχεία μπορούν να περιέχουν πολλά μεταδεδομένα συμπεριλαμβανομένου πληροφορίες για τον δημιουργό(π.χ όνομα και e-mail), αριθμό φορών που έγιναν αλλαγές στο έγγραφο, αριθμό εκτυπώσεων, πληροφορίες για τον χρόνο που αφιερώθηκε στην επεξεργασία του, το όνομα του τελευταίου χρήστη που άνοιξε το έγγραφο για επεξεργασία και διάφορες σημάνσεις χρόνου.

Εργαλεία

Στο Λίνουξ υπάρχει η **Libforensics** που είναι μια βιβλιοθήκη σε Python 3.1 από τον Michael Murr, για την ανάπτυξη εφαρμογών της ψηφιακής δικανικής. Πληροφορίες γι αυτήν υπάρχουν στην ιστοσελίδα `http://code.google.com/`

p/libforensics/. Παράδειγμα εργαλείου της Libforensics για OLE αρχεία είναι το olels.py το οποίο επιστρέφει όλες τις εγγραφές που υπάρχουν στο αρχείο (και αντικείμενα ροής και αποθήκευσης). Για Λίνουξ, μπορεί επίσης να χρησιμοποιηθεί το **wvSummary** του πακέτου vw.

Για Windows υπάρχει το εργαλείο **OffVis** της Microsoft και διατίθεται στην ιστοσελίδα
http://www.downloadcrew.com/article/12283-microsoft_offvis. Παρουσιάζει τη δυαδική δομή αρχείων του Office και μπορεί να χρησιμοποιηθεί για την εξέτασή της.

PDF

Το PDF είναι ένας ανοιχτός τύπος αρχείων σχεδιασμένος για να παρουσιάζει το ίδιο έγγραφο σε διαφορετικά συστήματα χωρίς να χρειάζεται η εγκατάσταση επιπλέον γραμματοσειρών, γραφικών, βιβλιοθηκών ή οποιοδήποτε άλλο λογισμικό εκτός από κάποιο πρόγραμμα προβολής PDF αρχείων. Το PDf είναι ένα αρχείο κοντέινερ που φέρει κάποιες οδηγίες σε PostScript για την διάταξη καθώς και ενσωματωμένα γραφικά και γραμματοσειρές. Πέρα από την παρουσίαση απλών δεδομένων, τα PDF αρχεία μπορούν να περιέχουν φόρμες με πεδία τα οποία μπορεί να συμπληρώσει ο χρήστης. Πλέον σε αυτά τα αρχεία περιέχονται και σύνδεσμοι σε δεδομένα έξω από το αρχείο, JavaScript και αντικείμενα ταινίας.

Τα PDF αρχεία μπορούν να περιέχουν δύο είδη μεταδεδομένων. Το πρώτο είδος περιλαμβάνει ζευγάρια κλειδιού/τιμής με πληροφορίες για τον δημιουργό, τον τίτλο του εγγράφου και σημάνσεις χρόνου δημιουργίας/τροποποίησης. Το δεύτερο είδος είναι τα XMP μεταδεδομένα (περιγράφηκαν στην ενότητα για τα αρχεία εικόνας) που υποστηρίζουν πιο σύγχρονα PDF αρχεία. Επιπλέον, σε κάποια PDF που δημιουργούνται από ειδικές εφαρμογές όπως ο Adobe InDesign, καταγράφεται ιστορικό αλλαγών στο αρχείο οι οποίες περιέχουν και τις ημερομηνίες όπου συνέβησαν. Μπορεί να είναι δυνατή ακόμα και η εξαγωγή παλαιότερων εκδόσεων του εγγράφου.

Εργαλεία

Το **exiftool** μπορεί να εξάγει μεταδεδομένα από PDF αρχεία. Ιδιαίτερου ενδιαφέροντος στα μεταδεδομένα που επιστρέφονται από το εργαλείο αυτό είναι οι ετικέτες Creator/Producer. Πολλά PDF αρχεία με κακόβουλο λογισμικό δημιουργούνται με εργαλεία γραμμής εντολών που βάζουν το όνομά τους στη θέση του Creator/Producer. Επίσης το εργαλείο **pdfresurrect** εξετάζει παλαιότερες εκδόσεις ενός PDF αρχείου.

Κεφάλαιο 4

Εργαλεία Δικανικής Υπολογιστών

Ως εδώ έχουμε μιλήσει για χαρακτηριστικά και διαδικασίες που απαιτούνται για την απόκτηση και ανάλυση ψηφιακών δεδομένων στα πλαίσια της δικανικής υπολογιστών. Κατά τη διάρκεια της περιγραφής αυτής, αναφέρθηκαν δυνατότητες και ιδιαιτερότητες εργαλείων που αποσκοπούν κατά κύριο λόγο σε μια συγκεκριμένη λειτουργία (π.χ ο Regripper για την ανάλυση του Registry). Στο κεφάλαιο αυτό θα παρουσιαστούν εργαλεία (ελεύθερα και μη) που υποστηρίζουν ποικιλία λειτουργιών. Αν και καλό είναι ένας ερευνητής να μην στηρίζεται σε ένα και μόνο εργαλείο για μια πλήρη εξέταση, η γνώση τους έχει αξία για αυτόν καθώς προσφέρουν μεταξύ άλλων, αυτοματισμό κάποιων ενεργειών (π.χ αυτόματη επεξεργασία της διαδικτυακής δραστηριότητας ενός χρήστη), εκτεταμένες δυνατότητες αναζήτησης και ένα ”χώρο” (συνήθως ένα γραφικό περιβάλλον) όπου μπορεί να διεξαχθεί η έρευνα πιο συγκεντρωμένη.

4.1 Εμπορικά Εργαλεία

4.1.1 EnCase

Το Encase είναι μια σουίτα προγραμμάτων της ψηφιακής δικανικής φτιαγμένη από την Guidance SoftWare. Είναι από τα πιο δημοφιλή εργαλεία στο χώρο αλλά παράλληλα και από τα πιο ακριβά.

Το Encase προσφέρει γρήγορη δημιουργία αντιγράφου δίσκου σε αρχείο με τύπο Expert Witness Format (ο FTK imager της Access Data έδινε τη δυνατότητα για περισσότερους τύπους αρχείων-εικόνων). Από την πέμπτη έκδοση του Encase, άρχισε να διατίθεται μαζί και ένα εργαλείο, το LinEn, που εκτελείται σε λειτουργικό Linux και είναι μόνο για δημιουργία αντιγράφων. Πολλά live CDs

όπως το Helix (`http://www.e-fense.com/products.php`) έχουν ενσωματωμένο το LinEn.

Σχετικά με την αναζήτηση, το Encase δίνει δυνατότητα τοποθέτησης των δεδομένων σε ευρετήρια για την πιο γρήγορη αναζήτηση σε αυτά αλλά και δυνατότητα απλής αναζήτησης με βάση λέξεις κλειδιά. Επιπλέον, προσφέρει την επεξεργασία και ανάλυση αρχείων διαφόρων μορφών όπως αρχεία του Registry και e-mail και διαθέτει μια σουίτα αποκρυπτογράφησης (Encase Decryption Suite) που αποκρυπτογραφεί δεδομένα και αρχεία κρυπτογραφημένα με το Windows Encrypted File System (EFS)[1]. Τέλος παρέχει δυνατότητα συγγραφής μικρο-προγραμμάτων script (Encrypt) με τα οποία ο ερευνητής μπορεί να αυτοματοποιήσει πολλές ενέργειες με βάση την προτίμησή του.
Διατίθεται στην ιστοσελίδα `https://www.guidancesoftware.com/\products/Pages/encase-forensic/overview.aspx`.

4.1.2 FTK

Το FTK (Forensic Toolkit) είναι μια σουίτα εργαλείων της δικανικής υπολογιστών φτιαγμένη από την AccessData για πλατφόρμες Windows και με χαμηλότερη τιμή από αυτή του Encase.

Το FTK συνδυάζει σε μία μεμονωμένη σουίτα λογισμικού, μία ποικιλία εργαλείων της δικανικής υπολογιστών. Προσφέρει ένα εύχρηστο γραφικό περιβάλλον (θεωρείται πιο φιλικό για το χρήστη από του Encase) και οργανώνει όλα τα ψηφιακά στοιχεία σε ομάδες ανάλογα με τον τύπο τους (π.χ έγγραφα, γραφικά κτλ). Επιτρέπει την ανάλυση μιας συσκευής αποθήκευσης και την αναζήτηση για αρχεία, φακέλους, e-mail, έγγραφα, εικόνες και οποιοδήποτε άλλο στοιχείο ακόμα κι αν είναι σβησμένο ή κατεστραμμένο. Το εργαλείο αναζήτησης που παρέχει είναι ισχυρό καθώς επιτρέπει αναζήτηση συγκεκριμένων λέξεων κλειδιών ή μοτίβων αριθμών που μπορούν να αποκαλύψουν για παράδειγμα, εγκλήματα με αριθμούς πιστωτικών καρτών. Η αναζήτηση μπορεί να είναι είτε απλή είτε με ευρετήρια και λέγεται ότι η δημιουργία ευρετηρίων με το FTK (που έτσι κι αλλιώς είναι πολύ χρονοβόρα διαδικασία) είναι γρηγορότερη από ότι με το EnCase. Αφού προσδιοριστούν τα ζητούμενα στοιχεία, το FTK προσφέρει τη δημιουργία αναφοράς για την καταγραφή της ανάλυσης και των διαδικασιών που χρησιμοποιήθηκαν, βοηθώντας έτσι τον ερευνητή να ”χτίσει” την υπόθεση του.
Διατίθεται στην ιστοσελίδα
`http://www.accessdata.com/support/\product-downloads`.

[1] Το EFS είναι μια δυνατότητα του NTFS που παρέχει κρυπτογράφηση σε επίπεδο συστήματος αρχείων. Είναι ενσωματωμένη σε όλες τις εκδόσεις Windows (από το Windows 2000 και μετά) και επιτρέπει κρυπτογράφηση αρχείων ή και ολόκληρων τόμων του δίσκου (disk volumes)

4.2 Εργαλεία Ελεύθερου Κώδικα

4.2.1 PyFlag

Το PyFlag είναι ένα γραφικό περιβάλλον βασισμένο σε Python κατασκευασμένο από τους Michael Cohen και David Collett για να υποστηρίξει την εξέταση ανόμοιων τύπων δεδομένων που συχνά συναντώνται στις σύγχρονες έρευνες ψηφιακής δικανικής. Αυτό το πετυχαίνει χρησιμοποιώντας ένα ενοποιημένο εικονικό σύστημα αρχείων (Virtual File System (VFS)) για όλα τα αντικείμενα που εξετάζονται. Κάθε ένα από αυτά, το PyFlag το θεωρεί έναν inode και κάθε αντικείμενο που προστίθεται του ανατίθεται ένα PyFlag inode. Επομένως οποιοσδήποτε αριθμός εικόνων συστημάτων αρχείων, καταγραφές διαδικτυακής κίνησης, μεμονωμένα αρχεία καταγραφής (log files) και ακόμα και σειρές μη δομημένων δεδομένων μπορούν να προστεθούν στο PyFlag. Τα αντικείμενα αυτά μπορούν να προσπελαστούν από σαρωτές με συγκεκριμένο σκοπό (π.χ να εξετάσουν αν είναι αρχεία του Outlook).

Το PyFlag χρησιμοποιείται για ανάλυση αρχείων καταγραφής (έχει ενσωματωμένη γνώση της δυαδικής δομής των αρχείων καταγραφής του Windows, επιτρέπει μόνο αναζητήσεις βασισμένες σε ευρετήρια, επεξεργάζεται διάφορα πρωτόκολλα του στρώματος εφαρμογών του διαδικτύου όπως SMTP και POP και αλληλεπιδρά με το Volatility Framework το οποίο χρησιμοποιείται για ανάλυση εικόνων μνήμης συστημάτων με Windows και Linux. Αντικείμενα που εξάγονται από καταγραφές διαδικτύου ή μνήμης μπορούν να εισαχθούν στο PyFlag και να δεχθούν περαιτέρω επεξεργασία από κατάλληλους σαρωτές.

Τέλος, ένα βασικό του πλεονέκτημα είναι ότι ουσιαστικά αποτελεί μια βάση δεδομένων που στηρίζεται στον παγκόσμιο ιστό, οπότε ο χρήστης γενικά χρειάζεται μόνο έναν περιηγητή ιστού για να χρησιμοποιήσει το εργαλείο. Έχει πλεονέκτημα απέναντι σε παραδοσιακά εργαλεία που χρησιμοποιούνται σε έναν υπολογιστή και από έναν χρήστη κάθε φορά, διότι μπορούν πολλοί χρήστες να δουλεύουν ταυτόχρονα στην ίδια υπόθεση ή σε διαφορετικές υποθέσεις.

Διατίθεται στην ιστοσελίδα `http://pyflag.sourceforge.net/Downloads/index.html`.

4.2.2 SleuthKit-Autopsy

Το **Sleuthkit** είναι μια συλλογή από εφαρμογές γραμμής εντολών που αρχικά δημιουργήθηκαν από τον Brian Carrier, που χρησιμοποιούνται για την ανάκτηση και ανάλυση δεδομένων. Χωρίζονται σε δύο κατηγορίες.

Στην πρώτη κατηγορία ανήκουν τα εργαλεία συστήματος αρχείων που επιτρέπουν την εξέταση των συστημάτων αρχείων ενός υπολογιστή. Δεν στηρίζονται στο λειτουργικό σύστημα για να επεξεργαστούν τα συστήματα αρχείων οπότε φαίνονται και διεγραμμένα αρχεία και κρυμμένα δεδομένα.

Στην δεύτερη κατηγορία ανήκουν τα εργαλεία του συστήματος τόμων (volume system tools) που επιτρέπουν την εξέταση της διάταξης δίσκων και άλλων αποθηκευτικών μέσων. Με τα εργαλεία αυτά μπορεί να προσδιοριστεί η θέσει των διαμερισμάτων στον δίσκο και να γίνει η εξαγωγή τους ώστε μετά να αναλυθούν από τα εργαλεία συστήματος αρχείων.

Το **Autopsy** είναι η διεπαφή για τα εργαλεία του Sleuthkit και ο συνδυασμός τους συνιστά μια αξιόλογη σουίτα για διεξαγωγή έρευνας στην ψηφιακή δικανική η οποία μάλιστα είναι εντελώς δωρεάν. Κάποιες από τις δυνατότητες της είναι:

- Αναγνώριση και προσπέλαση εικόνων dd, EWF και AFF.
- Προσπέλαση αρχείων συστήματος NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS,YAFFS2 και ISO 9660.
- Εργαλεία που ανιχνεύουν κακόβουλο λογισμικό τύπου Rootkit και μπορούν να εκτελεστούν σε ”ζωντανά” λειτουργικά συστήματα Unix και Windows και τα οποία δε μεταβάλλουν τις ημερομηνίες τροποποίησης και προσπέλασης των αρχείων.
- Προβολή των ADs(Alternate Data Streams).
- Προβολή λεπτομεριών για το σύστημα αρχείων και τα μεταδεδομένα του.
- Παρουσίαση των αρχείων σε κατηγορίες ανάλογα με τον τύπο τους (π.χ εκτελέσιμα αρχεία, εικόνες, βίντεο κτλ)
- Εξετάζει τιμές κατακερματισμού γνωστών αρχείων από την βάση δεδομένων της NIST ή κι από άλλες βάσεις.
- Δημιουργία timeline της δραστηριότητας των διαφόρων αρχείων του συστήματος.
- Εξάγει ιστορικό, cookies και σελιδοδείκτες από Internet Explorer, FireFox και Chrome.
- Δημιουργία αναφορών.

Το Sleuthkit και το Autopsy ανανεώνονται συνεχώς από την κοινότητα ελεύθερου λογισμικού και διατίθενται στην ιστοσελίδα `http://www.sleuthkit.org/`.

Κεφάλαιο 5

Εργαστήρια

Στο κεφάλαιο αυτό, φτιάξαμε τρία εργαστήρια ώστε να δούμε και στην πράξη πώς πραγματοποιούνται κάποιες από τις ενέργειες ενός αναλυτή της δικανικής υπολογιστών.

Στο πρώτο εργαστήριο, περιγράφεται η διαδικασία απόκτησης αντιγράφου μιας μνήμης USB μέσα από δύο διαφορετικά λειτουργικά συστήματα (Windows και Linux), και με χρήση διαφορετικών εργαλείων για το κάθε σύστημα.

Στο δεύτερο εργαστήριο, περιγράφονται λεπτομερώς οι ενέργειες που απαιτούνται για την ανίχνευση της δραστηριότητας ενός χρήστη, σε ένα σύστημα με Windows 7. Μελετάται ποικιλία πηγών του Windows 7 και παράλληλα κατασκευάζεται βήμα-βήμα ένα timeline της δραστηριότητας του χρήστη στο σύστημα. Δίνεται ένα σενάριο μαζί με ένα image δίσκου, ώστε να μπορούν τα βήματα να εφαρμοστούν στην πράξη και να επιβεβαιωθούν τα αποτελέσματα που δίνονται στην εργασία.

Στο τελευταίο εργαστήριο, αναλύονται πηγές ενός συστήματος Windows 7 που περιέχουν ίχνη σύνδεσης μιας USB μνήμης. Δίνεται και εδώ image δίσκου όπου εφαρμόζονται τα βήματα στην πράξη.

Στο τέλος κάθε εργαστηρίου, προτείνονται ασκήσεις για περαιτέρω μελέτη και εξάσκηση, οι οποίες μπορούν να εφαρμοστούν στα images που δίνονται στο αντίστοιχο εργαστήριο.

Για το δεύτερο και τρίτο εργαστήριο, η πλατφόρμα εργασίας (όπου εξετάζονται τα images) είναι ένα σύστημα με Windows 7.
Εγκαταστάθηκαν σε αυτήν τα εξής εργαλεία:

1. ActivePerl
2. Autopsy
3. Text Editor

4. LogParser

5. RegRipper

6. regslack.pl

7. tln _ tools

Τα εργαλεία που επιλέχθηκαν διατίθενται όλα ελεύθερα στο διαδίκτυο.

5.1 Αντίγραφο Δίσκου

Σκοπός: Εξοικείωση με την δημιουργία αρχείου-εικόνας (image file) ψηφιακών μέσων αποθήκευσης σε πλατφόρμες εργασίας Windows και Linux.
Εξοικείωση με τα εργαλεία dd, dcfldd, FTK Imager (έκδοση 3.2.0.0).
Εργαλεία: FTK Imager, dd, dcfldd.
Resources: USB μνήμη, Caine live CD.

5.1.1 Windows

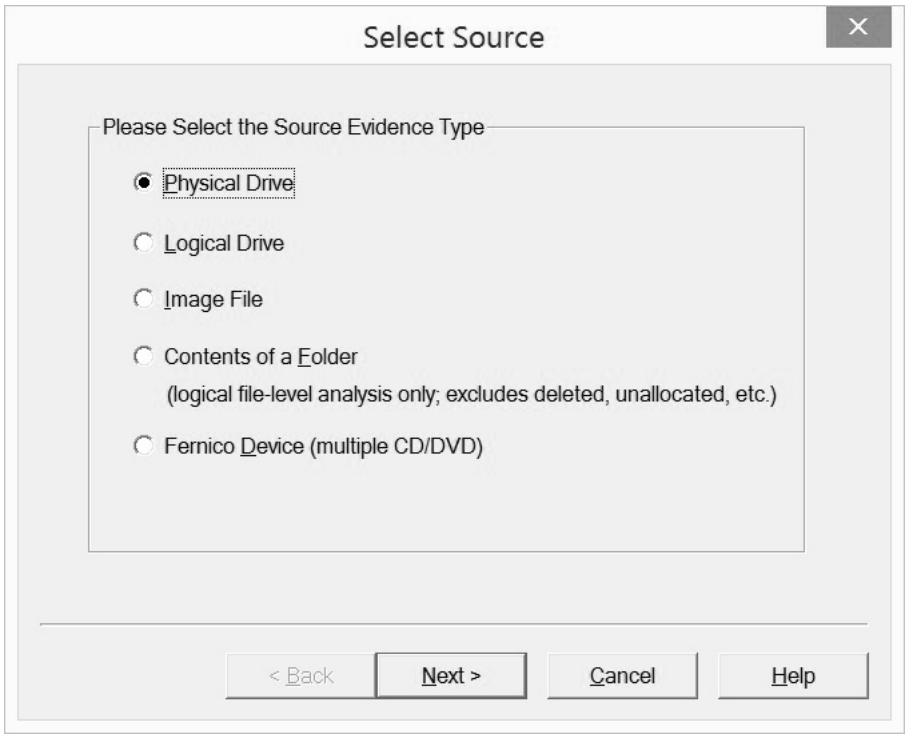
1. Δημιουργείστε αντίγραφο της USB μνήμης με το εργαλείο FTK Imager.[1]

2. Φτιάξτε ένα φάκελο εργασίας όπου θα αποθηκεύσετε το αντίγραφο του δίσκου. Για την παρακάτω περιγραφή τον ονομάσαμε ”C:/Work”.

3. Ανοίξτε τον FTK Imager ως διαχειριστής και επιλέξτε ”Create Disk Image” από το μενού File.

4. Στο κουτί ”Select Source” διαλόγου που θα εμφανιστεί επιλέξτε το είδος της πηγής που θέλετε να αντιγράψετε. Εδώ επιλέξτε ”Physical Drive”, δηλαδή αντιγραφή ολόκληρου του δίσκου.

[1] Σε μία πραγματική έρευνα η USB μνήμη θα έπρεπε επιπλέον να συνδεθεί σε έναν write blocker ώστε το σύστημα που εκτελεί την αντιγραφή, να μη γράψει δεδομένα σε αυτήν.



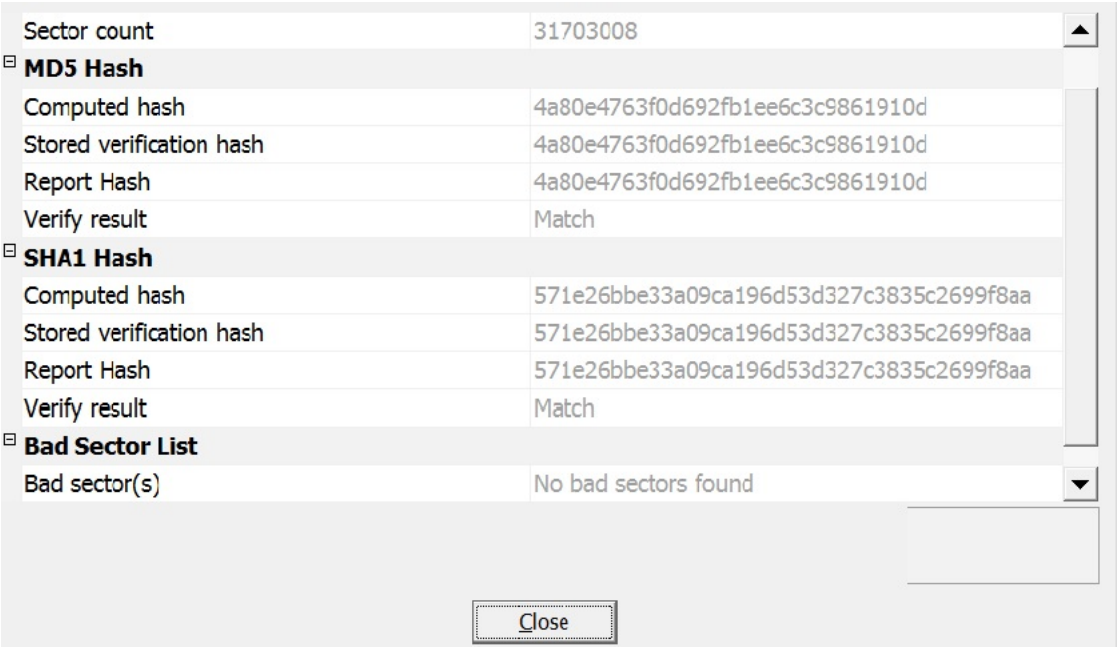
Σχήμα 5.1: Επιλογή είδους πηγής για αντιγραφή

5. Στο κουτί διαλόγου ”Select Drive” επιλέξτε τη USB μνήμη που θα αντιγράψετε.

6. Στο κουτί διαλόγου ”Create Image” επιλέξτε το κουμπί ”Add” και στο παράθυρο διαλόγου ”Select Image Type” επιλέξτε τον τύπο του αρχείου εικόνας που θα δημιουργηθεί (raw, AFF, E01 ή SMART). Επιλέξτε το E01 και πατήστε ”Next”.

7. Στο επόμενο παράθυρο συμπληρώνετε στοιχεία για τη συγκεκριμένη έρευνα και στο τελευταίο παράθυρο ”Select Image Destination” επιλέγετε τον φάκελο αποθήκευσης του αρχείου-εικόνας (εδώ C:/Work) και το όνομα του αρχείου. Πατήστε ”Finish” για να αρχίσει η δημιουργία της εικόνας.

8. Αφού τελειώσει η διαδικασία απόκτησης, εμφανίζεται το κουτί ”Disk/Image Verify Results” με τις τιμές κατακερματισμού για το αρχείο και το δίσκο όπου βλέπουμε ότι αυτές ταιριάζουν.



Σχήμα 5.2: Τιμές κατακερματισμού δίσκου και αρχείου

5.1.2 Linux

1. Συνδέστε στον υπολογιστή την USB μνήμη που θα αντιγράψετε και μία δεύτερη συσκευή αποθήκευσης ίσης χωρητικότητας με την USB μνήμη, σε ένα partition της οποίας θα αποθηκευθεί το αρχείο-εικόνα που θα δημιουργήσετε.

2. Εκκινήστε τον υπολογιστή σας από το Caine live CD (`http://www.caine-live.net/`) [2]

3. Ανοίξτε ένα τερματικό (terminal) ως root.

4. Με την εντολή fdisk -l παίρνετε μια λίστα με όλους τους δίσκους που υπάρχουν στο σύστημα. Ας υποθέσουμε ότι το partition του δίσκου αποθήκευσης είναι το /dev/sdd1 και της USB μνήμης το /dev/sdc1.

5. Εξετάστε την USB μνήμη για ύπαρξη HPA με το εργαλείο hdparm του Linux.

[2] Τώρα δεν απαιτείται write blocker αφού το Caine live CD είναι ειδικά διαμορφωμένη έκδοση Linux που προσαρτεί τα μέσα αποθήκευσης μόνο προς ανάγνωση

5.1. Για HPA εκτελέστε την παρακάτω εντολή:

Εντολή: hdparm -N /dev/sdc

5.2. Αν τα αποτελέσματα έχουν την παρακάτω μορφή, δεν υπάρχει HPA στη συσκευή!
/dev/sdc:
max sectors = 1465149168/1465149168, HPA is disabled

Σχόλιο: 1465149168 είναι οι τομείς που βλέπει ο χρήστης και 1465149168 οι συνολικοί τομείς της συσκευής. Εδώ οι τιμές συμπίπτουν και συμπεραίνεται η μη ύπαρξη HPA!

5.3. Αν όμως έχουν την παρακάτω μορφή, υπάρχει HPA στη συσκευή!

/dev/sdc:
max sectors = 586070255/586072368, HPA is enabled

Σχόλιο: 586070255 είναι οι τομείς που βλέπει ο χρήστης και 5860723688 οι συνολικοί τομείς της συσκευής. Εδώ οι τιμές δεν συμπίπτουν και συμπεραίνεται ύπαρξη HPA μεγέθους 2113 τομέων!

5.4. Στη δεύτερη περίπτωση, πρέπει να αφαιρέσετε πρώτα την HPA με κάποιο εργαλείο όπως το hdparm.

Εντολή: hdparm -N p586072368 /dev/sdc

6. Υπολογίστε μία τιμή κατακερματισμού του partition της USB μνήμης με το ενσωματωμένο εργαλείο md5sum του Linux.

7. Προετοιμάστε το φάκελο που θα αποθηκευθεί το αρχείο-εικόνα

7.1. Δημιουργείστε στον φάκελο mnt του Linux, ένα φάκελο με όνομα sdd1 και κάντε mount το partition αποθήκευσης.

Εντολή: mount /dev/sdd1 /mnt/sdd1

7.2. Στον φάκελο /mnt/sdd1 που έγινε το mount, δημιουργήστε ένα φάκελο με όνομα img _ lab1 για να αποθηκεύσετε το αρχείο.

8. Φτιάξτε και πιστοποιείστε το αρχείο-εικόνα.

8.1. Χρησιμοποιήστε το εργαλείο dd για τη δημιουργία του αρχείου-εικόνας.

Εντολή: dd if=/dev/sdc1 of=/mnt/sdd1/img _ lab1/lab1.dd

8.2. Το dd δεν έχει ενσωματωμένο υπολογισμό τιμών κατακερματισμού, οπότε υπολογίστε την τιμή αυτή για το αρχείο-εικόνα που δημιουργήσατε με το ενσωματωμένο εργαλείο md5sum του Linux. Συγκρίνετε

την τιμή αυτή με την τιμή που υπολογίσατε στο βήμα 5 για να βεβαιωθείτε ότι η εικόνα πάρθηκε σωστά.

Εντολή: md5sum /mnt/sdd1/img _ lab1/lab1.dd

8.3. Τέλος υπολογίστε ξανά την τιμή κατακερματισμού του δίσκου για επιβεβαίωση ότι δεν έγινε κάποια τροποποίηση σε αυτόν κατά την διάρκεια της απόκτησης.

5.1.3 Επιπλέον Ασκήσεις

1. Στο περιβάλλον Linux, ελέγξτε την ύπαρξη τμήματος DCO στην USB μνήμη.

   Υπόδειξη: Εργαλείο hdparm και όρισμα –dco-identify.

2. Στο περιβάλλον Linux, πάρτε την εικόνα της USB μνήμης με το εργαλείο dcfldd. Ποια από τα παραπάνω βήματα είναι περιττά;

   Υπόδειξη: Το dcfldd έχει ενσωματωμένη δυνατότητα υπολογισμού τιμών κατακερματισμού!

3. Σε Windows, αποκτήστε την εικόνα της USB μνήμης με χρήση του εργαλείου dd για Windows. Τι αλλάζει σε σχέση με την εφαρμογή του εργαλείου σε Linux; Τι επιπλέον χρειάστηκε να κάνετε που δεν απαιτήθηκε με τον FTK Imager;

   Υπόδειξη: Το μονοπάτι (path) του partition αλλάζει και απαιτείται υπολογισμός τιμών κατακερματισμού με εξωτερικά εργαλεία όπως κάποιος hex editor ή τα εργαλεία md5deep.exe, sha1deep.exe.

5.2 Ανίχνευση Δραστηριότητας Χρήστη

Σκοπός: Εξοικείωση με την ανίχνευση ενεργειών που πραγματοποιήθηκαν στο λειτουργικό σύστημα Windows 7 και οι οποίες σχετίζονται με τον λογαριασμό ενός συγκεκριμένου χρήστη (tracking user activity).
Εξοικείωση με την δημιουργία timeline της δραστηριότητας ενός συστήματος.
Εξοικείωση με τα εργαλεία Regripper, LogParser, Autopsy.

Εργαλεία: Regripper, LogParser, Autopsy

Σενάριο: Υπάρχει υποψία ότι ο υπάλληλος Alice επεξεργάστηκε παράνομες εικόνες και βίντεο μέσω ενός υπολογιστή της εταιρείας την ημέρα 19 Αυγούστου 2014. Δίνεται το image του partition του υπολογιστή που χρησιμοποιούσε η Alice

με Windows 7. Για τους σκοπούς της άσκησης, οι ”παράνομες” εικόνες έχουν θεματολογία ”Υπολογιστής” και τα βίντεο είναι πανεπιστημιακές διαλέξεις.

5.2.1 Εργαστήριο

1. Φτιάξτε ένα φάκελο εργασίας όπου θα αποθηκεύετε κάθε αρχείο ή φάκελο που θα χρειαστεί να εξάγετε από το δοθέν image. Για την παρακάτω περιγραφή τον ονομάσαμε ”C:/Work”.

   Μπορείτε να εξάγετε αρχεία του image, φορτώνοντας το σε ένα πρόγραμμα όπως ο FTK imager ή το Autopsy.

2. Προσδιορίστε την έκδοση του Windows που χρησιμοποιείται ώστε στη συνέχεια να χρησιμοποιήσετε κατάλληλες πηγές στοιχείων και εργαλεία. Το κλειδί Microsoft \Windows NT \CurrentVersion του System hive αποθηκεύει την πληροφορία αυτή. Εξάγετε την με το winnt_ cv plugin του Regripper.

   Εντολή: rip -r C:/Work/system -p winnt_ cv.

   Αποτέλεσμα: Windows 7 Ultimate

3. Βρείτε τη ζώνη ώρας (time zone) του συστήματος ώστε να ξέρετε την τοπική ώρα κάθε συμβάντος. [3]Το κλειδί Microsoft \CurrentControlSet\Control TimeZoneInformation του System hive αποθηκεύει την πληροφορία αυτή. Εξάγετε την με το timezone plugin του Regripper.

   Εντολή: rip -r C:/Work/system -p timezone.

   Αποτελέσματα:

   LastWrite Time Mon Aug 18 11:54:34 2014 (UTC)

   DaylightName -> @tzres.dll,-361
   StandardName -> @tzres.dll,-362
   Bias -> -120 (-2 hours)
   ActiveTimeBias -> -180 (-3 hours)
   DaylightBias -> -60 (-1 hours)
   TimeZoneKeyName -> GTB Standard Time

[3]Δεν έχει σημασία η τοποθεσία του υπολογιστή, η ζώνη ώρας μπορεί να έχει ορισθεί διαφορετικά.

Note: Bias (daylight not considered) and ActiveTimeBias (daylight considered) are values with sign that must be added to localtime to get UTC time

Η τοπική ώρα του υπολογιστή είναι +2 ώρες από τον UTC (μεταβλητή Bias) αλλά πρέπει να ληφθεί υπόψη και η θερινή ώρα (daylight saving) η οποία φαίνεται στη μεταβλητή DaylightBias. Τελικώς για να βρούμε την ώρα σε UTC θα προσθέτουμε 3 ώρες και ανάποδα για την τοπική ώρα θα αφαιρούμε 3 ώρες από τον UTC.

4. Βρείτε τους χρήστες που είχαν λογαριασμό στο σύστημα.

   4.1. Η πληροφορία αυτή υπάρχει στο κλειδί Users στον SAM hive του Registry. Εξάγετε την με το samparse.pl plugin του Regripper.

   Εντολή: rip -r C:/Work/SAM -p samparse.pl

   4.2. Στα αποτελέσματα θα βρείτε τους χρήστες Guest, ALICE και Administrator.

5. Εξάγετε από το image του δίσκου τα αρχεία εικόνας και βίντεο που περιέχει συμπεριλαμβανομένου και των διαγραμμένων αρχείων (όσων μπορούν να ανακτηθούν). Εντοπίστε τις ύποπτες εικόνες και βίντεο και προσδιορίστε τα timestamps τους. Τι παρατηρείτε;

   5.1. Εκτελέστε το Autopsy ως διαχειριστής, δημιουργείστε μία νέα υπόθεση και προσθέστε το image που σας δίνεται.

   5.2. Στο αριστερό τμήμα του κυρίως παραθύρου του προγράμματος, επεκτείνετε το αντικείμενο Views και μετά το File Types. Η υπόθεση αφορά εικόνες και βίντεο, οπότε επιλέξτε τα αντικείμενα Images και Videos και αναζητείστε τα ”παράνομα” αρχεία.

   5.3. Εντοπίστηκαν οι εικόνες laptop.jpg, desktop.png, network.jpg, office_ PCs.bmp και cartoon_ pc.png και τα βίντεο lecture1.mp4 και lecture2.mp4 στον φάκελο C:\Users\Public\images.

   5.4. Από τα timestamps των υπό εξέταση αρχείων παρατηρούμε ότι αυτά δημιουργήθηκαν, τροποποιήθηκαν και αποκτήθηκε πρόσβαση σε αυτά για τελευταία φορά (created, modified και access time) την 22/08/2013, δηλαδή πολύ καιρό πριν το δοθέν διάστημα (19/08/2014).

   Ερώτημα: Μπορούμε να συμπεράνουμε ότι τελικά ο χρήστης Alice δεν σχετίζεται με την δημιουργία κι επεξεργασία των συγκεκριμένων αρχείων;

Απάντηση: ΟΧΙ! Οι ημερομηνίες αυτές είναι τα timestamps του γνωρίσματος $STANDARD_ INFORMATION ($SIA) της MFT εγγραφής του αντίστοιχου αρχείου και είναι πολύ εύκολο να τροποποιηθούν με μία anti-forensic τεχνική που καλείται ”timestomping”. Επιπλέον οι ημερομηνίες τροποποίησης της MFT εγγραφής των αρχείων (Change Time) θα έπρεπε να ταιριάζουν με τα υπόλοιπα timestamps. Όμως είναι άσχετες και μάλιστα ταιριάζουν με το δοθέν διάστημα! Απαιτείται ΟΠΟΣΔΗΠΟΤΕ περαιτέρω διερεύνηση των αρχείων και του συστήματος γενικότερα για να καταλήξουμε σε συμπεράσματα.

5.5. Για τον εντοπισμό πιθανού timestomping μπορούμε να συγκρίνουμε τα timestamps του $SIA με αυτά του γνωρίσματος $FILE_ NAME ($FNA) της MFT εγγραφής του κάθε αρχείου καθώς ξέρουμε ότι τα τελευταία είναι πιο δύσκολο να τροποποιηθούν[3].

5.5.1. Εξάγετε από το image το $MFT αρχείο που βρίσκεται στον φάκελο ρίζα του συστήματος (root) και αποθηκεύστε τον στο φάκελο εργασίας σας.

5.5.2. Με το πρόγραμμα analyzeMFT.py, αποθηκεύστε τα περιεχόμενα του MFT σε ένα αρχείο Excel.

Εντολή: analyzeMFT.py -f C:\Work \$ MFT -c C:\Work \mft.csv

5.5.3. Αναζητείστε με βάση το όνομα τα αρχεία που εντοπίσατε στα βήματα 2.1-2.3 και βρείτε τα timestamps του γνωρίσματος $FNA τους.

5.5.4. Φαίνεται ότι τα timestamps του γνωρίσματος $FNA δεν συμπίπτουν με αυτά του $SIA και μάλιστα βρίσκονται εντός του δοθέντος διαστήματος που σημαίνει ότι έχει γίνει προσπάθεια απόκρυψης πληροφοριών σχετικά με τα υπό εξέταση αρχεία! Συνεχίζουμε την εξέταση του συστήματος για να ανακαλύψουμε τι συνέβη τελικά με αυτά!

6. Κατασκευάστε ένα timeline των γεγονότων που συνέβησαν στο σύστημα το δοθέν διάστημα, συνδυάζοντας πολλαπλές πηγές σχετικά με την δραστηριότητα του χρήστη.

Υπενθύμιση: Πρώτα κατασκευάζουμε ένα ενδιάμεσο αρχείο (ονομάστε το events.txt) σε μορφή TLN που συγκεντρώνει τα γεγονότα από όλες τις πηγές και μετά το επεξεργαζόμαστε και δημιουργούμε το τελικό timeline.

7. Προσθέστε στο events.txt, συνδέσεις χρηστών στο σύστημα το δοθέν διάστημα ώστε να βρεθεί ποιος λογαριασμός χρήστη ήταν συνδεδεμένος το διάστημα που συνέβαιναν γεγονότα ενδιαφέροντος και για πόσο.
   Θα επιβεβαιωθεί ότι το δοθέν διάστημα κάποιος χρήστης συνδέθηκε τοπικά (μέσω του πληκτρολογίου) και όχι με απομακρυσμένη πρόσβαση στο σύστημα.

   7.1. Συνδέσεις και αποσυνδέσεις βρίσκονται στο log αρχείο Security.evtx του Windows 7. Εξάγετε το από το φάκελο C:\Windows \System32 \winevt \Logs του image και αποθηκεύστε το στο φάκελο εργασίας σας.

   7.2. Με τον LogParser εκτελέστε το παρακάτω SQL ερώτημα για να πάρετε όλες τις εγγραφές με Event ID 4624 (σύνδεση) ή 4647 (αποσύνδεση) και για τις οποίες, στην περίπτωση του γεγονότος σύνδεσης, ο τύπος[4]του γεγονότος να είναι 2 (σύνδεση μέσω πληκτρολογίου) ,3 (σύνδεση μέσω διαδικτύου π.χ σε κοινούς φακέλους) ή 10 (σύνδεση απομακρυσμένα) [5]

   Εντολή: logparser -i:evt -o:csv

   *"**SELECT** EventLog, RecordNumber,*
   TO_ UTCTIME(TimeGenerated) as "TimeGenerated",
   TO_ UTCTIME(TimeWritten) as "TimeWritten",
   EventID, EventType, EventTypeName,
   EventCategory, EventCategoryName, SourceName,
   Strings, ComputerName, SID, Message, Data,
   EXTRACT_ TOKEN(Strings,8,'|') as Logon_ type
   ***FROM** C:\Work\Security.evtx*
   ***WHERE** ((EventID=4624) AND (Logon_ type in ('2';'3';'10')))*
   OR (EventID=4647)"
   > C:\Work\security.csv

8. **Προσπέλαση αρχείων από το χρήστη**

   Ξεκινήστε εντάσσοντας στο events.txt πιθανές πηγές ενδείξεων του ποιοι χρήστες προσπέλασαν τα παράνομα αρχεία και πότε.

---

[4]Λίστα με ακριβή περιγραφή των τύπων γεγονότος σύνδεσης θα βρείτε στην `http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624`

[5]Όταν ένας χρήστης συνδέεται, δημιουργούνται πολλά, διαφορετικού τύπου, γεγονότα σύνδεσης. Κρατήσαμε αυτά που μας ενδιαφέρουν περισσότερο στην υπόθεση αυτή για να έχουμε ένα λιτό και καθαρό timeline

8.1. Το κλειδί RecentDocs του NTUSER.dat hive αποθηκεύει αρχεία (ανά τύπο αρχείου) που προσπέλασε ο αντίστοιχος χρήστης και τη σειρά προσπέλασης για τον κάθε τύπο. Εισάγετε στο events.txt τα περιεχόμενα του RecentDocs με το recentdocs_ tln.pl plugin του Regripper αφού εξάγετε τον NTUSER.dat από το δοθέν image (βρίσκεται στο προφίλ του χρήστη Alice).

Εντολή: rip -r C:/Work/ntuser.dat -p recentdocs_ tln.pl.pl -u User -s SERVER » C:/Work/events.txt

Όπου User είναι ο χρήστης (εδώ ALICE) και SERVER το όνομα του υπολογιστή (εδώ ALICE-PC) το οποίο βρίσκεται από τον System hive με το compname.pl plugin του Regripper.

8.2. ShellBags είναι ένα σύνολο κλειδιών του USRCLASS.dat hive που αποθηκεύουν ρυθμίσεις που έκανε ο χρήστης σε παράθυρα που άνοιξε με τον Windows Explorer και άρα από αυτά εξάγονται συμπεράσματα για φακέλους και αρχεία που έχει ανοίξει ο χρήστης. Προσθέστε πληροφορίες από αυτά στο events.txt (όπως παραπάνω) με το shellbags_ tln.pl plugin του Regripper αφού εξάγετε τον USRCLASS.dat από το δοθέν image (path: AppData\Local \Microsoft \Windows).

8.3. Το κλειδί TypedPaths του NTUSER.dat αποθηκεύει μονοπάτια (paths) που πληκτρολογεί ο χρήστης στην μπάρα του Windows Explorer . Εισάγετε στο events.txt τα περιεχόμενα του TypedPaths με το typedpaths_ tln.pl plugin του Regripper.

8.4. Η εφαρμογή MS Paint του NTUSER.dat αποθηκεύει στο Registry τα πρόσφατα ανοιγμένα αρχεία της. Εισάγετε στο events.txt με το applets _ tln.pl plugin του Regripper.

9. **Εκτέλεση Εφαρμογών από το χρήστη**

Συμπεριλάβετε στο events.txt πιθανές πηγές ενδείξεων για εφαρμογές που έτρεξαν στο σύστημα από συγκεκριμένους χρήστες. Έτσι θα προσδιοριστούν και θα επιβεβαιωθούν ενέργειες χρηστών σχετικά με τα παράνομα αρχεία (π.χ προβολή, μεταφορά εκτός υπολογιστή).

9.1. Το κλειδί UserAssist του NTUSER.dat αποθηκεύει πληροφορίες για προγράμματα που έχει τρέξει ο χρήστης μέσω του Windows Explorer ή μενού προγραμμάτων. Εισάγετε στο events.txt τα περιεχόμενα του UserAssist με το userassist_ tln.pl plugin του Regripper.

9.2. Τα Prefetch αρχεία δείχνουν πότε μια εφαρμογή έτρεξε για τελευταία φορά και πόσες φορές έχει τρέξει. Δεν συνδέονται άμεσα με κάποιον χρήστη, όμως συνδυάζοντας τα με γεγονότα που συνέβησαν σε κοντινούς χρόνους μπορούν να εξαχθούν/επιβεβαιωθούν συμπεράσματα και για τις ενέργειες ενός χρήστη. Εισάγετε στο events.txt τα περιεχόμενα του φακέλου Prefetch με το εργαλείο pref.pl αφού τον εξάγετε από το δοθέν image.

Εντολή: pref.pl -d C:/Work/Prefetch -v -t -s SERVER » C:/Work/events.txt

Σχόλιο: Με το όρισμα -f ακολουθούμενο από το αντίστοιχο μονοπάτι, θα μπορούσαμε να επεξεργαστούμε ένα μόνο prefetch αρχείο και όχι όλα τα αρχεία του Prefetch φακέλου.

9.3. Τα κλειδιά Direct* του Software hive, είναι κλειδιά που το όνομά τους αρχίζει από ”Direct” όπως Direct3D, DirectDraw κτλ. Μπορεί να αποθηκεύουν την τελευταία εφαρμογή που χρησιμοποίησε τα συγκεκριμένα γραφικά. Εισάγετε στο events.txt τα περιεχόμενα των Direct* με το direct_ tln.pl plugin του Regripper.
Όπως και τα prefetch αρχεία, δε συνδέονται άμεσα με κάποιον χρήστη, όμως μπορούν να αξιοποιηθούν συνδυαστικά.

9.4. Το κλειδί Tracing του Software hive, μπορεί να περιλαμβάνει αναφορές σε εφαρμογές που φαίνεται να έχουν δικτυακές δυνατότητες. Εισάγετε στο events.txt τα περιεχόμενα του Tracing με το tracing_ tln.pl plugin του Regripper. Και το κλειδί tracing δε συνδέεται άμεσα με κάποιον χρήστη, όμως μπορεί να αξιοποιηθεί συνδυαστικά.

10. Μελετήστε επιπλέον στοιχεία δραστηριότητας του χρήστη που δεν μπορούν να μπουν αυτοματοποιημένα στο timeline. Αν βρείτε στοιχείο ενδιαφέροντος που να διαθέτει χρονική πληροφορία, μπορείτε να το βάλετε στο timeline μεμονωμένα, με το εργαλείο γραφικού περιβάλλοντος tln.pl.

10.1. Προσπέλαση αρχείων από το χρήστη

10.1.1. Το κλειδί WordWheelQuery του NTUSER.dat αποθηκεύει πληροφορίες για προγράμματα που έχει τρέξει ο χρήστης μέσω του Windows Explorer ή μενού προγραμμάτων. Εξάγετε το wordwheelquery κλειδί με το wordwheelquery.pl plugin του Regripper.

Αποτελέσματα:

wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

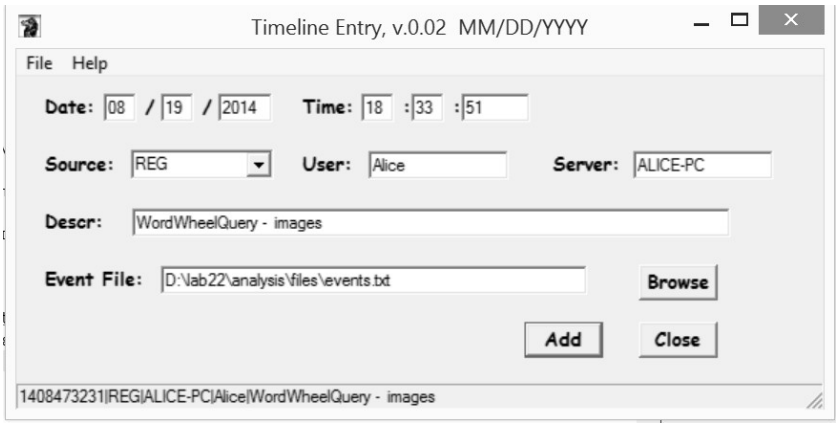
Software\Microsoft
Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Tue Aug 19 18:33:51 2014 (UTC)

Searches listed in MRUListEx order

2 images
1 ftp.exex
0 infraview

Ο χρήστης αναζήτησε πρώτα την λέξη infraview, μετά το ftp.exe πληκτρολογώντας το λάθος και τέλος τη λέξη images που λογικά αναφέρεται στο φάκελο με τα "ύποπτα" αρχεία. Τα αποτελέσματα είναι σε σειρά MRUListEx [6] άρα τελευταία αναζήτηση ήταν της λέξης images. Ο χρόνος LastWrite του κλειδιού μας δείχνει πότε αυτό τροποποιήθηκε για τελευταία φορά και άρα, στο συγκεκριμένο κλειδί, πότε έγινε η τελευταία αναζήτηση (εδώ στις 19/08/2014 και ώρα 18:33:51 (UTC)). Προσθέστε την πληροφορία αυτή στο timeline με το tln.pl δίνοντας την ημερομηνία, την πηγή της πληροφορίας και την περιγραφή (σχήμα 5.3).

[6] Υπενθυμίζεται ότι MRUList ή MRUListEx είναι μια λίστα που διατηρεί τη σειρά που διάφορες τιμές χρησιμοποιήθηκαν (ανάλογα με την εφαρμογή στην οποία αναφέρεται).



Σχήμα 5.3: Εισαγωγή εγγραφής στο timeline από το WordWheelQuery με το tln.pl

10.1.2. Το κλειδί Comdlg32 του NTUSER.dat αναφέρεται σε συνηθισμένους διαλόγους που είναι διαθέσιμοι στο Windows όπως οι ”Open and Save as” διάλογοι. Εξάγετε το Comdlg32 κλειδί με το comdlg32.pl plugin του Regripper.

Αποτελέσματα:
Στα αποτελέσματα θα βρείτε τα εξής κλειδιά:
Το CIDSizeMRU περιέχει εφαρμογές που έτρεξε πρόσφατα ο χρήστης.
Το OpenSavePidMRU ανιχνεύει αρχεία που προσπέλασε ο χρήστης με Open and Save As διαλόγους. Περιέχει, για λόγους πληρότητας, αρχεία που αποθηκεύτηκαν ή απλώς ανοίχτηκαν πρόσφατα.
Για κάθε τύπο αρχείου υπάρχει ένα υποκλειδί του OpenSavePidMRU (π.χ το penSavePidMRU\jpeg) που περιέχει αρχεία που ανοίχθηκαν ή αποθηκεύθηκαν.
Στο υποκλειδί OpenSavePidMRU* περιλαμβάνει από τον κάθε τύπο αρχείου, τα αρχεία που προσπελάστηκαν πιο πρόσφατα.
Το LastVisitedPidlMRU κλειδί ανιχνεύει την εφαρμογή που χρησιμοποιήθηκε τελευταία για να ανοιχθεί ο διάλογος και να προσπελαστούν τα αρχεία που αναφέρονται στο OpenSavePidMRU και στα υποκλειδιά του καθώς και τον φάκελο που προσπελάστηκε από την εφαρμογή.
Ένα τμήμα του αποτελέσματος από το Comdlg32 είναι το εξής:

LastVisitedPidlMRU

LastWrite: Tue Aug 19 14:10:13 2014
Note: All value names are listed in MRUListEx order.

mspaint.exe - My Computer\G:
iexplore.exe - Users

OpenSavePidlMRU
LastWrite: Tue Aug 19 14:09:53 2014
*OpenSavePidlMRU**
LastWrite Time: Tue Aug 19 14:10:13 2014
Note: All value names are listed in MRUListEx order.

My Computer\G:\3images.jpg
Users\iview438_ setup.exe
Users\7z922.exe

Βλέπουμε το εξής ενδιαφέρον: Από το LastVisitedPidlMRU, τελευταία εφαρμογή που χρησιμοποιήθηκε για τα αρχεία του OpenSavePidMRU είναι η MS Paint στις 19/08/2014 και ώρα 14:10:13(UTC), και μάλιστα για να προσπελάσει μία εξωτερική συσκευή συνδεδεμένη στο γράμμα G. Από το OpenSavePidMRU* βλέπουμε ότι το αρχείο που ανοίχθηκε ή αποθηκεύτηκε στην εξωτερική συσκευή λέγεται 3images.jpg. Προσθέστε την πληροφορία αυτή στο timeline σας με το tln.pl όπως παραπάνω.

10.1.3. Οι Jump Lists είναι λίστες με αρχεία που ανοίχτηκαν πρόσφατα από το χρήστη μέσω συγκεκριμένων εφαρμογών.
Εξάγετε από το image τον φάκελο στον οποίο βρίσκονται (στο προφίλ χρήστη στον φάκελο AppData \Roaming \Microsoft \ Windows \Recent \AutomaticDestinations).
Εισάγετε στο εργαλείο JumpLister ένα-ένα τα αρχεία του φακέλου.
Σε κάθε αρχείο jump list εμφανίζεται το όνομα της εφαρμογής, μια ταξινομημένη λίστα με τα αρχεία που έχουν ανοιχθεί ξεκινώντας από το πιο πρόσφατα ανοιγμένο αρχείο και το τμήμα DestList στο οποίο υπάρχει το πεδίο Date/Time και δίνει, για κάθε ανοιγμένο αρχείο, την τελευταία φορά που ανοίχτηκε με την εφαρμογή αυτή.
Ενδιαφέρον στο συγκεκριμένο σενάριο έχουν οι λίστες των εφαρμογών InfraView, MS Paint και Windows Media Player. Μπορείτε να εισάγετε χρονικές πληροφορίες από αυτές στο timeline με το tln.pl.

10.2. **Εκτέλεση Εφαρμογών από το χρήστη**

10.2.1. Το κλειδί MUIcache του USRCLASS.DAT (Για Windows XP και πίσω βρίσκεται στον NTUSER.dat) συχνά περιέχει αναφορές σε εφαρμογές που έτρεξαν από έναν χρήστη (ακόμα κι αν αυτές έχουν διαγραφεί από το σύστημα). Μπορεί να περιέχει ενδείξεις ακόμα και εργαλεία γραμμής εντολών ή για εργαλεία που εκτελούνται από εξωτερική συσκευή. [7] Εξάγετε το MUIcache κλειδί με το muicache.pl plugin του Regripper.

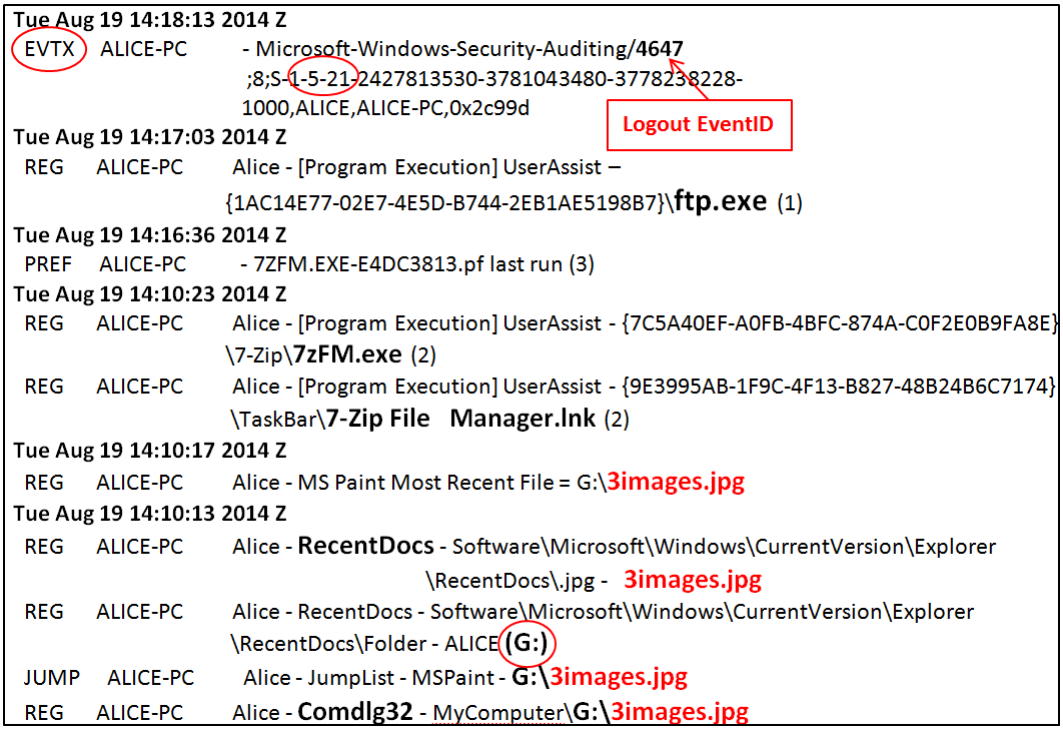
10.2.2. Το κλειδί AppCompatFlags του NTUSER.dat περιέχει πληροφορίες για εφαρμογές που εκτελέστηκαν από τον χρήστη μέσω του βοηθού συμβατότητας προγράμματος
(Program Compatibility Assistant)[8] Εξάγετε το AppCompatFlags κλειδί με το appcompatflags.pl plugin του Regripper.

11. Δημιουργείτε το τελικό timeine από το events.txt.
Εντολή: parse.pl -f
C:/Work/events.txt -r 08/19/2014-08/19/2014 » C:/Work/timeline.txt

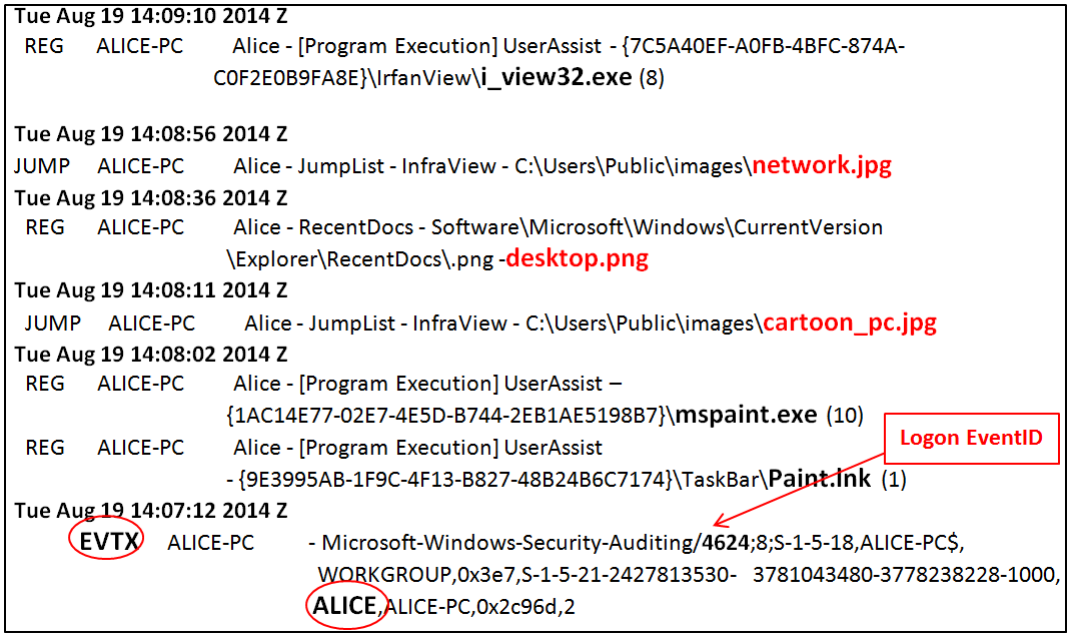
12. Ακολουθεί μέρος των αποτελεσμάτων του timeline. Για την καλύτερη παρουσίασή του, αφαιρέσαμε κάποιες εγγραφές γεγονότων (χωρίς σημασία).

[7] Το μόνο timestamp που περιέχει είναι το LastWrite του ίδιου του κλειδιού και όχι ένα timestamp για την κάθε εφαρμογή που έχει καταγράψει. Ενδείξεις για το πότε έτρεξαν οι εφαρμογές αυτές μπορούν να βρεθούν συνδυαστικά με άλλες πηγές όπως το UserAssist και τα prefetch.

[8] Χρησιμοποιείται για να προσδιορίσει αν ένα πρόγραμμα πρέπει να εκτελεστεί σε λειτουργία Windows XP (Windows XP mode) ακόμα κι αν δεν εφαρμόστηκε τελικά σε αυτά κάποια λειτουργία συμβατότητας.



Σχήμα 5.4: Πρώτο τμήμα του timeline.



Σχήμα 5.5: Δεύτερο τμήμα του timeline.

Σχόλια: Στο σχήμα 5.5 φαίνεται ένα γεγονός σύνδεσης του χρήστη Alice στις 14:07:12. Αμέσως μετά, στις 14:08:02 βλέπουμε δύο εγγραφές από το κλειδί UserAssist που δείχνουν την εκτέλεση της εφαρμογής MS Paint. Λίγα δευτερόλεπτα αργότερα, εκτελείται η εφαρμογή infraview κι έχουμε την προβολή με το infraview δύο ”παράνομων” αρχείων (network.jpg, cartoon_pc .jpg), όπως φαίνεται από τις εγγραφές της jump list της εφαρμογής αυτής. Επίσης έχουμε και το άνοιγμα του desktop.png (εγγραφή του RecentDocs κλειδιού). Προφανές συμπέρασμα είναι ότι ο χρήστης Alice γνώριζε την ύπαρξη των ”παράνομων” εικόνων και βλέπουμε πότε και με τι εφαρμογές τις προσπέλασε.

Στο σχήμα 5.6, βλέπουμε στις 14:10:13, από εγγραφές του κλειδιού RecentDocs και από μια εγγραφή της Jump List του MS Paint, ένα νέο όνομα αρχείου (3images.jpg) που προσπελάστηκε από έναν τόμο (volume) με γράμμα G. Επιπλέον υπάρχει και μία εγγραφή του κλειδιού Comdlg32 (διάλογοι Open and Save as) που αναφέρεται στο αρχείο 3images.jpg. Αυτό μας υποψιάζει αμέσως ότι ο χρήστης ίσως επεξεργάστηκε τις εικόνες με το MS Paint ή το infraview και αμέσως μετά έσωσε μία νέα εικόνα σε εξωτερική συσκευή (προσαρτημένη στο γράμμα G). Στη συνέχεια από το UserAssist και ένα Prefetch αρχείο, βλέπουμε την εκτέλεση της εφαρμογής 7-zip και μετά από κάποια λεπτά την εκτέλεση του ftp.exe. Συμπεραίνουμε ότι, με μεγάλη πιθανότητα, ο χρήστης συμπίεσε τις παράνομες εικόνες και προσπάθησε να τις στείλει σε κάποιο άλλο σύστημα.

5.2.2 Επιπλέον Ασκήσεις

1. Στο timeline που κατασκευάσατε, εντοπίσατε γεγονότα σύνδεσης στο σύστημα από έναν χρήστη με όνομα Bob ο οποίος δεν υπήρχε στη λίστα με τους χρήστες που έχουν λογαριασμό στο σύστημα και την οποία είδαμε στον Sam hive. Τι μπορεί να σημαίνει αυτό; Τι συμπεράσματα βγαίνουν για τον Bob από το timeline της δραστηριότητας της Alice που φτιάξατε;

   Υπόδειξη: Εξάγετε τον ελεύθερο χώρο του SAM hive με το εργαλείο regslack.

5.3 Ίχνη Συσκευής USB

Σκοπός: Εξοικείωση με τις ενέργειες που απαιτούνται ώστε να βρεθούν τα ίχνη της χρήσης μιας USB μνήμης (ή άλλου προσωρινού μέσου αποθήκευσης) σε έναν υπολογιστή.

Εξοικείωση με τα εργαλεία RegRipper και LogParser.

Εργαλεία: Regripper, LogParser

Resources: Δίνεται μία μνήμη USB Transcend των 4GB που περιέχει ευαίσθητα αρχεία κειμένου.

5.3.1 Εργαστήριο

1. Φτιάξτε ένα φάκελο εργασίας όπου θα αποθηκεύετε κάθε αρχείο που θα δημιουργήσετε ή που θα χρειαστεί να εξάγετε από το δοθέν image. Για την παρακάτω περιγραφή τον ονομάσαμε "C:/Work".

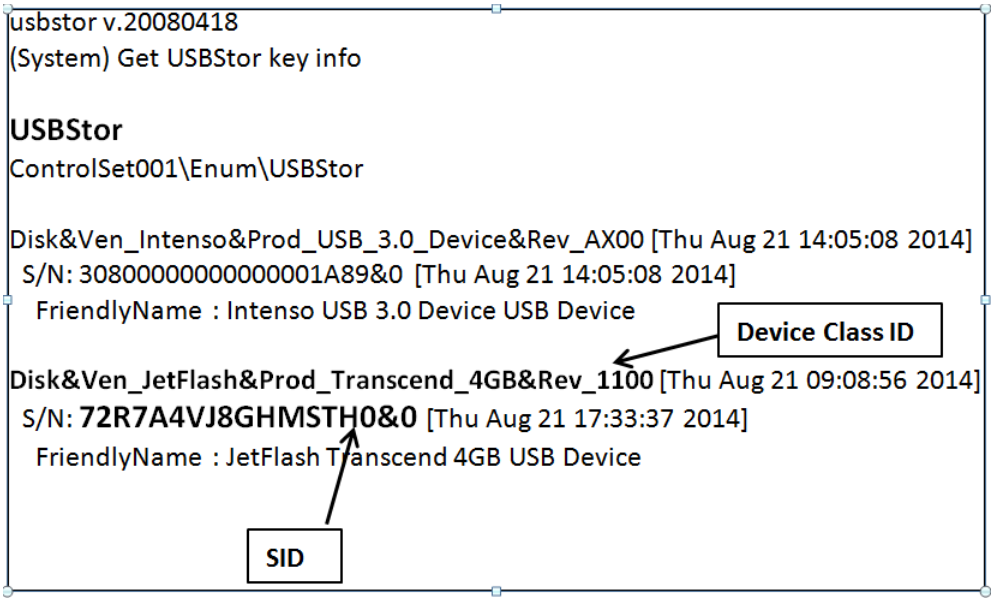
2. Ελέγξτε αν η υπό εξέταση μνήμη usb έχει συνδεθεί στον συγκεκριμένο υπολογιστή και προσδιορίστε βασικά χαρακτηριστικά της. Συγκεκριμένα βρείτε τον κατασκευαστή (vendor), την έκδοση (version) της συσκευής και τα ID του προϊόντος και του κατασκευαστή (product και vendor IDs). Επιπλέον προσδιορίστε τον σειριακό αριθμό (SID) [9] της συσκευής ο οποίος θα βοηθήσει στην αντιστοίχηση της με άλλα σημαντικά στοιχεία της ανάλυσής σας.

   2.1. Πρώτο βήμα είναι η επιβεβαίωση ότι η υπό εξέταση μνήμη USB έχει συνδεθεί στο σύστημα. Πληροφορία για όλες τις αφαιρούμενες συσκευές αποθήκευσης USB που έχουν συνδεθεί στο σύστημα, βρίσκεται στο κλειδί USBStor στον System hive του Registry, όπου υπάρχει ένα υποκλειδί για κάθε συσκευή που έχει συνδεθεί στο σύστημα. Εξάγετε πληροφορίες για USBStor με το usbstor.pl plugin του Regripper και αποθηκεύστε τες (για ευκολία) σε αρχείο με όνομα usbstor.txt.

   Εντολή: rip -r C:/Work/ntuser.dat -p usbstor.pl > C:/Work/usbstor.txt

   Αποτελέσματα:

[9] Δεν είναι βέβαιο ότι κάθε USB μνήμη έχει μοναδικό σειριακό αριθμό. Έχουν αναφερθεί περιπτώσεις συσκευών του ίδιου κατασκευαστή, με τον ίδιο σειριακό αριθμό. Υπάρχουν και συσκευές χωρίς σειριακό αριθμό και τότε τους αποδίδεται ένα μοναδικό αναγνωριστικό από το Windows όπου συνδέθηκαν και το οποίο έχει δεύτερο χαρακτήρα το &[3].



Η υπό εξέταση συσκευή έχει συνδεθεί στο σύστημα κι έχει Device class ID ”Disk& Ven_ JetFlash& Prod_ Transcend_ 4GB& Rev_ 1100”. Από αυτό βλέπουμε ότι ο κατασκευαστής είναι η Jetflash και έκδοση 1100.

2.2. Το σειριακό αριθμό της συσκευής τον βρίσκουμε από το όνομα του υποκλειδιού του Device class ID της όπου στην περίπτωσή μας είναι 72R7A4VJ8GHMSTH0& 0.

2.3. Για τα ID του προϊόντος και του κατασκευαστή ανατρέχουμε στο κλειδί USB του System hive χρησιμοποιώντας το usdevicesb.pl plugin του Regripper και βρίσκουμε το υποκλειδί με όνομα το σειριακό αριθμό της usb μνήμης.

Αποτελέσματα:

VID_ 174C& PID_ 55AA
LastWrite: Thu Aug 21 14:05:05 2014
SN : 308000000000000001A89
*LastWrite: Thu Aug 21 14:05:08 2014 VID_ 8564& PID_*

1000]
LastWrite: Thu Aug 21 09:08:56 2014
SN : 72R7A4VJ8GHMSTH0
LastWrite: Thu Aug 21 17:33:37 2014

Το ID προϊόντος είναι 1000 και το ID κατασκευαστή είναι 8564.

3. Προσδιορίστε το καθολικά μοναδικό αναγνωριστικό του τόμου του δίσκου (volume GUID) και το γράμμα δίσκου[10] στο οποίο είχε αντιστοιχιστεί η usb μνήμη.

   3.1. Οι πληροφορίες αυτές υπάρχουν στις τιμές (values) του κλειδιού MountedDevices του System hive και μπορείτε να τις βρείτε με το mountdev.pl plugin του RegRipper.

   3.2. Αναζητείστε, στα αποτελέσματα του Regripper, τον σειριακό αριθμό της υπό εξέτασης συσκευής. Βλέπουμε ότι το ζητούμενο GUID είναι το b114386d-2912-11e4-834d-60a44cac858c και το drive letter το H.

4. Ελέγξτε ποιοι χρήστες έχουν συνδέσει τη usb μνήμη στο σύστημα.

   4.1. Πληροφορίες για το αν κάποιος χρήστης είχε πρόσβαση στη συσκευή υπάρχουν στο κλειδί MountPoints2 του αντίστοιχου user hive. Υποκλειδιά του είναι GUIDs τα οποία μπορούν να αντιστοιχιστούν στα GUIDs του κλειδιού MountedDevices (βήμα 2). Μοναδικός χήστης στο συγκεκριμένο σύστημα είναι η Alice [11] Βρείτε τις πληροφορίες αυτές εφαρμόζοντας το mp2.pl plugin του RegRipper στον user hive της Alice.

   Αποτελέσματα:

   MountPoints2
   Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
   LastWrite Time Thu Aug 21 14:05:20 2014 (UTC) Remote

   Drives:

   Volumes:
   Thu Aug 21 17:33:39 2014 (UTC)
   b114386d-2912-11e4-834d-60a44cac858c
   Thu Aug 21 14:08:48 2014 (UTC)
   f9941c2b-293b-11e4-9157-60a44cac858c
   Wed Aug 20 22:41:02 2014 (UTC)

[10] **Προσοχή:** Το γράμμα του δίσκου δεν είναι πάντα δυνατόν να βρεθεί διότι για το κάθε γράμμα διατηρούνται πληροφορίες μόνο για την συσκευή που αντιστοιχήθηκε τελευταία σε αυτό.

[11] Μπορείτε να βρείτε τους χρήστες του συστήματος από τον SAM hive με το samparse.pl plugin του RegRipper.

4919aace-28b5-11e4-aeff-806e6f6e6963
Wed Aug 20 22:14:37 2014 (UTC)
1b5a7c4d-9396-4a38-ab14-6559a74df235
af394822-8a9d-4a81-9e6e-9a67699820bc
Wed Aug 20 22:07:43 2014 (UTC)
18eb7759-b125-e2a7-0b75-3dc0d23dc9ad
2edd3537-f5cb-6669-cd2f-37c7907dcad5

Στα αποτελέσματα, αναζητείστε το GUID στο οποίο αντιστοιχεί η υπό εξέταση συσκευή (στην περίπτωσή μας το b114386d-2912-11e4-834d-60a44cac858c). Το GUID, άρα ο χρήστης Alice έχει συνδέσει την usb μνήμη. Μας δίνεται επίσης το LastWrite time του GUID το οποίο μας λέει ότι Πέμπτη 21 Αυγούστου 2014 και ώρα 17:33:39 (UTC) ήταν η τελευταία φορά που συνδέθηκε η συσκευή στον υπολογιστή από τον χρήστη Alice.

5. Προσδιορίστε την πρώτη φορά που συνδέθηκε η συγκεκριμένη usb μνήμη στον υπολογιστή.

   5.1. Εξάγετε από το δοθέν image το αρχείο setupapi.dev.log [12] που βρίσκεται στο φάκελο C:\Windows\inf\setupapi.dev.log και εκτελέστε αναζήτηση στο αρχείο κειμένου που εξάγατε με βάση τον σειριακό αριθμό της συσκευής.

   5.2. Η ημερομηνία και ώρα που θα βρείτε (Εδώ 21/08/2014 και 12:08:18 τοπική ώρα[13]), είναι η πρώτη φορά που συνδέθηκε η usb μνήμη στον συγκεκριμένο υπολογιστή.

6. Προσδιορίστε την τελευταία φορά που συνδέθηκε η συγκεκριμένη usb μνήμη στον υπολογιστή.

   6.1. Στο πρώτο βήμα επεξεργαστήκαμε το κλειδί USB του System hive. Το LastWrite time του υποκλειδιού με όνομα τον σειριακό αριθμό της

[12] Περιέχει πληροφορίες για εγκαταστάσεις συσκευών και οδηγών. Οποτεδήποτε μια συσκευή προσωρινής αποθήκευσης συνδεθεί στον υπολογιστή για πρώτη φορά, ο διαχειριστής Plug and Play ζητάει προσδιοριστικές πληροφορίες για τη συσκευή, δημιουργεί έναν device class ID γι αυτήν και βρίσκει τον κατάλληλο οδηγό. Αυτές οι πληροφορίες αποθηκεύονται στο setupapi.dev.log

[13] Για να βρείτε την ώρα σε UTC, πρέπει να προσδιορίσετε την ζώνη ώρας του συστήματος και να συμπεριλάβετε και τη θερινή ώρα (αν υπάρχει). Χρήση timezone.pl plugin του Regripper όπως στο εργαστήριο 2, βήμα 3

συσκευής μας δίνει την τελευταία φορά που αυτή συνδέθηκε στο σύστημα. Στην περίπτωση μας την Πέμπτη 21 Αυγούστου 2014 και ώρα 17:33:37 (UTC). Αυτή η πληροφορία φαίνεται να είναι αρκετά συνεπής ανάμεσα στα διάφορα συστήματα.

6.2. Στο τρίτο βήμα είδαμε την τελευταία φορά που χρησιμοποίησε το usb ο χρήστης Alice. Στην περίπτωσή μας οι δύο ημερομηνίες συμπίπτουν.

7. Προσδιορίστε την πρώτη φορά που συνδέθηκε η usb μνήμη μετά την τελευταία επανεκκίνηση [14]

7.1. Πρώτη πηγή της πληροφορίας αυτής είναι το κλειδί USBStor που είδαμε στο πρώτο βήμα. Από το LastWrite time του υποκλειδιού με όνομα το σειριακό αριθμό βλέπουμε ότι πρώτη σύνδεση μετά την τελευταία επανεκκίνηση έγινε την Πέμπτη 21 Αυγούστου 2014 και ώρα 17:33:37 (UTC).
Προσοχή: Έχουν αναφερθεί περιπτώσεις μιας ανωμαλίας [15] όπου όλες οι συσκευές που βρίσκονται στο κλειδί USBStor έχουν το ίδιο LastWrite time [3].

7.2. Άλλη πηγή αποτελεί το κλειδί DeviceClasses του System hive. (Εξάγετε το DeviceClasses κλειδί με το devclasses.pl plugin του Regripper.) Υποκλειδί του είναι το GUID 53f56307-b6bf-11d0-94f2-00a0c91efb8b που αναφέρεται στις συσκευές που αναγνωρίζονται ως δίσκοι. Κάτω από αυτό βρίσκεται ένα υποκλειδί που περιλαμβάνει το device class ID και τον σειριακό αριθμό της υπό εξέτασης συσκευής. Το LastWrite time του κλειδιού αυτού είναι το ζητούμενο.

Αποτελέσματα:

DevClasses - Disks
ControlSet001\Control\DeviceClasses\53f56307-b6bf-11d0-94f2-00a0c91efb8b

Thu Aug 21 17:33:37 2014 (UTC)

[14] **Προσοχή:** Μετά την εκκίνηση ενός συστήματος, μία συσκευή μπορεί να συνδεθεί και αποσυνδεθεί από αυτό πολλές φορές αλλά το LastWrite time των κλειδιών που ακολουθούν, αντιπροσωπεύει την πρώτη φορά που συνδέθηκε η συσκευή κατά τη διάρκεια του τελευταίου boot session.

[15] Πιθανόν είναι αποτέλεσμα ενός Service Pack ή κάποιου εγκατεστημένου patch ή ενός αντικειμένου πολιτικής ομάδας (Group Policy Object) που τροποποιεί τις ACLs των κλειδιών

Disk& Ven_ JetFlash& Prod_ Transcend_ 4GB& Rev_ 1100,72R7A4VJ8GHMSTH0& 0

Thu Aug 21 14:05:08 2014 (UTC)

Disk& Ven_ Intenso& Prod_ USB_ 3.0_ Device& Rev_ AX00,308000000000000001A89& 0

DevClasses - Volumes
ControlSet001\Control\DeviceClasses\53f5630d-b6bf-11d0-94f2-00a0c91efb8b

Σχόλιο: Η εξέταση πολλών διαφορετικών κλειδιών για την εύρεση ενός timestamp αρχικά δε φαίνεται χρήσιμη, όμως προσφέρει επιπλέον συνδυαστική πληροφορία για έναν αναλυτή. Είναι ιδιαίτερα χρήσιμη όταν κάποιος έχει προσπαθήσει να καλύψει τα ίχνη του κι έχει, για παράδειγμα, διαγράψει το περιεχόμενο του USBStor.

8. Βρείτε πόσες φορές έχει συνδεθεί το usb στον υπό εξέταση υπολογιστή, ποιες ημερομηνίες και ώρες και για πόσο χρόνο την κάθε φορά.

   8.1. Πληροφορίες για συνδέσεις και αποσυνδέσεις συσκευών usb βρίσκονται στο log αρχείο
   Microsoft-Windows-DriverFrameworks-UserMode/Operational
   του Windows 7. Εξάγετε το από το φάκελο C:\Windows \System32 \winevt \Logs και αποθηκεύστε το στο φάκελο εργασίας σας.

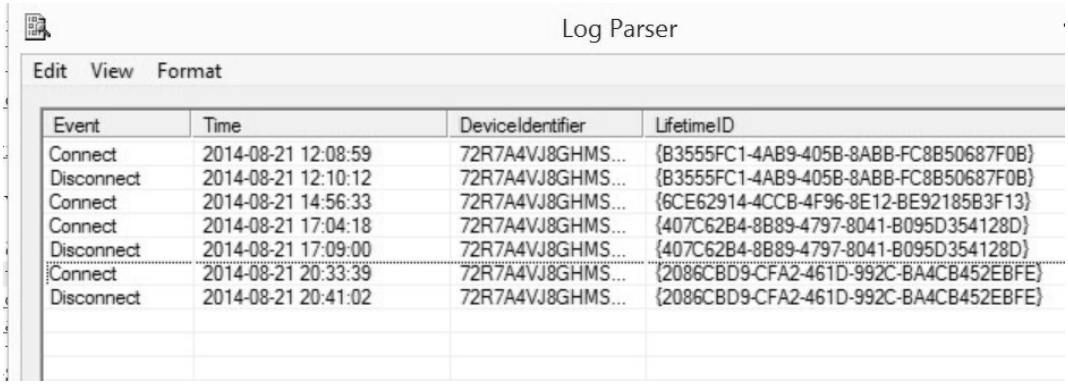
   8.2. Χρησιμοποιώντας τον LogParser μπορείτε να απομονώσετε τις εγγραφές γεγονότων που σχετίζονται με συνδέσεις και αποσυνδέσεις και να αναλύσετε το τμήμα συμβολοσειρών της εγγραφής.
   Για παράδειγμα, χρησιμοποιείστε το παρακάτω ερώτημα για να πάρετε όλες τις εγγραφές με Event ID 2003 (σύνδεση) ή 2100 (αποσύνδεση) και για τις οποίες ο σειριακός αριθμός της υπό εξέτασης συσκευής περιλαμβάνεται στο τμήμα συμβολοσειρών της εγγραφής αλλά και , στην περίπτωση του γεγονότος αποσύνδεσης, το κείμενο ”27|23” [16] περιλαμβάνεται επίσης στο τμήμα συμβολοσειρών.

   LogParser ερώτημα:
   LogParser -i EVT -o datagrid

[16] Στην αποσύνδεση δημιουργούνται εγγραφές γεγονότος με ID 2100,2102 και πιθανόν κι άλλες που εξαρτώνται και από το αν υπάρχουν άλλες USB συσκευές συνδεδεμένες. Όμως, εγγραφές με ID 2100 και το κείμενο ”Received a PnP or Power operation(27,23) for device <deviceInfo>” και άλλες ”27|23” εμφανίζονται πάντοτε στην αποσύνδεση.

"SELECT CASE EventID WHEN 2003 THEN 'Connect' WHEN 2100 THEN 'Disconnect' END As Event,
TimeGenerated AS Time,'72R7A4VJ8GHMSTH0' as DeviceIdentifier,
EXTRACT_ TOKEN(Strings,0,'|') as LifetimeID[17]
FROM C:\Work \Microsoft-Windows-DriverFrameworks-UserMode %4Operational.evtx WHERE (EventID=2003
AND STRINGS Like '%12LMAL2G7EDSYFES%') OR (EventID=2100
AND STRINGS LIKE '%72R7A4VJ8GHMSTH0%27|23%')"

Αποτελέσματα:



Event	Time	DeviceIdentifier	LifetimeID
Connect	2014-08-21 12:08:59	72R7A4VJ8GHMS...	{B3555FC1-4AB9-405B-8ABB-FC8B50687F0B}
Disconnect	2014-08-21 12:10:12	72R7A4VJ8GHMS...	{B3555FC1-4AB9-405B-8ABB-FC8B50687F0B}
Connect	2014-08-21 14:56:33	72R7A4VJ8GHMS...	{6CE62914-4CCB-4F96-8E12-BE92185B3F13}
Connect	2014-08-21 17:04:18	72R7A4VJ8GHMS...	{407C62B4-8B89-4797-8041-B095D354128D}
Disconnect	2014-08-21 17:09:00	72R7A4VJ8GHMS...	{407C62B4-8B89-4797-8041-B095D354128D}
Connect	2014-08-21 20:33:39	72R7A4VJ8GHMS...	{2086CBD9-CFA2-461D-992C-BA4CB452EBFE}
Disconnect	2014-08-21 20:41:02	72R7A4VJ8GHMS...	{2086CBD9-CFA2-461D-992C-BA4CB452EBFE}

Βλέπουμε τρία ζευγάρια γεγονότων Σύνδεσης-Αποσύνδεσης με το ίδιο LifeTimeID μαζί με τις ημερομηνίες και ώρες των γεγονότων αυτών. Υπάρχει κι ένα γεγονός σύνδεσης (στις 14:56:33) χωρίς αντίστοιχο γεγονός αποσύνδεσης. Αυτό σημαίνει ότι η usb μνήμη αποσυνδέθηκε ΑΦΟΥ ο υπολογιστής είχε απενεργοποιηθεί. Άρα συνολικά έχουμε 4 συνδέσεις στον συγκεκριμένο υπολογιστή.

5.3.2 Επιπλέον Ασκήσεις

1. Ποιες άλλες USB συσκευές προσωρινής αποθήκευσης έχουν συνδεθεί στο υπό εξέταση σύστημα; Παρατηρείτε διαφορές στα στοιχεία τους που φυλάσσονται στο Registry σε σχέση με αυτά της USB μνήμης; **Υπόδειξη:** Θα βρείτε έναν εξωτερικό σκληρό δίσκο συνδεδεμένο και θα σας χρειαστεί η

[17] Η τιμή LifetimeID που συνδέεται με το session σύνδεσης του USB και βοηθάει να συνδέσουμε ένα συγκεκριμένο γεγονός αποσύνδεσης με το αντίστοιχο γεγονός σύνδεσης.

υπογραφή του δίσκου (disk signature)[18] που είναι ”bb c7 72 32”.

2. Ποια ευαίσθητα αρχεία από την USB μνήμη άνοιξε/τροποποίησε ο χρήστης που τη συνέδεσε στον υπό εξέταση υπολογιστή;
   Υπόδειξη: Ερευνήστε πηγές που ανιχνεύουν τη δραστηριότητα χρήστη (αναφέρθηκαν στο δεύτερο εργαστήριο) και αναζητείστε το γράμμα του δίσκου στο οποίο αντιστοιχήσατε την υπό εξέταση USB μνήμη. Στα ευαίσθητα αρχεία συμπεριλαμβάνονται και έγγραφα οπότε προσθέστε στις πηγές, πρόσφατα ανοιγμένα αρχεία του Adobe Reader
   (Regripper plugin: adoberdr.pl) και jump lists της εφαρμογής αυτής.

[18] Είναι τα 4 bytes στο offset 440(0x1B80) μέσα στο MBR του δίσκου και αλλάζει κάθε φορά που γίνεται format στο δίσκο. Έχοντας το δίσκο στα χέρια μας, την βλέπουμε με κάποιον hex editor [2].

Βιβλιογραφία

[1] Digital Forensics Research *Workshop A Road Map for Digital Forensic Research*, 2001

[2] Harlan Carvey *Windows Registry Forensics, Advanced Digital Forensic Analysis of the Windows Registry*, 2011

[3] Harlan Carvey *Windows Forensic Analysis Toolkit, Advanced Analysis Techniques for Windows 7 | 3E*, 2012

[4] Brian Carrier *File System Forensic Analysis*, 2005

[5] Cory Altheide, Harlan Carvey *Digital Forensics with Open Source Tools*, 2011

[6] John Sammons *The Basics of Digital Forensics, The Primer for Getting Started with Digital Forensics*, 2012

[7] Bill Nelson, Amelia Phillips, Christofer Steuart *Guide to Computer Forensics and Investigations 3rd Edition*, 2010

[8] Steve Bunting *EnCE, Encase Computer Forensics: The Official Certified Examiner, 3rd Edition*, 2012

[9] Ryan Jones, Computer Science Laboratory University of Kent at Canterbury United Kingdom *Safer Live Forensic Acquisition* `http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf`

[10] Marthie Lessing, Basie von Solms *Live Forensic Acquisition as Alternative to Traditional Forensic Processes*

[11] Harlan Carvey, *Windows Incident Response Block*
http://windowsir.blogspot.gr/