ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

CERTCOOP

ΤΕΧΝΙΚΟ ΕΓΧΕΙΡΙΔΙΟ

ΣΥΛΛΟΓΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΣΕ WINDOWS ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ

ΑΘΗΝΑ, ΜΑΡΤΙΟΣ 2018
ΤΥΠΟΓΡ. ΕΛΛΗΝΙΚΟΥ ΣΤΡΑΤΟΥ

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

./.

ΚΕΦΑΛΑΙΟ «Α»
ΕΙΣΑΓΩΓΗ

ΤΜΗΜΑ 1
ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΟΔΗΓΟ

Αυτός ο οδηγός παρέχει πληροφορίες σχετικά με την ψηφιακή εγκληματολογική ανάλυση ενός Windows λειτουργικού συστήματος. Επικεντρώνεται στη διαδικασία συγκέντρωσης αποδεικτικών στοιχείων και αναφέρεται στα Windows 10, στα Windows 8, Windows 8.1 και 7. Τα παραδείγματα που αναφέρονται ισχύουν, σε πολλές περιπτώσεις, για όλες τις εκδόσεις Windows λειτουργικών συστημάτων, καθώς έχουν παρόμοια δομή.

Παρέχει μια γενική παρουσίαση της διαδικασίας συλλογής αποδεικτικών στοιχείων, εξηγώντας από τι συνίσταται, για πιο λόγο πραγματοποιείται, τα στάδια που την απαρτίζουν, τις μεθόδους για να την πραγματοποιήσουμε και ταυτόχρονα δίνει μία συγκεκριμένη μεθοδολογία. Ο οδηγός παρουσιάζει μία γενική εικόνα της ψηφιακής εγκληματολογικής ανάλυσης και εστιάζει κυρίως στη φάση της απόκτησης-συλλογής των αποδεικτικών στοιχείων και αυτή είναι η βασική επιδίωξη του.

Το κοινό-στόχος αυτού του εγγράφου είναι οι επαγγελματίες του τομέα της πληροφορικής (τεχνικοί υποστήριξης, διαχειριστές συστήματος, διαχειριστές δικτύου, αναλυτές ιομορφικού λογισμικού, κ.λπ.) που έχουν γνώση των υπολογιστών, αλλά δεν είναι εξοικειωμένοι με την ψηφιακή διαδικασία εγκληματολογικής ανάλυσης και μπορεί να χρειαστεί να αντιμετωπίσουν ένα περιστατικό (κυβερνοεπίθεση) που θα απαιτούσε την εφαρμογή της εν λόγω διαδικασίας.

Το έγγραφο στοχεύει να είναι ένας πρακτικός οδηγός, που θα περιγράφει τα βήματα που θα πρέπει να ακολουθηθούν, όταν προκύψει ένα κυβερνο-περιστατικό, που με την σειρά του απαιτεί τη συλλογή των απαραίτητων αποδεικτικών στοιχείων, για τη διενέργεια της επακόλουθης ψηφιακής εγκληματολογικής ανάλυσης που οδηγεί στην αντιμετώπιση του περιστατικού. Αυτή η επακόλουθη ανάλυση είναι πέρα από το αντικείμενο του παρόντος εγγράφου.

Στον συγκεκριμένο οδηγό, θα χρησιμοποιηθούν εργαλεία που είναι ελεύθερα στο διαδίκτυο και δεν απαιτούν εμπορική άδεια.

ΤΜΗΜΑ 2
ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΟΙ ΣΥΜΒΟΛΙΣΜΟΙ

Οι ακόλουθοι συμβολισμοί θα χρησιμοποιηθούν στο έγγραφο:

Παράδειγμα Τμήματα ή μέρη του εγγράφου, που στόχο έχουν να πραγματοποιήσουν μια επίδειξη που να δείχνει πότε η παρεχόμενη πληροφορία θα μπορούσε να χρησιμοποιηθεί.

Σημαντικό Υπογραμμίζει ορισμένες πληροφορίες που είναι σημαντικές και θα πρέπει να τύχουν ιδιαίτερης προσοχής.

Σημείωση Ενημερώνει για μια πτυχή-διάσταση που πρέπει να έχουμε κατά νου.

Άλλα εργαλεία Παρουσιάζει-προτείνει και άλλα εργαλεία με παρόμοια χαρακτηριστικά ή λειτουργίες σε σχέση με αυτό που προαναφέρθηκε στην προηγούμενη ενότητα.

ΚΕΦΑΛΑΙΟ «Β»
ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ

ΤΜΗΜΑ 3
ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ

Η έννοια της ψηφιακής εγκληματολογικής ανάλυσης αναφέρεται σε ένα συνδυασμό διαδικασιών συλλογής και ανάλυσης αποδεικτικών στοιχείων που διεξάγονται με σκοπό την αντιμετώπιση ενός κυβερνο-περιστατικού, που σχετίζεται με την ασφάλεια υπολογιστών και δικτύων και που -σε ορισμένες περιπτώσεις- μπορεί να χρησιμοποιηθεί ως αποδεικτικό στοιχείο στο δικαστήριο. Ο στόχος είναι να απαντήσουμε στο **τι, πού, πότε, γιατί, ποιος** και **πώς**, με την ολοκλήρωση αυτής της διαδικασίας. Ως ανάλυση ορίζουμε την συλλογή δεδομένων, την συσχέτιση μεταξύ τους και την ερμηνεία τους.

Η Ψηφιακή σήμανση (Digital forensics) είναι ένας κλάδος της σήμανσης που περιλαμβάνει την ανάκτηση και την έρευνα του ψηφιακού υλικού (που βρίσκεται σε ψηφιακές συσκευές), που έχει σχέση με το έγκλημα πληροφορικής (κυβερνοέγκλημα). (Wikipedia).

Αντικειμενικός σκοπός της ψηφιακής σήμανσης είναι, να παρουσιάσει τα αποδεδειγμένα γεγονότα, δηλαδή, να περιγράψει ακριβώς τι έγινε στο υπό εξέταση σύστημα.

Ο διαχειριστής συμβάντος θα πρέπει να περιγράψει ακριβώς τι έγινε, να πει την ιστορία, να δείξει το τι συνέβη, ενώ αντίθετα ο κακόβουλος χρήστης θέλει να επιτύχει το σκοπό του!

Αυτή η επιστήμη έχει αρχίσει να αποκτά έναν πολύ σημαντικό ρόλο τα τελευταία χρόνια, καθώς όλο και συχνότερα έχουμε να αντιμετωπίσουμε διαφορετικά κυβερνο-περιστατικά που σχετίζονται με την ασφάλεια των υπολογιστών, όπως παράνομες εισβολές σε υπολογιστές και δίκτυα, την υποκλοπή πληροφοριών, τις μολύνσεις από ιούς, κλπ.

Η χρήση της επεκτείνεται μέσω ποικίλων πεδίων, για παράδειγμα:

- Δίωξη ψηφιακών εγκλημάτων όπως παραβίαση συστημάτων (hacking), οικονομική απάτη, φοροδιαφυγή, παρενόχληση ή παιδική πορνογραφία.
- Περιπτώσεις διάκρισης ή παρενόχλησης.
- Έρευνα ασφάλισης.

- Ανάκτηση διαγραφέντων αρχείων.
- Κλοπή πνευματικής ιδιοκτησίας.
- Κυβερνοτρομοκρατία.
- Ενίσχυση της ανθεκτικότητας των επιχειρήσεων, ή με άλλα λόγια, η ικανότητα ανάκτησης από επιθέσεις.

Το πώς αντιμετωπίζονται οι διαφορετικές περιπτώσεις, θα αντικατοπτριστεί σε ολόκληρο το έγγραφο, καθώς είναι ζωτικής σημασίας να έχουμε μια σαφή ιδέα για τα βήματα που ακολουθούν κατά τη διενέργεια μιας ψηφιακής εγκληματολογικής ανάλυσης, ώστε να μην καταστρέψουμε αποδεικτικά στοιχεία που θα καταστήσουν αδύνατη την επίλυση του περιστατικού με έναν αποτελεσματικό τρόπο. Ένα περιστατικό έχει επιλυθεί με ικανοποιητικό τρόπο, όταν εξάγονται συμπεράσματα που δίνουν τη δυνατότητα να απαντήσουμε στις ερωτήσεις που αναφέρθηκαν προηγουμένως. Επίσης ένα περιστατικό έχει επιλυθεί σωστά, όταν ακολουθώντας την ίδια διαδικασία, καταλήγουμε στο ίδιο συμπέρασμα.

Στην περίπτωση της παραβίασης ενός υπολογιστή ή ενός δικτύου υπολογιστών ο αντικειμενικός σκοπός της ψηφιακής σήμανσης είναι:

- Να ανακαλύψουμε τη φύση και τον σκοπό του ιομορφικού λογισμικού
- Να καθορίσουμε το μηχανισμό μόλυνσης
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με τον μολυσμένο υπολογιστή.
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με το δίκτυο
- Να καθορίσουμε πως ο κακόβουλος χρήστης αλληλεπιδρά με το ιομορφικό πρόγραμμα
- Να καθορίσουμε το σκεπτικό και το σκοπό της κυβερνοεπίθεσης, καθώς και το επίπεδο, το σχεδιασμό της επίθεσης.
- Να καθορίσουμε την έκταση της μόλυνσης του προσωπικού υπολογιστή αλλά και την επέκταση της μόλυνσης στο δίκτυο.

Με την ψηφιακή εγκληματολογική ανάλυση μπορούμε να πετύχουμε αρκετά, όπως:

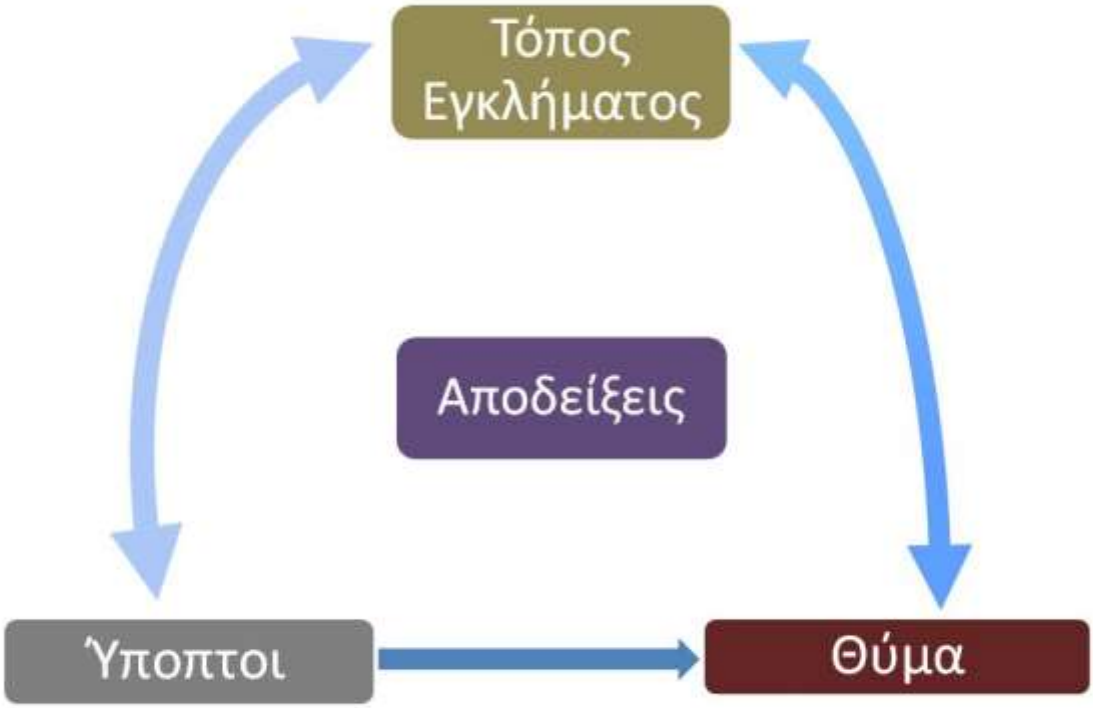
- Αποκατάσταση διαγραφέντων δεδομένων
- Αποκάλυψη πότε τα αρχεία τροποποιήθηκαν, δημιουργήθηκαν, διαγράφτηκαν.
- Μπορούμε να καθορίσουμε ποιες συσκευές τοποθετήθηκαν σε συγκεκριμένο υπολογιστή.
- Ποιες εφαρμογές εγκατασταθήκαν και από ποιον χρήστη.
- Ποιες ιστοσελίδες επισκεφτήκαμε...

Τι δεν μπορούμε να πετύχουμε:

- Εάν έχει καταστραφεί το αποθηκευτικό μέσο, δεν μπορούμε να κάνουμε αποκατάσταση δεδομένων.
- Εάν το αποθηκευτικό μέσο, έχει διαγραφεί με ασφαλή τρόπο, τότε δύσκολα έως αδύνατον να πετύχουμε αποκατάσταση δεδομένων.

ΤΜΗΜΑ 4
Η ΑΡΧΗ ΤΗΣ ΑΝΤΑΛΛΑΓΗΣ ΤΟΥ LOCARD

Κατά τη διενέργεια μιας ψηφιακής εγκληματολογικής ανάλυσης είναι ζωτικής σημασίας να έχουμε κατά νου την αρχή της ανταλλαγής του Locard. Ο Γάλλος εγκληματολόγος Edmond Locard είχε εκφράσει την άποψη πως είναι αδύνατον για έναν εγκληματία να δράσει χωρίς να αφήσει ίχνη της παρουσίας του. Μ' άλλα λόγια, πίστευε πως ο εγκληματίας θα αφήσει κάτι στον τόπο του εγκλήματος και ταυτόχρονα θα πάρει κάτι μαζί του. Αυτή είναι και η βασική αρχή της εγκληματολογικής επιστήμης, που έγινε γνωστή ως **αρχή της ανταλλαγής του Locard: Η επαφή μεταξύ δύο στοιχείων, πάντα θα επιφέρει μιαν ανταλλαγή.** Αυτό σημαίνει ότι κάθε είδος εγκλήματος, συμπεριλαμβανομένων εκείνων που σχετίζονται με την πληροφορική, που είναι και αυτό που μας αφορά, αφήνει ένα ίχνος, που σημαίνει ότι μέσα από μια διαδικασία εγκληματολογικής ανάλυσης είναι δυνατό να συγκεντρωθούν αποδεικτικά στοιχεία.



Εικόνα 1: Η αρχή της ανταλλαγής του Locard

Σημαντικό

Ομοίως, η αρχή της ανταλλαγής του Locard λαμβάνει χώρα και κατά τη διενέργεια της πραγματικής εγκληματολογικής ψηφιακής ανάλυσης, πράγμα που σημαίνει ότι θα πρέπει να είμαστε εξαιρετικά προσεκτικοί, έτσι ώστε το σύστημα να επηρεαστεί όσο το δυνατόν λιγότερο και τα αποκτηθέντα αποδεικτικά στοιχεία να μην μεταβληθούν.

ΤΜΗΜΑ 5
ΤΥΠΟΙ ΨΗΦΙΑΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΑΝΑΛΥΣΗΣ

Η ταξινόμηση των τύπων της ψηφιακής εγκληματολογικής ανάλυσης μπορεί να γίνει ανάλογα με το τι αυτή αποσκοπεί να αναλύσει (ποιο είναι το αντικείμενο). Έχοντας αυτό υπόψη είναι δυνατόν να προσδιοριστούν τέσσερις περιπτώσεις ανάλυσης:

- Εγκληματολογική ψηφιακή ανάλυση λειτουργικού συστήματος: όλα τα λειτουργικά συστήματα όπως Windows, OSX, GNU/Linux, κλπ.
- Εγκληματολογική ψηφιακή ανάλυση δικτύου.
- Εγκληματολογική ψηφιακή ανάλυση ενσωματωμένου συστήματος.
- Εγκληματολογική ψηφιακή ανάλυση μνήμης (προσωρινής αποθήκευσης - volatile memory).

Ο οδηγός αυτός, όπως υποδηλώνει το όνομά του και έχει αναφερθεί προηγουμένως, εστιάζει στη συλλογή αποδεικτικών στοιχείων στα Windows λειτουργικά συστήματα, αν και η διαδικασία από μια γενικότερη άποψη είναι παρόμοια για όλους τους τύπους λειτουργικών συστημάτων.

ΤΜΗΜΑ 6
ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Η διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης πρέπει να κατέχει τα ακόλουθα χαρακτηριστικά:

- **Επαληθεύσιμη**: πρέπει να είναι δυνατόν να επιβεβαιωθεί η εγκυρότητα των συμπερασμάτων που προέκυψαν από την ανάλυση που διενεργήθηκε.

- **Αναπαράξιμη**: όλες οι δοκιμές που πραγματοποιήθηκαν καθ' όλη τη διαδικασία πρέπει να μπορούν να αναπαραχθούν ανά πάσα στιγμή.

- **Τεκμηριωμένη**: η όλη διαδικασία πρέπει να τεκμηριώνεται σωστά και πρέπει να πραγματοποιείται με κατανοητό και λεπτομερή τρόπο.

- **Ανεξάρτητη**: τα συμπεράσματα που προκύπτουν πρέπει να είναι τα ίδια, ανεξάρτητα από το πρόσωπο που διενεργεί τη διαδικασία και τη μέθοδο που χρησιμοποιείται.

ΤΜΗΜΑ 7
ΦΑΣΕΙΣ

Η διαδικασία της εγκληματολογικής ανάλυσης αποτελείται από τις ακόλουθες φάσεις:

Εικόνα 2: Οι φάσεις της διαδικασίας της εγκληματολογικής ανάλυσης

- **Διατήρηση**: Αντιστοιχεί στη φάση που εγγυάται ότι κανένα αποδεικτικό στοιχείο που έχει συλλεχθεί για μεταγενέστερη ανάλυση δεν θα χαθεί. Μία έλλειψη γνώσης, δηλαδή της ορθής διαδικασίας συλλογής πληροφοριών, θα μπορούσε να οδηγήσει σε απώλεια σχετικών πληροφοριών που θα μπορούσαν να είναι καθοριστικές για την επίλυση του κυβερνο-περιστατικού. Κρίσιμες ενέργειες όπως η μη απενεργοποίηση του συστήματος για να διατηρηθούν οι πληροφορίες προσωρινής αποθήκευσης (συλλογή μνήμης) ή η σωστή σήμανση των δεδομένων-στοιχείων που πρόκειται στην συνέχεια να αναλυθούν, λαμβάνουν χώρα κατά τη διάρκεια αυτής της φάσης.

Ομοίως, θα πρέπει να πραγματοποιείται μια σταθερή και συνεχόμενη καταγραφή όλων των ενεργειών που λαμβάνουν χώρα στο υλικό (στοιχεία) που πρόκειται να αναλυθεί. Σκοπός της καταγραφής είναι να διατηρηθεί η νομική εγκυρότητα των στοιχείων που συγκεντρώθηκαν, ώστε να αποδειχθούν όλα νόμιμα στην περίπτωση αντιδικίας. Αν τα δεδομένα (αποδεικτικά στοιχεία) χρειαστεί να μεταφερθούν, αυτό θα πρέπει να γίνει με τη μεγαλύτερη δυνατή προσοχή, αποφεύγοντας να αλλοιωθούν οι πληροφορίες ή να εκτεθούν σε ακραίες θερμοκρασίες (σκληροί δίσκοι) ή σε ηλεκτρομαγνητικά πεδία.

- **Απόκτηση-συλλογή**: Αυτή είναι η φάση με την οποία ασχολείται ο εν λόγω οδηγός. Η συγκεκριμένη φάση θα παρουσιαστεί με την μέγιστη λεπτομέρεια και που αντιστοιχεί στο στάδιο όπου συγκεντρώνονται τα αποδεικτικά στοιχεία. Ως αποδεικτικό στοιχείο μπορεί να οριστεί κάθε απόδειξη που μπορεί να χρησιμοποιηθεί σε μια νομική διαδικασία, αν και αυτό δεν είναι πάντα η υπόθεση.

Χαρακτηριστικά των αποδεικτικών στοιχείων:

- **Παραδεκτά**: πρέπει να έχουν νομική αξία.

- **Αυθεντικά**: πρέπει να είναι αληθή και να μην χειραγωγούνται-αλλοιώνονται με οποιοδήποτε τρόπο. Για το σκοπό αυτό, πρέπει να έχουν εξαχθεί τα αντίστοιχα αποτελέσματα των αλγορίθμων κατακερματισμού (hashes - ελέγχου ακεραιότητας) για να εξασφαλίζεται η ακεραιότητά τους.

- **Ολοκληρωμένα**: πρέπει να παρουσιάζουν τα αποδεικτικά στοιχεία από μια αντικειμενική και τεχνική άποψη, χωρίς προσωπικές εκτιμήσεις ή προκαταλήψεις.

- **Σαφή**: πρέπει να είναι κατανοητά.

- **Αξιόπιστα**: οι τεχνικές που χρησιμοποιούνται για τη συγκέντρωση αποδεικτικών στοιχείων δεν πρέπει να δημιουργούν αμφιβολίες ως προς την ειλικρίνεια και την αυθεντικότητα τους.

Μπορούν να ταξινομηθούν σε δύο τύπους:

• Φυσικά αποδεικτικά στοιχεία: αναφέρονται στα υλικά του υπολογιστή όπως σκληροί δίσκοι, pen drives, κλπ.

• Ψηφιακά αποδεικτικά στοιχεία: αντιστοιχούν στις πληροφορίες που αποθηκεύονται στα ηλεκτρονικά αποδεικτικά στοιχεία.

Μερικά παραδείγματα των ψηφιακών αποδεικτικών στοιχείων είναι:

- Τα ψηφιακά αρχεία.
- Οι Διεργασίες/υπηρεσίες.
- Τα μητρώα καταγραφής συμβάντων (Log files).
- Τα προσωρινά αρχεία (Temporary files).
- Οι καταχωρήσεις – εγγραφές στην registry.

• **Ανάλυση**: Κατά τη διεξαγωγή της ανάλυσης των συλλεχθέντων πληροφοριών πρέπει να έχουμε κατά νου το συγκεκριμένο τύπο του περιστατικού για να ενεργήσουμε αντίστοιχα. Δηλαδή διαφορετικές είναι οι ενέργειες στην περίπτωση παράνομης διείσδυσης σε έναν υπολογιστή και διαφορετική στην περίπτωση παιδικής πορνογραφίας. Ανάλογα με την περίπτωση, μπορεί να είναι χρήσιμο να κάνουμε μία σε βάθος ανάλυση διαφορετικών αντικειμένων όπως:

- **MFT ή Master File Table**: Είναι ο πίνακας που αποθηκεύει όλες τις πληροφορίες σχετικά με τα αρχεία στο δίσκο. Αποθηκεύει πληροφορίες όπως το όνομα, την πρόσβαση, τις ημερομηνίες δημιουργίας και τροποποίησης, τη θέση σχετικά με τα δεδομένα στο δίσκο, το μέγεθος, κλπ.

- **Μνήμη (Memory):** Η μνήμη είναι ηλεκτρονικά κυκλώματα, τα οποία «αποθηκεύουν» προγράμματα και δεδομένα για να χρησιμοποιηθούν από τον μικροεπεξεργαστή. Υπάρχουν δύο είδη μνήμης. Η μνήμη ROM (Read Only Memory) και η μνήμη RAM (Random Access Memory). Χαρακτηριστικό μέγεθος της μνήμης είναι και πάλι η χωρητικότητα, η οποία μετριέται με τις ίδιες μονάδες μέτρησης, όπως και η χωρητικότητα του σκληρού δίσκου.

- **Paging (Pagefile.sys)**: είναι ένα αρχείο στον φυσικό δίσκο, που επιτρέπει τη βέλτιστη χρήση της μνήμης RAM. Το λειτουργικό σύστημα στέλνει προσωρινά εκεί τις πληροφορίες που δεν είναι απαραίτητες στην μνήμη και στη συνέχεια τις ανακτά αν κάποιο πρόγραμμα τις ζητήσει.

- **Κάδος ανακύκλωσης**.

- **Unassigned space (Μη εκχωρημένος χώρος)**: αντιστοιχεί

στον ελεύθερο χώρο του δίσκου που διατίθεται για την αποθήκευση πληροφοριών. Όταν ένα αρχείο διαγράφεται στα Windows, το λειτουργικό σύστημα αφαιρεί μόνο την αναφορά στις εν λόγω πληροφορίες, αλλά όχι την ίδια την πληροφορία. Αντ' αυτού, η αντίστοιχη περιοχή στο δίσκο χαρακτηρίζεται ως ελεύθερη-εγγράψιμη. Ως εκ τούτου, οι διαγραμμένες πληροφορίες μπορούν να ανακτηθούν με διαφορετικά μέσα.

- **Windows registry (Το Μητρώο ρυθμίσεων των Windows)**: αποθηκεύει διάφορες πληροφορίες-ρυθμίσεις των windows, όπως τα δίκτυα με τα οποία το σύστημα έχει συνδεθεί, μια λίστα των επισκεφθέντων ιστοσελίδων, εγκατεστημένες εφαρμογές, το ιστορικό των συσκευών USB που έχουν συνδεθεί, κλπ.

- **Slack Space**: αναφέρεται στον ελεύθερο χώρο που παραμένει μέσα σε ένα cluster (σετ των διπλανών τομέων του δίσκου που συνθέτουν τη μικρότερη μονάδα πληροφορίας σε ένα δίσκο) μετά την αποθήκευση ενός αρχείου.

- **Κίνηση του δικτύου**.

- **Διεργασίες του συστήματος**.

- **Μητρώα καταγραφής συμβάντων του συστήματος (Log files)**: όπως τα αρχεία καταγραφής των συμβάντων που σχετίζονται με το σύστημα, την ασφάλεια ή τις εφαρμογές.

Είναι ζωτικής σημασίας η όλη διαδικασία να διενεργείται με αντικειμενική άποψη, χωρίς να αποκλείεται αυτό που ο αναλυτής μπορεί να θεωρήσει προφανές.

• **Τεκμηρίωση:** Μια θεμελιώδη διάσταση στη διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης είναι η τεκμηρίωση. Η συγκεκριμένη φάση θα πρέπει να πραγματοποιείται με ένα πολύ μεθοδικό και λεπτομερή τρόπο. Οι ακόλουθες ενέργειες, μεταξύ άλλων, μπορούν να χρησιμοποιηθούν-πραγματοποιηθούν:

- Φωτογραφίζουμε τις αποδείξεις.
- Διατηρούμε την αλυσίδα παρακολούθησης-επιτήρησης (chain of custody).
- Καταγράφουμε κάθε βήμα που λαμβάνεται κατά τη διάρκεια της διαδικασίας, κρατώντας ένα αρχείο καταγραφής με τις ημερομηνίες και τις ώρες κάθε ενέργειας που πραγματοποιείται στο αποδεικτικό στοιχείο.
- Εκπονούμε δύο τύπους για τις αναφορές συμπερασμάτων: έναν εκτελεστικό (περιληπτικό) και έναν τεχνικό.

• **Παρουσίαση**: Η παρουσίαση των πληροφοριών είναι εξίσου σημαντική καθώς τα συμπεράσματα που εξάγονται κατά την διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης θα πρέπει να είναι προσβάσιμα και απόλυτα κατανοητά.

Για να το επιτύχουμε αυτό αυτό, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

- Ετοιμάζουμε μια παρουσίαση με έναν εκπαιδευτικό τρόπο, ώστε να είναι εύκολα κατανοητή.
- Περιγράφουμε λεπτομερώς τα συμπεράσματα.
- Εξηγούμε με σαφήνεια τη διαδικασία που έχει ακολουθηθεί για την απόκτηση των αποδεικτικών στοιχείων.
- Αποφεύγουμε τις μη-αποδείξιμες επιβεβαιώσεις ή υποκειμενικές κρίσεις.
- Εκπονούμε-παρουσιάζουμε τα συμπεράσματα από μια αντικειμενική άποψη.

Θα πρέπει να σημειωθεί ότι οι φάσεις δεν είναι διαδοχικές αλλά επαναλαμβανόμενες και διαπλεκόμενες. Για παράδειγμα, η φάση της τεκμηρίωσης αρχίζει κατά τη διάρκεια της φάσης της διατήρησης.

ΤΜΗΜΑ 8
ΜΕΘΟΔΟΙ ΚΑΙ ΟΔΗΓΟΙ

Υπάρχουν διάφορες μέθοδοι και οδηγοί κατά την εκτέλεση μιας ψηφιακής εγκληματολογικής ανάλυσης, αλλά όλα έχουν κοινές πτυχές.

Παρακάτω είναι μια άλλη σειρά οδηγών που θα μπορούσαν να χρησιμοποιηθούν ως σημείο αναφοράς για αναγνώστες που ενδιαφέρονται να ψάξουν περαιτέρω το θέμα:

• *Guidelines for the best practices in the forensic examination of digital technology*[1]
• *Electronic Crime Scene Investigation: A Guide for First Responders*[2]
• *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*[3]

Μία γενικότερη προσέγγιση-μέθοδος της ψηφιακής εγκληματολογικής ανάλυσης θα μπορούσαν να αποτελέσουν τα παρακάτω βήματα:

1. Επιβεβαίωση συμβάντος (Verification)
2. Περιγραφή συστήματος (System description)
3. Συλλογή δεδομένων (Evidence Acquisition)
4. Χρονική ανάλυση δεδομένων (Timeline Analysis)
5. Ανάλυση συσκευών αποθήκευσης (Media analysis)
6. Αλφαριθμική αναζήτηση ή αναζήτηση κατά Byte
7. Αποκατάσταση δεδομένων (Data Recovery)
8. Αναφορά (Reporting)

Στον συγκεκριμένο οδηγό θα παρουσιάσουμε το τρίτο βήμα που αφορά την συλλογή δεδομένων, ενώ θα αναφερθούμε και στα δύο πρώτα, που αφορούν επιβεβαίωση συμβάντος και περιγραφή συστήματος.

Μία ακόμα γενική προσέγγιση περιγραφής βημάτων της ψηφιακής εγκληματολογικής ανάλυσης είναι και η ακόλουθη:

---

1 http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html
2 https://www.ncjrs.gov/pdffiles1/nij/187736.pdf
3 https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Φάση 1: Ανάκτηση, Διατήρηση (σωστή διαδικασία φύλαξης/επιμέλειας -chain of custody-) και εξέταση των πτητικών δεδομένων

Φάση 2: Ανάλυση της μνήμης

Φάση 3: Ανάλυση ψηφιακής σήμανσης: εξέταση της registry και των σκληρών δίσκων.

Φάση 4: Εντοπισμός και ανάλυση αγνώστων αρχείων

Φάση 5: Δυναμική και στατική ανάλυση ιομορφικού λογισμικού.

Εμείς θα επικεντρωθούμε στην πρώτη φάση: Ανάκτηση, Διατήρηση (σωστή διαδικασία φύλαξης-επιμέλειας -chain of custody) και εξέταση των πτητικών δεδομένων.

ΚΕΦΑΛΑΙΟ «Γ»
ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΑ

ΤΜΗΜΑ 9
ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΕΝΟΣ ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΟΥ

Υπάρχει μια πληθώρα περιστατικών που σχετίζονται με την παραβίαση της ασφάλειας υπολογιστών και δικτύων:

Λαμβάνοντας υπόψη τα κυβερνο-περιστατικά που πιθανών να κληθεί κάποιος επαγγελματίας να αντιμετωπίσει, αυτά μπορούν να προσδιοριστούν στις ακόλουθες περιπτώσεις:

- **Κλοπή πληροφοριών**: Η κλοπή προσωπικών ή πληροφοριών μιας επιχείρησης, είναι μία από τις σημαντικότερες ανησυχίες τόσο για τους χρήστες

όσο και για τις επιχειρήσεις. Υπάρχουν μια σειρά από τεχνικές που επιτρέπουν την κλοπή πληροφοριών, όπως η παρακολούθηση της κυκλοφορίας του δικτύου μέσω **sniffer**, η υποκλοπή των emails ή απλά η σύνδεση μιας συσκευής **usb** για αντιγραφή ιδιωτικών πληροφοριών, κλπ. Αυτές οι πληροφορίες χρησιμοποιούνται κυρίως για οικονομικό όφελος, αλλά σε ορισμένες περιπτώσεις, απλώς χρησιμοποιούνται για να βλάψουν την εικόνα του θιγόμενου μέρους.

- **Απάτη**: Υπάρχει ένας αριθμός παραδειγμάτων Διαδικτυακής Απάτης, όπως:

  - Ψευδείς προσφορές εργασίας.
  - Απάτες λοταρίας και βραβείων.
  - Ψευδείς κληρονομιές.
  - Απάτες επενδύσεων και πιστώσεων.
  - Ψευδή emails που ζητούν δωρεές σε ΜΚΟ.
  - Πλαστά τιμολόγια από υπηρεσίες μηνυμάτων.
  - Μεταφορτώσεις τιμολόγιων από υπηρεσίες SMS.
  - Πρόστιμα για παράνομες λήψεις (μεταφορτώσεις δεδομένων).

Καθ' όλη τη διάρκεια του χρόνου, ένας μεγάλος αριθμός παράνομων ενεργειών λαμβάνουν χώρα, αξιοποιώντας στο έπακρο τις σημαντικές ημερομηνίες ή τα γεγονότα, για να πολλαπλασιάσουν αυτά τα είδη των απειλών.

- **Ιομορφικό λογισμικό**: Το ιομορφικό λογισμικό είναι άλλο ένα από τα πιο χαρακτηριστικά περιστατικά που ένας αναλυτής ψηφιακού εγκλήματος μπορεί να συναντήσει. Η επαγγελματοποίηση της αγοράς έχει δημιουργήσει μια σημαντική αύξηση του όγκου αυτών των ειδών των απειλών, φθάνοντας σε πολύ εξελιγμένα επίπεδα σε ορισμένες περιπτώσεις. Μερικά από τα πιο σημαντικά στατιστικά είναι τα ακόλουθα:

  - Υπάρχουν σχεδόν 170 εκατομμύρια δείγματα κακόβουλου λογισμικού, εκ των οποίων σχεδόν 70 εκατομμύρια έχουν εμφανιστεί το 2013.
  - Αύξηση κατά 91% σε στοχευμένες επιθέσεις το 2013
  - Αύξηση κατά 62% στον αριθμό των παραβιάσεων για το 2013
  - Πάνω από 552 εκατομμύρια προσωπικές ταυτότητες εκτέθηκαν με παραβιάσεις το 2013
  - 23 zero-day ευπάθειες ανακαλύφθηκαν το 2013
  - 38% των χρηστών κινητής τηλεφωνίας έχουν βιώσει επίθεση στο κινητό τους, τους τελευταίους 12 μήνες
  - Ο όγκος των Spam μειώθηκε στο 66% του συνόλου της κίνησης των emails
  - 1 στα 392 μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν επιθέσεις phishing
  - Οι Web-based επιθέσεις έχουν αυξηθεί κατά 23%
  - 1 στις 8 νόμιμες ιστοσελίδες έχουν μια κρίσιμη ευπάθεια

Στην περίπτωση που έχουμε μόλυνση με ιομορφικό λογισμικό, τότε ο αντικειμενικός σκοπός της ψηφιακής σήμανσης είναι:

- Να ανακαλύψουμε την φύση και τον σκοπό του ιομορφικού λογισμικού
- Να καθορίσουμε τον μηχανισμό μόλυνσης
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με τον μολυσμένο υπολογιστή.
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με το δίκτυο
- Να καθορίσουμε πως ο κακόβουλος χρήστης αλληλεπιδρά με το ιομορφικό πρόγραμμα
- Να καθορίσουμε το σκεπτικό και το σκοπό της κυβερνοεπίθεσης, καθώς και το επίπεδο, το σχεδιασμό της επίθεσης.
- Να καθορίσουμε την έκταση της μόλυνσης του προσωπικού υπολογιστή αλλά και την επέκταση της μόλυνσης στο δίκτυο

- **Μη-εξουσιοδοτημένη πρόσβαση**: Σύμφωνα με μία μελέτη του ThreatTrack Security, η μη-εξουσιοδοτημένη πρόσβαση σε δικτυακούς τόπους με σεξουαλικό περιεχόμενο είναι ένας από τους κύριους λόγους μόλυνσης των εταιρικών υπολογιστών. Ένα άλλο παράδειγμα είναι η εκμετάλλευση τρωτοτήτων του λογισμικού για την απόκτηση προνομίων και πρόσβασης σε φακέλους και έγγραφα που περιέχουν εμπιστευτικές πληροφορίες.

- **Μη ορθή χρήση πόρων**: Η μη ορθή χρήση των πόρων είναι μία αρκετά συνήθης πρακτική στις επιχειρήσεις που μπορεί να τις εκθέσουν. Η εκτύπωση προσωπικών εγγράφων είναι ένα από τα πιο χαρακτηριστικά παραδείγματα.

- **Πνευματική ιδιοκτησία**: Η παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας έχει ως αποτέλεσμα ένα πολύ σημαντικό ετήσιο κόστος. Σύμφωνα με μια μελέτη για τις οικονομικές επιπτώσεις της εγκληματικότητας στον κυβερνοχώρο από τη McAfee, αυτό προκαλεί, σε παγκόσμιο επίπεδο, ζημίες μέχρι 400.000 εκατομμύρια δολάρια και ένας από τους κύριους λόγους είναι η κλοπή της πνευματικής ιδιοκτησίας. Υπάρχει ένας τεράστιος αριθμός ιστοσελίδων όπου μπορούμε να μεταφορτώσουμε ταινίες, μουσική, λογισμικό, κλπ, τα οποία έχουν άμεσο αντίκτυπο σε αυτές τις απώλειες.

- **Άρνηση παροχής υπηρεσιών (Denial-of-service)**: Μια επίθεση άρνησης παροχής υπηρεσιών στοχεύει να εμποδίσει την πρόσβαση σε υπηρεσίες και πόρους ενός οργανισμού. Αυτά τα είδη των επιθέσεων συνήθως διαπράττονται μέσω της χρήσης των botnets (δίκτυα μολυσμένων υπολογιστών) ή με την εκμετάλλευση αδυναμιών των υπηρεσιών και έχουν αυξηθεί σημαντικά τα τελευταία χρόνια, μερικές φορές προκαλούνται από ενέργειες χακτιβιστών (hacktivist actions).

Παρά την ποικιλομορφία των κυβερνο-περιστατικών, η διαδικασία που ακολουθείται κατά τη συγκέντρωση των αποδεικτικών στοιχείων είναι κοινή στην πλειονότητα των περιπτώσεων. Πρέπει να έχουμε κατά νου ότι η ανάλυση που ακολουθεί, θα είναι συγκεκριμένη και διαφορετική, ανάλογα με τον τύπο του κυβερνο-περιστατικού.

Υπάρχουν και άλλα είδη περιστατικών, που σχετίζονται κυρίως με την παιδική πορνογραφία, κυβερνοτρομοκρατία, εκβιασμούς (η ομάδα αυτή περιλαμβάνει την παρενόχληση στον κυβερνοχώρο -cyberharassment-), τον εκφοβισμό στον κυβερνοχώρο (cyberbullying), η αποπλάνηση ανηλίκου, το sexting ή την σεξουαλική παρενόχληση (intimacy infringement)], κλπ, τα οποία πρέπει να διαβιβάζονται στις αρμόδιες αρχές για να ξεκινούν την έρευνα και να λαμβάνουν τα μέτρα που κρίνουν κατάλληλα. Αυτά τα είδη των περιστατικών είναι πέρα από το αντικείμενο του συγκεκριμένου οδηγού. Στην πραγματικότητα, μερικά από τα περιστατικά που περιγράφονται σε αυτό το σημείο μπορεί να απαιτούν τη διαβίβασή τους στις αρχές, όπως εκείνα που σχετίζονται με την κλοπή πληροφοριών ή την απάτη. Για όλα αυτά θα πρέπει να ερχόμαστε σε επαφή με την Δίωξη Ηλεκτρονικού Εγκλήματος και να ακολουθούμε τα βήματα που θα μας υποδείξουν.

ΚΕΦΑΛΑΙΟ «Δ»
ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΟΔΗΓΙΕΣ ΓΙΑ ΤΗ ΣΥΛΛΟΓΗ ΚΑΙ ΑΠΟΘΗΚΕΥΣΗ ΤΩΝ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Το *RFC 3227* είναι ένα έγγραφο που περιλαμβάνει τις «*κατευθυντήριες γραμμές για τη συλλογή και αποθήκευση αποδεικτικών στοιχείων*» και μπορεί να χρησιμοποιηθεί ως πρότυπο για τη συλλογή πληροφοριών σε περιστατικά ασφαλείας.

Το έγγραφο περιλαμβάνει τις παρακάτω ενότητες:

ΤΜΗΜΑ 10
ΑΡΧΕΣ ΚΑΤΑ ΤΗ ΣΥΓΚΕΝΤΡΩΣΗ ΤΩΝ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

- Ανακτούμε ένα ακριβές αντίγραφο του συστήματος που θα είναι όσο το δυνατόν πιο πιστό αντίγραφο.
- Κρατούμε λεπτομερείς σημειώσεις, συμπεριλαμβανομένων ημερομηνιών και ωρών που αναγράφονται εάν χρησιμοποιείται η τοπική ή η παγκόσμια (UTC) ώρα.
- Ελαχιστοποιούμε τις αλλαγές στις πληροφορίες που έχουν συγκεντρωθεί και εξαλείφουμε εξωτερικούς παράγοντες που μπορεί να πραγματοποιήσουν αλλαγές.
- Αν αντιμετωπίζουμε ένα δίλημμα μεταξύ συλλογής και ανάλυσης, επιλέγουμε πρώτα συλλογή και δεύτερον ανάλυση.
- Συγκεντρώνουμε τις πληροφορίες ανάλογα με τη σειρά της πτητικότητας/μεταβλητότητας (από τις περισσότερο στις λιγότερο μεταβλητές).
- Λαμβάνουμε υπόψιν ότι με κάθε συσκευή η συλλογή πληροφοριών μπορεί να πραγματοποιηθεί με έναν διαφορετικό τρόπο.

Η σειρά μεταβλητότητας (Volatility order)

Η σειρά μεταβλητότητας αναφέρεται στο χρονικό διάστημα κατά το οποίο ορισμένες πληροφορίες είναι προσβάσιμες. Ως εκ τούτου, είναι απαραίτητο να συγκεντρωθούν πρώτες οι πληροφορίες που πρόκειται να είναι διαθέσιμες για τον ελάχιστο χρόνο, με άλλα λόγια, οι πληροφορίες με τη μεγαλύτερη μεταβλητότητα.

Ακολουθώντας αυτή την σειρά, μπορεί να δημιουργηθεί η ακόλουθη λίστα από το περισσότερο στο λιγότερο μεταβλητό:

- Περιεχόμενα μητρώου (registers) και μνήμης (cache).
- Πίνακας δρομολόγησης (Routing table), ARP μνήμη (ARP cache), πίνακας διεργασιών (process table), στατιστικά στοιχεία του πυρήνα (kernel statistics), και μνήμη.
- Προσωρινές πληροφορίες στο σύστημα.
- Δίσκος.
- Αρχεία καταγραφής συστήματος.
- Φυσική διαμόρφωση και τοπολογία του δικτύου.
- Έγγραφα.

Ενέργειες που πρέπει να αποφεύγονται

Οι παρακάτω ενέργειες πρέπει να αποφεύγονται για να μην ακυρώσουν τη διαδικασία συλλογής πληροφοριών, δεδομένου ότι πρέπει να διατηρηθεί η ακεραιότητά τους, έτσι ώστε τα λαμβανόμενα αποτελέσματα να μπορούν να χρησιμοποιηθούν στο δικαστήριο, εάν χρειαστεί:

- Δεν απενεργοποιούμε τον υπολογιστή μέχρι να συλλεχθούν όλες οι μεταβλητές-πτητικές πληροφορίες.
- Δεν εμπιστευόμαστε τις πληροφορίες που παρέχονται από το λογισμικό του συστήματος, καθώς ενδέχεται να έχει μολυνθεί. Οι πληροφορίες πρέπει να συλλέγονται μέσω λογισμικού που είναι αποθηκευμένο σε ένα προστατευμένο μέσο (USB, CD-ROM), όπως θα εξηγηθεί στη συνέχεια.
- Δεν εκτελούμε λογισμικό που τροποποιεί την ημερομηνία και την ώρα της πρόσβασης όλων των αρχείων του συστήματος.

Θέματα προστασίας προσωπικών δεδομένων (Privacy considerations)

Όλες οι πληροφορίες που συγκεντρώθηκαν κατά τη διάρκεια της διαδικασίας, θα πρέπει να είναι εγγυημένο πως θα αντιμετωπίζονται μέσα στο θεσπισμένο νομικό πλαίσιο, διατηρώντας την απαιτούμενη προστασία προσωπικών δεδομένων. Τα αρχεία καταγραφής συμβάντων περιλαμβάνονται σε αυτό το πλαίσιο προστασίας προσωπικών δεδομένων, καθώς μπορούν να αποθηκεύουν τα μοτίβα συμπεριφοράς του χρήστη του συστήματος.

Νομικά ζητήματα/σκέψεις (Legal considerations)

Πρέπει να σημειωθεί πως ο νόμος είναι διαφορετικός σε κάθε χώρα, έτσι τα αποδεικτικά στοιχεία μπορούν να γίνουν αποδεκτά σε μία χώρα και σε μία άλλη όχι. Σε κάθε περίπτωση, τα αποδεικτικά στοιχεία πρέπει να έχουν μια σειρά από κοινά χαρακτηριστικά.

- **Αποδεκτά**: η ισχύουσα νομοθεσία πρέπει να γίνεται σεβαστή για να έχουν τα αποδεικτικά στοιχεία μια δικαστική αξία.

- **Αυθεντικά**: πρέπει να είναι ευαπόδεικτο ότι τα αποδεικτικά στοιχεία αντιστοιχούν στο εν λόγω περιστατικό.
- **Ολοκληρωμένα**: πρέπει να αντιστοιχούν στο σύνολο των πληροφοριών και όχι απλώς σε μια μερική άποψη.
- **Αξιόπιστα**: δεν πρέπει να υπάρχουν αμφιβολίες ως προς το πώς προέκυψαν τα αποδεικτικά στοιχεία ή σχετικά με οποιοδήποτε μεταγενέστερο χειρισμό που θα μπορούσαν να εγείρουν αμφιβολίες σχετικά με την αυθεντικότητα και την ειλικρίνειά τους.
- **Αξιόπιστα/Σαφή**: πρέπει να είναι εύλογα και εύκολα κατανοητά για τον δικαστή στο δικαστήριο.

ΤΜΗΜΑ 11
ΔΙΑΔΙΚΑΣΙΑ ΣΥΛΛΟΓΗΣ

Η διαδικασία συλλογής πρέπει να είναι όσο το δυνατόν **πιο λεπτομερής**, εξασφαλίζοντας ότι δεν είναι διφορούμενη, δεν εμφανίζονται διλήμματα που θα απαιτούν αποφάσεις με λίγα λόγια επιδιώκουμε την μείωση/ αποφυγή λήψης αποφάσεων όσο το δυνατόν περισσότερο. Οι μέθοδοι που χρησιμοποιούνται για τη συλλογή των αποδεικτικών στοιχείων πρέπει να είναι διαφανείς και **αναπαράξιμες**. Θα πρέπει να είμαστε έτοιμοι να αναπαράξουμε με ακρίβεια τις μεθόδους που χρησιμοποιήθηκαν, και οι μέθοδοι αυτές πρέπει να έχουν ελεγχθεί από ανεξάρτητους εμπειρογνώμονες.

Βήματα

- Που είναι τα αποδεικτικά στοιχεία; Κάνουμε μια λίστα των συστημάτων που εμπλέκονται στο περιστατικό και αυτών που μπορούν να χρησιμοποιηθούν για την εξαγωγή στοιχείων.
- Καθορίζουμε τι είναι σχετικό. Σε περίπτωση αμφιβολίας, είναι καλύτερο να συγκεντρώσουμε περισσότερες πληροφορίες παρά ελλειπείς.
- Ορίζουμε τη σειρά μεταβλητότητας για κάθε σύστημα.
- Συλλέγουμε τις πληροφορίες σύμφωνα με την καθορισμένη σειρά.
- Επιβεβαιώνουμε το επίπεδο συγχρονισμού του ρολογιού του συστήματος.
- Καθώς γίνονται τα βήματα συλλογής αναρωτιόμαστε τι επιπλέον θα μπορούσε να αποτελέσει αποδεικτικό στοιχείο.
- Καταγράφουμε κάθε μας βήμα.
- Δεν ξεχνάμε τους ανθρώπους που εμπλέκονται. Σημειώνουμε ποιοι ήταν εκεί, τι έκαναν, τι έψαχναν και πως αντέδρασαν.

ΤΜΗΜΑ 12
Η ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΑΠΟΘΗΚΕΥΣΗΣ

Αλυσίδα παρακολούθησης

Η αλυσίδα παρακολούθησης πρέπει να τεκμηριώνεται/καταγράφεται σαφώς και τα ακόλουθα σημεία να προσδιορίζονται με λεπτομέρεια:

- Που, πότε και ποιος ανακάλυψε και συγκέντρωσε τα αποδεικτικά

στοιχεία;

- Που, πότε και ποιος χειρίστηκε τα αποδεικτικά στοιχεία;
- Ποιος φύλαγε τα αποδεικτικά στοιχεία; Για πόσο καιρό; Και πώς τα αποθήκευε;
- Εάν τα αποδεικτικά στοιχεία άλλαξαν επιμέλεια / χέρια φύλαξης/παρακολούθησης, θα πρέπει να υποδείξουμε πότε και πώς έλαβε χώρα η ανταλλαγή, συμπεριλαμβανομένου του αριθμού δελτίου παράδοσης, κλπ.

<u>Που και πώς αποθηκεύουμε τις πληροφορίες</u>

Οι πληροφορίες πρέπει να αποθηκεύονται σε συσκευές με ένα επίπεδο ασφάλειας που έχει αποδειχθεί και που μπορεί να ανιχνεύσει μη εξουσιοδοτημένες απόπειρες πρόσβασης. Τα δεδομένα θα πρέπει να μεταφερθούν σε ένα εξωτερικό αποθηκευτικό μέσο, με συγκεκριμένη σειρά, ξεκινώντας από την μνήμη και πραγματοποιώντας συνεχώς έλεγχο ακεραιότητας. Τα πρώτα δεδομένα που συλλέγουμε στην περίπτωση που το σύστημα είναι ενεργό, είναι τα δεδομένα που θα χαθούν μόλις τεθεί εκτός λειτουργίας ο υπολογιστής (π.χ μνήμη).

ΤΜΗΜΑ 13
ΑΠΑΡΑΙΤΗΤΑ ΕΡΓΑΛΕΙΑ

Υπάρχει μια σειρά από κατευθυντήριες γραμμές που πρέπει να ακολουθούνται κατά την επιλογή των εργαλείων που πρόκειται να χρησιμοποιηθούν για τη διαδικασία της συλλογής:

- Εργαλεία που είναι εξωτερικά (εκτός συστήματος) από το σύστημα θα πρέπει να χρησιμοποιούνται, διότι θεωρούμε δεδομένο πως τα αντίστοιχα εργαλεία του συστήματος έχουν μολυνθεί.
- Θα πρέπει να χρησιμοποιούνται εργαλεία που αλλάζουν την υπόθεση – περιστατικό όσο το δυνατόν λιγότερο. Συγκεκριμένα, να αποφεύγουμε, όταν είναι δυνατό, τη χρήση των εργαλείων γραφικού περιβάλλοντος και των εργαλείων με μεγάλη κατανάλωση μνήμης.
- Το λογισμικό που πρόκειται να χρησιμοποιηθεί για τη συγκέντρωση αποδεικτικών στοιχείων πρέπει να βρίσκεται σε μία εξωτερική συσκευή ανάγνωσης (CD-ROM, USB, κλπ).
- Ένας συνδυασμός εργαλείων, κατάλληλων για τα λειτουργικά συστήματα-στόχους θα πρέπει να είναι έτοιμος από πριν και να έχουν προ-ελεγχθεί.
- Η εργαλειοθήκη ανάλυσης θα πρέπει να περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα είδη εργαλείων:
  - Λογισμικό για την καταγραφή και εξέταση των διαδικασιών.
  - Λογισμικό για την εξέταση της κατάστασης του συστήματος.
  - Λογισμικό για να πραγματοποιεί αντίγραφα σε χαμηλό επίπεδο, δηλαδή **bit by bit**.

ΤΜΗΜΑ 14
ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά τη διεξαγωγή της διαδικασίας συλλογής πληροφοριών σε ένα σύστημα που έχει υποστεί ένα περιστατικό ασφαλείας, είναι απαραίτητο να έχουμε μια σαφή ιδέα για το τι ενέργειες πρέπει να διεξαχθούν, όντας πολύ σχολαστικοί και καταγράφοντας λεπτομερώς αυτή τη διαδικασία ανά πάσα στιγμή. Επομένως, η διαδικασία πρέπει να διεξαχθεί προσπαθώντας να είναι όσο το δυνατόν πιο διακριτική, προκειμένου να διατηρηθεί το σύστημα στην αρχική του κατάσταση (ή με τις ελάχιστες αλλαγές που ωστόσο μπορούμε να τις τεκμηριώσουμε).

ΚΕΦΑΛΑΙΟ «Ε»
ΣΥΓΚΕΝΤΡΩΣΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Ένα από τα κύρια καθήκοντα – απαιτήσεις, κατά τη διενέργεια ψηφιακής εγκληματολογικής ανάλυσης, είναι να έχουμε μια σαφή ιδέα για το συγκεκριμένο είδος του κυβερνο-περιστατικού και στην συνέχεια να γνωρίζουμε τι πληροφορίες είναι απαραίτητες να συλλέξουμε και πώς θα προχωρήσουμε. Υπάρχουν κοινές διαδικασίες, αλλά δεν είναι το ίδιο να πραγματοποιούμε μια ψηφιακή εγκληματολογική ανάλυση σε μια περίπτωση ιομορφικού λογισμικού από ότι σε μια υπόθεση απάτης, δεδομένου ότι τα σημεία που ο ερευνητής πρέπει να επικεντρωθεί για να εντοπίσει αποδεικτικά στοιχεία είναι διαφορετικά.

Προφανώς, μερικά από τα βήματα που υποδεικνύονται προηγουμένως μπορεί να μην είναι απαραίτητα, όπως το να πρέπει να παρουσιάσουμε αποδεικτικά στοιχεία στο δικαστήριο, έτσι ώστε τελικά η τεκμηρίωση να μην πρέπει να είναι τόσο πολύ εξαντλητική, ωστόσο συνιστάται να διεξαχθεί η διαδικασία από μία επαγγελματική και αναπόσπαστη άποψη και για αυτό να είναι όσο το δυνατόν πληρέστερη. Εναπόκειται στον αναγνώστη να καθορίσει ποιες πτυχές θα λάβει υπόψη του, ανάλογα με την κατάσταση που θα πρέπει να αναλύσει, και ποια βήματα θα ακολουθήσει.

ΤΜΗΜΑ 15
ΖΗΤΗΜΑΤΑ/ΕΞΕΤΑΣΕΙΣ/ΣΚΕΨΕΙΣ ΠΡΙΝ ΤΗΝ ΣΥΛΛΟΓΗ

Υπάρχουν μια σειρά από ζητήματα/εξετάσεις/σκέψεις που πρέπει να έχουμε κατά νου πριν από την έναρξη της διαδικασίας συλλογής αποδεικτικών στοιχείων:

- Αρχικά, δεν αγγίζουμε τον υπολογιστή. Τον αφήνουμε ακριβώς όπως είναι, δεν ανοίγουμε αρχεία, δεν εκτελούμε λογισμικό, δεν διαγράφουμε φακέλους, κλπ. Εάν είναι ενεργοποιημένος δεν τον απενεργοποιούμε, και εάν είναι απενεργοποιημένος δεν τον ενεργοποιούμε. Πρέπει να έχουμε κατά νου ότι υπάρχει μεγάλος όγκος μεταβαλλόμενων πληροφοριών (προσωρινής αποθήκευσης), ο οποίος θα διαγραφεί εάν απενεργοποιηθεί ο υπολογιστής. Κατά συνέπεια αν ο υπολογιστής απενεργοποιηθεί, η απενεργοποίηση του θα οδηγούσε στην απώλεια πολύ σημαντικών πληροφοριών. Ομοίως, αν είναι απενεργοποιημένος η ενεργοποίησή του θα μπορούσε να οδηγήσει στην

τροποποίηση των ημερομηνιών ή στην απόκρυψη αρχείων αν υπάρχει rootkit.

• Καθιερώνουμε τα γενικά βήματα που πρόκειται να ακολουθηθούν, με στόχο να έχουμε μια συγκεκριμένη κατευθυντήρια γραμμή περιγραφής και εφαρμογής της διαδικασίας συλλογής πληροφοριών και προσέχουμε να μην ξεχνάμε κανέναν βήμα.

• Θα πρέπει να διαθέτουμε μία λεπτομερή περιγραφή των βημάτων της διαδικασίας που πρόκειται να ακολουθήσουμε. Σε αυτό το σημείο, θα πρέπει να λαμβάνονται υπόψη όλες οι πτυχές, όπως ο εκτιμώμενος χρόνος που θα πάρει η ανάλυση, ο επείγων χαρακτήρας της ανάλυσης ή οι αναγκαίοι πόροι για να πραγματοποιηθεί.

• Θα πρέπει να προβλέπουμε και να ελαχιστοποιούμε τους κινδύνους με σκοπό να διασφαλίσουμε, πως στην περίπτωση που θα αυτά προκύψουν προβλήματα δεν θα επηρεάσουν σημαντικά τη διαδικασία με αρνητικό τρόπο.

• Εκτιμούμε εάν το πρόσωπο που είναι υπεύθυνο για τη διεξαγωγή της διαδικασίας έχει την ικανότητα και τις γνώσεις που απαιτούνται για να την πράξει. Αν έχουμε αμφιβολία για την ικανότητά του να την πραγματοποιήσει, το καλύτερο πράγμα που πρέπει να κάνουμε είναι να συμβουλευτούμε κάποιον με εμπειρία και ευρεία γνώση, με σκοπό την παροχή συμβουλών του επί της διαδικασίας με σκοπό την προστασία των δεδομένων και την αποφυγή καταστροφής ή αλλοίωσης αποδεικτικών στοιχείων.

• Θα πρέπει να διαθέτουμε γραπτή άδεια για να είμαστε σε θέση να πραγματοποιήσουμε την ανάλυση και τη συλλογή των αποδεικτικών στοιχείων. Αυτή είναι μια θεμελιώδης αρχή, καθώς εμπιστευτικές πληροφορίες ή ζωτικής σημασίας δεδομένα για μια επιχείρηση θα μπορούσαν να ανακτηθούν κατά την διαδικασία. Θα μπορούσε παράλληλα να επηρεαστεί η διαθεσιμότητα των υπηρεσιών της επιχείρησης από το έργο του εγκληματολογικού ερευνητή. Σε ορισμένα είδη περιστατικών, θα είναι απαραίτητο να ζητηθεί δικαστική άδεια με σκοπό τη διασφάλιση της εγκυρότητας των συγκεντρωθέντων αποδεικτικών στοιχείων σε μια μελλοντική δικαστική υπόθεση.

• Ζητάμε τους απαραίτητους κωδικούς πρόσβασης για να αποκτήσουμε πρόσβαση σε κρυπτογραφημένα αρχεία ή δίσκους (volumes) ή ζητάμε να είναι παρών ο διαχειριστής που κατέχει τους κωδικούς.

• Έχουμε προετοιμάσει μια πλήρη συλλογή εργαλείων για να εφαρμόσουμε όλη την διαδικασία συλλογής αποδεικτικών στοιχείων χωρίς κανένα εμπόδιο.

• Ετοιμάζουμε μια λίστα των ανθρώπων που πρέπει να ενημερώνονται και να διατηρούνται στον κύκλο της διαδικασίας, συμπεριλαμβανομένων του ονόματός τους, της διεύθυνσης ηλεκτρονικού ταχυδρομείου, καθώς και κάθε άλλο είδος πληροφορίας που θα μπορούσε να είναι σχετική.

Η διαδικασία συλλογής αποδεικτικών στοιχείων μπορεί να ξεκινήσει, μόλις

έχουμε ξεκαθαρίσει και αξιολογήσει το είδος του κυβερνο-περιστατικού και τα βήματα που πρέπει να ληφθούν για την επίλυσή του.

ΤΜΗΜΑ 16
ΕΝΑΡΞΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ

Το πρώτο καθήκον είναι να κάνουμε καταγραφή-απογραφή (tag) του υλικού. Καταγράφουμε και φωτογραφίζουμε κάθε συσκευή που πρόκειται να αναλυθεί: σκληρούς δίσκους, pen drives, φωτογραφικές μηχανές, κλπ. Επίσης, ανάλογα με το είδος του περιστατικού, μπορεί να είναι απαραίτητο να συμπεριλάβουμε δρομολογητές, σαρωτές, εκτυπωτές, κλπ. Πρέπει να σημειωθούν, από όλα, η μάρκα, το μοντέλο, ο σειριακός αριθμός, ο τύπος της σύνδεσης (USB, firewire, κλπ). Ομοίως, θα πρέπει να καταγραφούν οι πληροφορίες του προσώπου που είναι υπεύθυνο για το σύστημα και ο χρήστης ή οι χρήστες που εργάζονται σε αυτό, καθώς και κάθε άλλη σχετική πληροφορία θα πρέπει να καταγραφεί. Θα πρέπει να σημειωθεί και το όνομα του χρήστη που εργαζόταν στο συγκεκριμένο σύστημα όταν καταγράφτηκε το γεγονός/περιστατικό. Η αλυσίδα της παρακολούθησης/επιμέλειας είναι θεμελιώδης, διότι αποδεικνύει ότι τα ληφθέντα αποδεικτικά στοιχεία δεν έχουν παραποιηθεί. Είναι υποχρεωτική η ιδιαίτερη σχολαστικότητα με την οποία διαχειριζόμαστε τα δεδομένα που συλλέγουμε. Για να γίνει αυτό, είναι απαραίτητο να καταγράψουμε όλα τα αποδεικτικά στοιχεία που ελήφθησαν.

Στις παρατηρήσεις, είναι σημαντικό να δικαιολογήσουμε το λόγο ως προς το γιατί τα προαναφερθέντα αποδεικτικά στοιχεία έχουν συλλεχθεί. Ο στόχος αυτού του βήματος είναι να διευκολύνει το έργο του αναλυτή, αν ο ίδιος ο ερευνητής δεν είναι το πρόσωπο που εκτελεί το ρόλο αυτό.

Από τη στιγμή που όλες οι συσκευές έχουν καταγραφεί, απογραφεί και φωτογραφηθεί, τα αποδεικτικά στοιχεία μπορούν να αρχίσουν να συγκεντρώνονται. Κατά ένα γενικό τρόπο, το είδος των αποκτηθέντων πληροφοριών μπορούν να ταξινομηθούν σε δύο μεγάλες ομάδες: μεταβλητές / πτητικές πληροφορίες (προσωρινής αποθήκευσης) και μη-μεταβλητές πληροφορίες (μόνιμης αποθήκευσης). Μπορούμε επίσης να μιλήσουμε για ζωντανή-ενεργή απόκτηση πληροφοριών που αντιστοιχεί στη συγκέντρωση των πληροφοριών σε ένα σύστημα που λειτουργεί, καθώς και για στατική απόκτηση πληροφοριών που αντιστοιχεί στη συγκέντρωση των πληροφοριών σε ένα σύστημα που είναι απενεργοποιημένο.

Σημαντικό

Για να πραγματοποιήσουμε μια σωστή συλλογή αποδεικτικών στοιχείων, είναι σημαντικό να χρησιμοποιήσουμε "καθαρό" μη μολυσμένο λογισμικό που μπορεί να το έχουμε σε συσκευές που προστατεύονται από την εγγραφή (pen drive, CD-ROM, κλπ.). Ομοίως, αν υπάρχει υποψία ότι το σύστημα έχει παραβιαστεί/προσβληθεί από ιομορφικό λογισμικό, τότε οι πληροφορίες πρέπει να συλλέγονται με την χρήση στατικών εκτελέσιμων αρχείων και όχι με την χρήση των APIs του συστήματος, διότι η ακεραιότητα των τελευταίων ενδέχεται να έχει αλλοιωθεί και δεν θα παρουσιάζουν τα

πραγματικά αποτελέσματα.

Στην συνέχεια παρουσιάζονται μια σειρά από ελεύθερα λογισμικά και live CDs που μπορούν να χρησιμοποιηθούν δωρεάν κατά την διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης. Ωστόσο ανάλογα με την εμπειρία του ερευνητή, μπορεί ο ίδιος να δημιουργήσει μία αντίστοιχη εργαλειοθήκη σύμφωνα με τις ανάγκες του.

Όνομα	URL
SIFT	SANS Investigative Forensic Toolkit (SIFT) http://digital-forensics.sans.org/community/downloads
Caine	http://www.caine-live.net
Digital Forensics Framework	http://www.digital-forensic.org
The Sleuth Kit y AutoSpy	http://www.sleuthkit.org
Helix Live CD	http://www.e-fense.com
Forensic and Incident Response Environment (F.I.R.E)	http://fire.dmzs.com
Digital Evidence & Forensic Toolkit	http://www.deftlinux.net

Πίνακας 1: Λίστα από open source συλλογές εργαλείων για την ψηφιακή εγκληματολογική ανάλυση.

Σημείωση

Συνήθως, είναι δυνατό να λαμβάνουμε μόνο ένα αντίγραφο της μνήμης (memory dump) και μόνο ένα αντίγραφο του δίσκου (disk dump), και από εκεί να εργαζόμαστε σε διαφορετικά αντίγραφα για να αποκτήσουμε το υπόλοιπο των αποδεικτικών στοιχείων. Η συλλογή πληροφοριών εξαρτάται από την υπόθεση και ανάλογα με την περίπτωση, μπορεί να μην είναι απαραίτητο να πραγματοποιήσουμε έναν ολικό αντίγραφο του συνόλου των πληροφοριών, αλλά μια απλή συλλογή συγκεκριμένων πληροφοριών να μας βοηθήσουν να επιλύσουμε την υπόθεση.

ΤΜΗΜΑ 17
ΜΕΤΑΒΛΗΤΕΣ (ΠΡΟΣΩΡΙΝΗΣ ΑΠΟΘΗΚΕΥΣΗΣ) ΠΛΗΡΟΦΟΡΙΕΣ

Όπως υποδείχθηκε προηγουμένως, οι μεταβλητές - πτητικές πληροφορίες (προσωρινής αποθήκευσης), είναι πολύ σημαντικές κατά την εκτέλεση της ψηφιακής εγκληματολογικής ανάλυσης, διότι ενδέχεται να περιέχουν αποδεικτικά στοιχεία συνδέσεων, διεργασιών, υπηρεσιών, κλπ. Η απώλεια αυτού του είδους των πληροφοριών θα μπορούσε να σημαίνει ότι η ψηφιακή εγκληματολογική ανάλυση δεν έχει ολοκληρωθεί με επιτυχία ή ότι η διαδικασία θα γίνει περίπλοκη σε μεγάλο βαθμό, διότι θα λείπουν δεδομένα. Αυτός είναι ο λόγος, όπως το *RFC 3227* υποδεικνύει, που τα μεταβλητά αποδεικτικά στοιχεία πρέπει υποχρεωτικά να συγκεντρώνονται. Ακολούθως, υποδεικνύεται η μέθοδος που πρέπει να χρησιμοποιείται, και παρουσιάζονται μερικά παραδείγματα περιστατικών όπου θα μπορούσαν να είναι χρήσιμα. Με αυτόν τον τρόπο, ο υπεύθυνος που πραγματοποιεί τη διαδικασία, μπορεί να συμπληρώσει τα βήματα που θεωρεί κατάλληλα, χρησιμοποιώντας τις κατευθυντήριες οδηγίες που δίνονται εδώ ως

βάση.

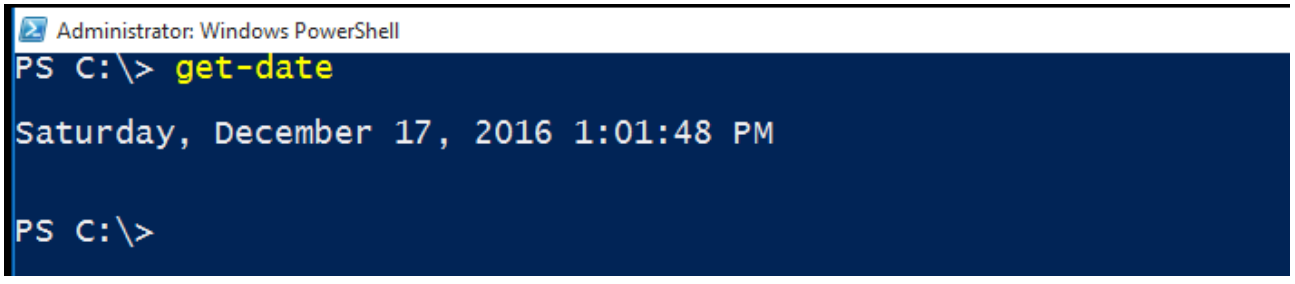
Ώρα και ημερομηνία του συστήματος

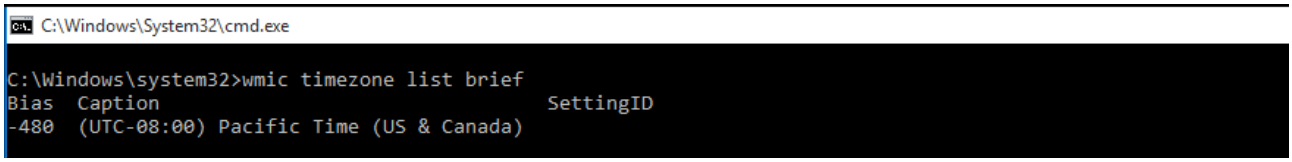
Όσον αφορά τις μεταβλητές πληροφορίες, το πρώτο πράγμα που πρέπει να αποκτηθεί είναι η ημερομηνία και η ώρα του συστήματος, προκειμένου να καθορίσουμε ένα χρονοδιάγραμμα της συλλογής των αποδεικτικών στοιχείων, τη διάρκεια της διαδικασίας, κλπ.

Για να γίνει αυτό, δίνουμε την ακόλουθη εντολή από μία ασφαλή κονσόλα γραμμής εντολών (secure Shell command):

c:\> **date /t > TimeInfo.txt & time /t >> TimeInfo.txt**

Εναλλακτικά μπορούμε να δώσουμε για την συγκέντρωση των χρονικών πληροφοριών του συστήματος τις ακόλουθες εντολές:
C:\> net time
C:\> date /t
C:\> time /t
C:\>echo %DATE% %TIME%
C:\>wmic timezone list brief
PS C:\> Get-Date | Out-File TimeInfo.txt
c:**> w32tm /tz** (για να γνωρίζουμε την Ωρική Ζώνη)





```
c:\>w32tm /tz
Time zone: Current:TIME_ZONE_ID_STANDARD Bias: 480min (UTC=LocalTime+Bias)
  [Standard Name:"Pacific Standard Time" Bias:0min Date:(M:11 D:1 DoW:0)]
  [Daylight Name:"Pacific Daylight Time" Bias:-60min Date:(M:3 D:2 DoW:0)]
```

Η ληφθείσα ημερομηνία πρέπει να συγκριθεί με τη συντονισμένη παγκόσμια ώρα (UTC), ένα πρότυπο της ώρας που ρυθμίζει την ώρα παγκοσμίως, για να προσδιοριστεί αν η καθιερωμένη ημερομηνία στο σύστημα είναι σωστή ή όχι και τι απόκλιση υπάρχει.

Θα πρέπει επίσης να έχουμε κατά νου, ότι τα FAT συστήματα αποθηκεύουν τις τιμές της ώρας ανάλογα με την τοπική ώρα του υπολογιστή, ενώ τα συστήματα NTFS τις αποθηκεύουν σε μορφή UTC. Αυτό σημαίνει ότι, ενώ τα NTFS συστήματα δεν επηρεάζονται από τις αλλαγές σε μια ζώνη ώρας ή σε θερινή/χειμερινή ώρα, τα FAT συστήματα θα έχουν διαφορετική τιμή, αν προβάλλονται στη μια περιοχή ή σε μια άλλη με διαφορετική ζώνη ώρας, ή αν προβάλλονται το καλοκαίρι ή το χειμώνα.

Ανάκτηση των Prefetch, Superfetch, RecentFileCache.bcf, αρχείων – πληροφοριών

Τα πρώτα δεδομένα που συλλέγουμε, πριν τροποποιηθούν από τις ενέργειές μας, είναι τα Prefetch, Superfetch, RecentFileCache.bcf αρχεία. Τα Windows Prefetch αρχεία, εμφανίστηκαν για πρώτη φορά στα Windows XP και έχουν σχεδιαστεί για να επιταχύνουν τη διαδικασία εκκίνησης μιας εφαρμογής. Τα Prefetch αρχεία περιέχουν το όνομα του εκτελέσιμου, μια Unicode λίστα με αρχεία DLL που χρησιμοποιούνται από το εν λόγω εκτελέσιμο, έναν αριθμό που δείχνει πόσες φορές έχει "τρέξει" το εκτελέσιμο και μια χρονική σήμανση που υποδεικνύει την τελευταία φορά που το πρόγραμμα εκτελέστηκε. Κάθε εφαρμογή έχει ένα αντίστοιχο αρχείο με extension PF, που αποθηκεύει πληροφορίες όπως το όνομα του εκτελέσιμου, τον αριθμό των φορών που έχει εκτελεστεί, τις βιβλιοθήκες, τον χρόνο εκτέλεσης κλπ. Τα Prefetch αρχεία βρίσκονται επίσης στα Windows 10, τα οποία έχουν βελτιωθεί και παρουσιάζονται ως SuperFetch, ReadyBoot και ReadyBoost. Εντολές και εργαλεία:

C:\> **winprefetchview.exe /shtml**
c:\> **forecopy_handy -p <directory_to_save>**

c:\> **forecopy_handy -f %SystemRoot%\AppCompat\Programs\RecentFileCache.bcf <directory_to_save>**

Άλλα εργαλεία

PrefetchForensics	http://www.woanware.co.uk/forensics/prefetchforensics.html
Windows Prefetch Parser (pf)	https://tzworks.net/prototype_page.php?proto_id=1
forecopy_handy	https://github.com/proneer/Tools/tree/master/forecopy

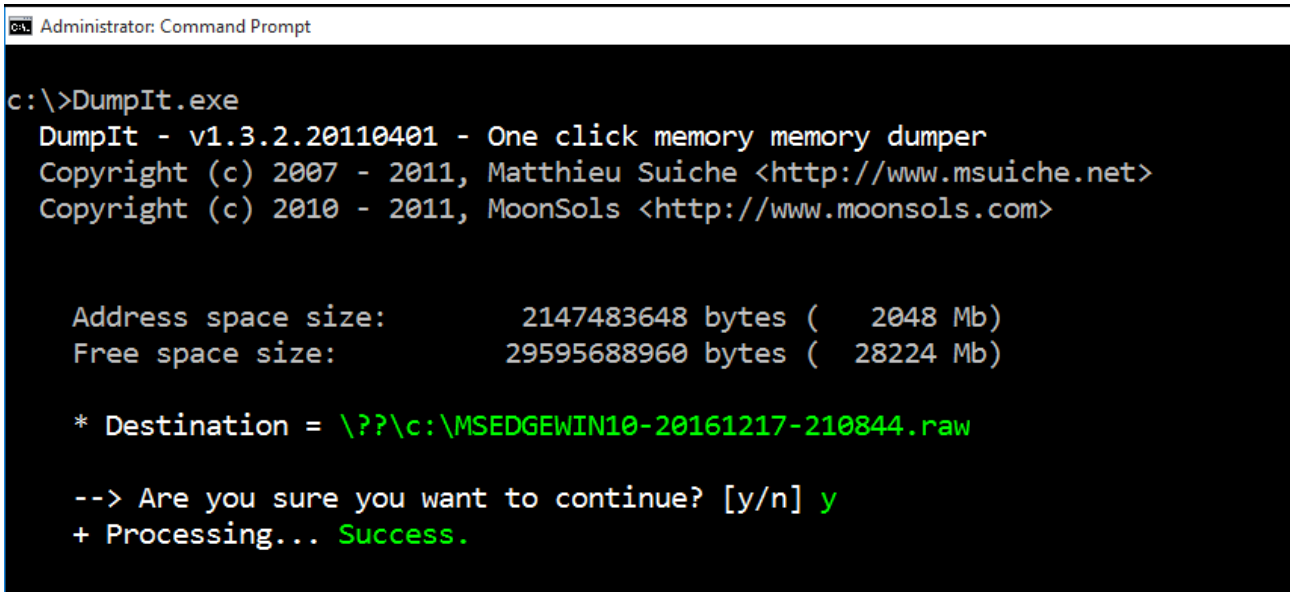
Λήψη αντιγράφου φυσικής μνήμης (memory dump)

Η λήψη αντιγράφου μνήμης (memory dumping) είναι μία από τις πιο σημαντικές και κρίσιμες ενέργειες στη φάση συλλογής των πληροφοριών. Όπως αναφέρθηκε προηγουμένως, η μνήμη αποθηκεύει σημαντικά αποδεικτικά στοιχεία, όπως εγκατεστημένες συνδέσεις, εκτελούμενες διεργασίες/υπηρεσίες, κρυπτογραφημένα συνθηματικά (passwords), κλπ. Η λήψη ενός σωστού αντιγράφου μνήμης (memory dump) μπορεί να κάνει τη διαφορά μεταξύ της επίλυσης ή της μη επίλυσης ενός κυβερνο-περιστατικού. Εξαιτίας αυτού πρέπει να είμαστε πολύ προσεκτικοί κατά τη διάρκεια αυτής της διαδικασίας συλλογής της μνήμης.

Κατά την συλλογή της μνήμης, θα πρέπει να έχουμε κατά νου ότι υπάρχουν δύο είδη μνήμης: η φυσική και η εικονική μνήμη. Η φυσική μνήμη αντιστοιχεί στην πραγματική μνήμη του συστήματος, ενώ η εικονική μνήμη αντιστοιχεί στο αρχείο σελιδοποίησης pagefile.sys που είναι αποθηκευμένο στον σκληρό δίσκο. Όπως αναφέρθηκε πριν, η εικονική μνήμη είναι ένα αρχείο στον φυσικό δίσκο, που επιτρέπει τη βέλτιστη χρήση της μνήμης RAM. Το λειτουργικό σύστημα στέλνει προσωρινά εκεί τις πληροφορίες που δεν είναι απαραίτητες στην μνήμη και στη συνέχεια τις ανακτά αν κάποιο πρόγραμμα τις ζητήσει.

Υπάρχει ένας μεγάλος αριθμός εργαλείων που επιτρέπουν την λήψη αντιγράφου μνήμης (memory dump), αλλά δύο είναι εξαιρετικά απλά το **Winpmem** και το **DumpIt** (λόγω της απλότητας και της συμβατότητάς τους με τις διαφορετικές εκδόσεις των Windows). Είναι αρκετά απλά στην χρήση τους, απλά τα εκτελούμε στην γραμμή εντολών με δικαιώματα διαχειριστή (administrator). Το αποτέλεσμα και των δύο εργαλείων είναι σε **raw format**.

Ένα παράδειγμα για το πώς να χρησιμοποιήσουμε το πρόγραμμα **Dumpit** είναι η Εικόνα 3:



Εικόνα 3: DumpIt

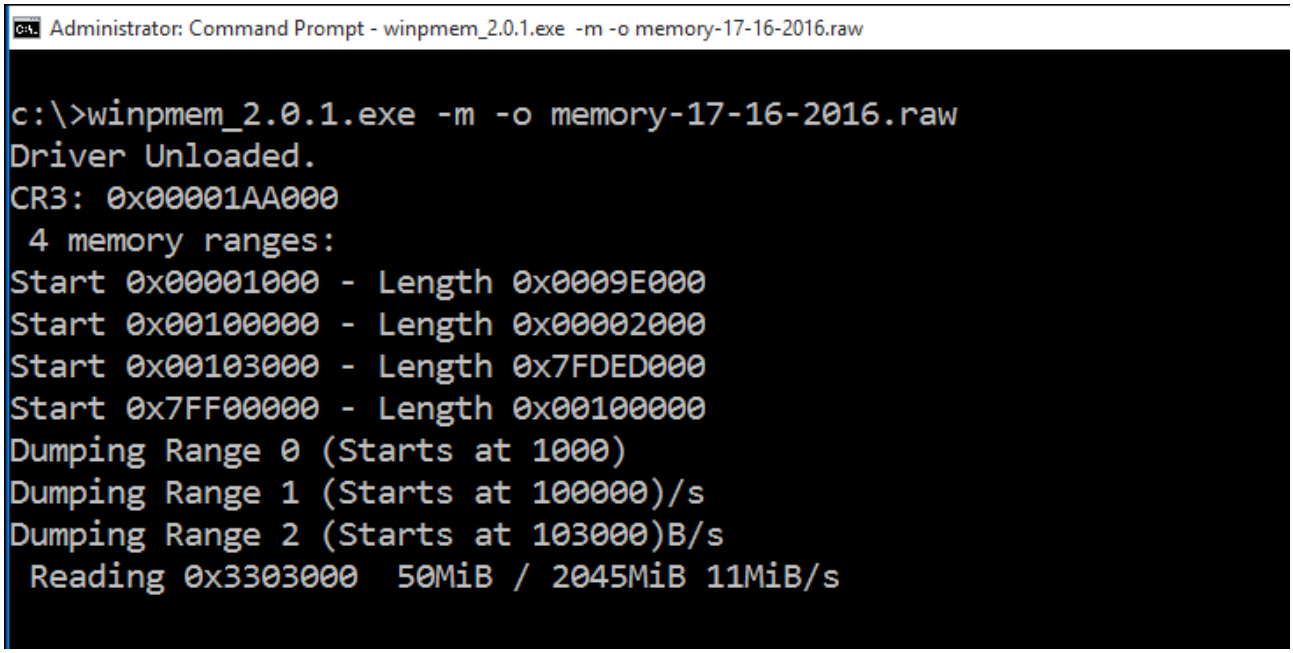
Άλλα εργαλεία

AccessData FTK Imager	http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.0
Memoryze	https://www.mandiant.com/library/MemoryzeSetup3.0.msi
MDD	http://sourceforge.net/projects/mdd/
Winpmem	https://github.com/google/rekall/releases/download/v1.3.2/winpmem_2.0.1.exe
Belkasoft Live RAM Capturer	https://belkasoft.com/en/ram-capturer

Το Winpmem είναι ένα απλό εργαλείο λήψης αντιγράφου της μνήμης. Η εντολή που δίνουμε είναι η ακόλουθη:

c:\> **winpmem_2.0.1.exe -m -o memory_image.raw**

C:\> winpmem<version>.exe output.aff4 --export PhysicalMemory -o memory.img



Εικόνα 4. winpmem memory dump

Σημαντικό

Εκτελούμε τα εργαλεία συλλογής μνήμης με δικαιώματα ADMINISTRATOR.

Υπάρχουν αρκετοί τρόποι συλλογής της μνήμης. Μπορούμε να συλλέξουμε την μνήμη με:

- Συλλογή με χρήση υλικού (Hardware Methods)
    1. Συλλογή μέσω Firewire
    2. PCI Acquisition (Tribble, CaptureGUARD PCIe card)

- Συλλογή με χρήση Λογισμικού (Software Methods)
    1. Μέσω Windows Hibernation

2. Suspension of Virtualization Software
3. Πρόκληση Windows Crash Dump
4. Χρήση εργαλείων όπως dumpit και winpmem (Standalone Acquisition Tools)

Έχουμε την δυνατότητα να συλλέξουμε την φυσική μνήμη μέσω πρόκλησης διακοπής λειτουργίας (crash), δηλαδή συλλογή της μνήμης με πρόκληση σε ένα Windows της BSOD (Blue Screen of Death). Μπορούμε να προκαλέσουμε memory crash dump με την χρήση του NotMyFault (SysInternals) και μπορούμε να κάνουμε ανάλυση με το εργαλείο LiveKD (απαιτεί εγκατάσταση του Windbg). Όταν έχουμε BSOD (Blue Screen of Death) το περιεχόμενο της φυσικής μνήμης αντιγράφεται στον σκληρό δίσκο. Όταν προκαλούμε την BSOD (Blue Screen of Death) δημιουργείται ένα αρχείο, όπως το minidump ή, αν έχει γίνει ρύθμιση, ένα πλήρες αντίγραφο της φυσικής μνήμης (%SystemRoot%\Memory.dmp), το οποίο στη συνέχεια μπορεί να αναλυθεί από το αντίστοιχο εργαλείο (LiveKD). Αν επιχειρήσουμε να αποκτήσουμε την φυσική μνήμη μέσω αυτής της μεθόδου είναι προτεινόμενο να επαληθεύσουμε την ακεραιότητα του αρχείου μέσω εργαλείων όπως το **Dumpchk**.

Για να το κάνουμε αυτό, πληκτρολογούμε την ακόλουθη εντολή:
c:**> dumpchk.exe samplrmemory.dmp**

Εικόνα 5. Dumpchk

Αν η ακεραιότητα του αρχείου επηρεάζεται, ένα μήνυμα λάθους (error) θα εμφανιστεί. Ωστόσο εάν η ακεραιότητα του αρχείου είναι σωστή, θα εμφανιστεί το ακόλουθο μήνυμα: «*Finished dump check*».

Εάν η φυσική πρόσβαση στο σύστημα, όπου πρόκειται να πραγματοποιηθεί η συλλογή αποδεικτικών στοιχείων, δεν είναι δυνατή, μπορούμε να συλλέξουμε την μνήμη και απομακρυσμένα με την χρήση εργαλείων όπως το **psexec.**

Μόλις ληφθεί το αντίγραφο (image) της μνήμης, είναι απαραίτητο να πραγματοποιήσουμε και τον έλεγχο ακεραιότητας του συγκεκριμένου αρχείου. Στο πλαίσιο της διαδικασία επιτήρησης, καταγράφουμε τις τιμές του ελέγχου ακεραιότητας (σωστό είναι να το κάνουμε και με διαφορετικούς αλγορίθμους). Σκοπός μας είναι να τηρήσουμε την διαδικασία επιτήρησης-παρακολούθησης για να εγγυηθούμε ότι το προαναφερθέν αντίγραφο (image) δεν έχει τροποποιηθεί μεταγενέστερα. Μπορούμε να χρησιμοποιήσουμε διάφορους αλγόριθμους, MD5, SHA-1, SHA-2, κλπ.

Σημαντικό

Η χρήση του MD5 hash, παρά την τεράστια χρήση του, παρουσιάζει το πρόβλημα της σύγκρουσης τιμών, με άλλα λόγια, θα μπορούσε να συμβεί διαφορετικά αρχεία να έχουν το ίδιο MD5, πράγμα που σημαίνει ότι η εγκυρότητα της απόδειξής του θα μπορούσε να αμφισβητηθεί. Γι' αυτό συνιστάται να μειωθεί η χρήση του.

Μια παρόμοια περίπτωση, μολονότι δεν είναι πανομοιότυπη, είναι το SHA-1, γι' αυτό καλό είναι να αναζητήσουμε διάφορες εναλλακτικές λύσεις, όπως τα SHA-256, SHA-512, κλπ.

```
c:\>sha256deep64.exe -h
sha256deep64.exe version 4.4 by Jesse Kornblum and Simson Garfinkel.
C:\> sha256deep64.exe [OPTION]... [FILES]...
See the man page or README.txt file or use -hh for the full list of options
-p <size> - piecewise mode. Files are broken into blocks for hashing
-r        - recursive mode. All subdirectories are traversed
-e        - show estimated time remaining for each file
-s        - silent mode. Suppress all error messages
-z        - display file size before hash
-m <file> - enables matching mode. See README/man page
-x <file> - enables negative matching mode. See README/man page
-M and -X are the same as -m and -x but also print hashes of each file
-w        - displays which known file generated a match
-n        - displays known hashes that did not match any input files
-a and -A add a single hash to the positive or negative matching set
-b        - prints only the bare name of files; all path information is omitted
-l        - print relative paths for filenames
-t        - print GMT timestamp (ctime)
-i/I <size> - only process files smaller/larger than SIZE
-v        - display version number and exit
-d        - output in DFXML; -u - Escape Unicode; -W FILE - write to FILE.
-j <num>  - use num threads (default 2)
-Z - triage mode;   -h - help;   -hh - full help
```

Εικόνα 6. sha256deep

Υπάρχει ένας μεγάλος αριθμός εργαλείων όπως τα **hashdeep**, **HashMyFiles**, **MD5deep**, **HashCalc**, **sha256deep** τα οποία μπορούν να βοηθήσουν στην δημιουργία διαφορετικών τιμών hashes για ένα αρχείο. Ένα παράδειγμα της χρήσης του **sha256deep** μπορεί να φανεί στην Εικόνα 7:

```
c:\>sha256deep64.exe serviwin.exe
86d8f63868b5fe470505646a30ab35875be290499a39ca77ff03592768d0dc84  c:\serviwin.exe
```

Εικόνα 7. sha256deep

Μεγάλο ενδιαφέρον για την ψηφιακή εγκληματολογική ανάλυση έχει και η ανάκτηση της εικονικής μνήμης (virtual memory), γι' αυτό συνιστάται να αντιγράφουμε και το **pagefile.sys** όποτε είναι δυνατόν. Για να γίνει αυτό, μπορούν να χρησιμοποιηθούν εξειδικευμένα εργαλεία όπως το **NTFSCopy και rawcopy**. Ο λόγος που χρησιμοποιούμε εξειδικευμένα εργαλεία, αφορά το γεγονός πως κάποια

αρχεία είναι κλειδωμένα από το ίδιο το λειτουργικό σύστημα και δεν επιτρέπεται η αντιγραφή τους. Εναλλακτικά, μπορούμε να απενεργοποιήσουμε τον υπολογιστή, να βγάλουμε τον σκληρό δίσκο, να τον μεταφέρουμε σε άλλον υπολογιστή και τότε να αντιγράψουμε την εικονική μνήμη. Αυτή η διαδικασία ωστόσο ενέχει τον κίνδυνο να χάσουμε την εικονική μνήμη, γιατί θα την έχει διαγράψει από πριν το λειτουργικό σύστημα.

Για τη συλλογή της εικονικής μνήμης (**pagefile.sys)** με την χρήση του **rawcopy** δίνουμε την ακόλουθη εντολή με δικαιώματα διαχειριστού:

RawCopy.exe /FileNamePath:C:\pagefile.sys /OutputPath:E:\output

Με την παραπάνω εντολή ζητάμε από το εργαλείο rawcopy να κάνει ένα αντίγραφο του pagefile.sys που βρίσκεται στο C: και να το αποθηκεύσει στη μονάδα E:.

Άλλα εργαλεία

AccessData FTK Imager	http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.3
Hobocopy	https://github.com/candera/hobocopy/downloads
rawcopy	https://github.com/jschicht/RawCopy
Ntfscopy	https://tzworks.net/prototype_page.php?proto_id=9
ShadowCopy	https://www.runtime.org/shadow-copy.htm
Invoke-Ninjacopy.ps1	https://github.com/clymb3r/PowerShell/tree/master/Invoke-NinjaCopy

Σημαντικό

Μπορούμε να αποκτήσουμε άμεσα το pagefile.sys μέσα από τον σκληρό δίσκο που έχουμε εξάγει, χωρίς να χρειαστεί να λάβουμε αντίγραφό του με εξειδικευμένα εργαλεία. Ο ερευνητής που πρόκειται να πραγματοποιήσει την ανάλυση των αποδεικτικών στοιχείων δεν θα έχει κανένα πρόβλημα να εξάγει την εικονική μνήμη (pagefile.sys) από τον πραγματικό δίσκο, με την χρήση της εντολής copy.

Μία άλλη τεχνική συλλογής της μνήμης είναι με την χρήση του Windows Hibernation. Στο αρχείο αδρανοποίησης (hibernation), hiberfil.sys, αποθηκεύεται ένα ακριβές αντίγραφο της μνήμης του υπολογιστή λίγο πριν την αδρανοποίηση του με σκοπό την αποκατάσταση της φυσικής μνήμης μέσου του αντιγράφου όταν ο υπολογιστής επανέλθει στην κανονική του λειτουργία. Το Hibernation αρχείο (%SystemDrive%/hiberfil.sys) δεν διαγράφεται ποτέ, ακόμα και μετά την επαναφορά του συστήματος διαγράφονται μόνο οι επικεφαλίδες του αρχείου (header file is wiped). Εάν η αδρανοποίηση δεν είναι ρυθμισμένη από προεπιλογή, μπορεί να γίνει μέσω του **Powercfg** και στη συνέχεια να αναγκάσει σε κατάσταση αδρανοποίησης με το εργαλείο **PsShutdown** ή πηγαίνοντας στο *Start- Shut down –Hibernate*.

Σε ορισμένες περιπτώσεις, μπορεί να μην είναι αναγκαίο, λόγω του περιστατικού, να λάβουμε αντίγραφο του συνόλου της μνήμης και αντί αυτού να λάβουμε τμήματα της μνήμης που περιέχουν την πληροφορία που χρειαζόμαστε. Εργαλεία όπως το **procdump** μπορούν να χρησιμοποιηθούν σε αυτή την περίπτωση.

Καταγραφή της χρονικής αλυσίδας των δεδομένων

Σημαντικό για την ψηφιακή ανάλυση είναι και η δημιουργία της χρονικής αλυσίδας των δεδομένων του αρχείου συστήματος (Filesystem timeline). Είναι σημαντικό να γνωρίζουμε πότε δημιουργηθήκαν ή τροποποιήθηκαν ή προσπελάστηκαν ή ακόμα πότε άλλαξαν τα μεταδεδομένα ενός αρχείου, ώστε γνωρίζοντας την ώρα του συμβάντος να επικεντρωθούμε εκεί.

Για την δημιουργία της χρονικής αλυσίδας των δεδομένων του αρχείου συστήματος (Filesystem timeline), μπορούμε να χρησιμοποιήσουμε εργαλεία όπως το **fls** του sleuthkit.

Έστω ότι θέλουμε να δημιουργήσουμε την χρονική αλυσίδα για το C drive ενός **συστήματος σε λειτουργία**, τότε δίνουμε την εντολή:

c:**> fls.exe -i raw -f ntfs -z CST6CDT -r -p -m c: \\.\c: > bodyfile.txt**

Η επιλογή "m" ορίζει στο FLS το αποτέλεσμα να είναι της μορφής BODYFILE.

Η επιλογή ‘C:/’ ορίζει στο FLS να προσθέσει ως γνώρισμα (identifier) στο παραγόμενο αποτέλεσμα. Με λίγα λόγια το αποτέλεσμα θα έχει ένα μονοπάτι (path), όπως αυτό στο c drive. Ως επιλογή μπορούμε να βάζουμε το γράμμα οποιοδήποτε drive επιλέγουμε να δημιουργήσουμε την χρονική αλυσίδα, όπως C:, D:, E: κλπ.

Η επιλογή –f ntfs ορίζει το αρχείο συστήματος (filesystem) ως ntfs. Μπορούμε να δώσουμε την εντολή "fls –t list" για μία λίστα από υποστηριζόμενα αρχεία συστήματος.

Η επιλογή -r \\.\C: ορίζει πως το πρόγραμμα θα τρέξει αναδρομικά (recursively) όλο το C:\.

Μόλις η εντολή FLS ολοκληρωθεί, μπορούμε να μετατρέψουμε το αρχείο της μορφής bodyfile, σε ένα πιο εύκολα αναγνώσιμο από εμάς αρχείο με την εντολή:

c:\> mactime.pl –d –b bodyfile.txt > path_to_timeline.csv

Θα πρέπει να έχουμε εγκατεστημένη την perl.

Εναλλακτικά μπορούμε να δώσουμε την εντολή

c:**> bodyfile.exe -f <Path-To-Bodyfile>\bodyfile.txt -s <όνομα-υπολογιστή> > timeline-events.txt**

Σημαντικό είναι να γνωρίζουμε τη δεντρική δομή των αρχείων και των φακέλων προκειμένου να αποδείξουμε την ύπαρξη ύποπτων αρχείων. Για να γίνει αυτό, είναι απαραίτητο να αποκτήσουμε 3 λίστες μέσω των ακόλουθων εντολών, οι οποίες αντιστοιχούν σε **MAC file times**:

- Λίστα με βάση την ημερομηνία τροποποίησης. Εντολή:

c:\> **dir /t:w /a /s /o:d** c:\ **> ListOfFilesPerModificationDate.txt**

- Λίστα με βάση την τελευταία πρόσβαση. Εντολή:

c:\> **dir /t:a /a /s /o:d** c:\ **> ListOfFilesPerLastAccessDate.txt**

- Λίστα με βάση την ημερομηνία δημιουργίας.

c:\> **dir /t:c /a /s /o:d** c:\ **> ListOfFilesPerCreationDate.txt**

Σημείωση

Αν υπάρχουν αρκετοί σκληροί δίσκοι ή κατατμήσεις (partitions) η εντολή πρέπει να εκτελεστεί για κάθε δίσκο ή κατάτμηση. Με άλλα λόγια, η εντολή πρέπει να εκτελεσθεί όσες φορές είναι αναγκαίο, αλλάζοντας τον κατάλογο (directory) όπου φτιάχνεται η λίστα (σε αυτήν την περίπτωση το c:\) και αλλάζοντας συγχρόνως το όνομα του αρχείου όπου θα αποθηκευτεί η λίστα.

Άλλα εργαλεία

Bodyfile.exe	https://github.com/keydet89/Tools/tree/master/exe
sleuthkit	https://github.com/sleuthkit/sleuthkit/releases/tag/sleuthkit-4.3.0
Log2timeline (plaso)	https://github.com/log2timeline/plaso/releases
MacMatch	http://ntsecurity.nu/toolbox/macmatch/

Σημαντικό επίσης είναι να γνωρίζουμε τις τιμές hashes των αρχείων προκειμένου να αποδείξουμε την ύπαρξη ύποπτων αρχείων. Για να γίνει αυτό, είναι απαραίτητο να αποκτήσουμε τις τιμές μέσω των ακόλουθων εντολών:

c:\> **sha256deep64.exe" -oe -u -t -r "%SystemDrive%*"**
c:\> **sha256deep64.exe" -oe -u -t -r** c:*****
c:\> **md5deep64.exe" -oe -u -t -r "%SystemDrive%*"**

Πληροφορίες δικτύου: κατάσταση, ενεργές συνδέσεις, ανοιχτές UDP και TCP θύρες.

ARP cache

Ο πίνακας ARP αποθηκεύει τη σχέση ανάμεσα στη φυσική διεύθυνση (MAC) και λογική διεύθυνση (IP) των συστημάτων με τα οποία ο υπολογιστής έχει επικοινωνήσει πρόσφατα. Πρέπει να έχουμε κατά νου ότι η αποθηκευμένη πληροφορία είναι προσωρινή και ότι, αν η επικοινωνία δεν διατηρείται, η αντίστοιχη καταχώρηση θα εξαλειφθεί σε σύντομο χρονικό διάστημα.

Για να αποκτήσουμε τον πίνακα ARP cache, χρησιμοποιούμε την εντολή **arp**.

Για να το κάνουμε αυτό, πληκτρολογούμε τις ακόλουθες εντολές:

c:\> **arp -a > arp-a.txt**
c:\> **arp -e > arp-e.txt**

Και το λαμβανόμενο αποτέλεσμα είναι η Εικόνα 8:

```
Interface: 192.168.21.111 --- 0x3
  Internet Address      Physical Address      Type
  192.168.21.1          00-11-6b-35-44-dd     dynamic
  192.168.21.108        00-0e-0c-dd-c7-08     dynamic
  224.0.0.251           01-00-5e-00-00-fb     static
```

Εικόνα 8: ARP cache

Κατάσταση του δικτύου- συλλογή δικτυακών πληροφοριών

Για να καταγράψουμε την κατάσταση του δικτύου, χρησιμοποιούμε τα εργαλεία που ακολουθούν δίνοντας τις εντολές που περιγράφονται.

Για να καταγράψουμε την λίστα των ενεργών συνδέσεων στον υπό εξέταση υπολογιστή, χρησιμοποιούμε την εφαρμογή **netstat**. Για να καταγράψουμε τις συγκεκριμένες πληροφορίες, πληκτρολογούμε τις ακόλουθες εντολές:

c:\> **netstat -an | findstr /i "state listening established" > netstat-a-n-est.txt**
c:\> **netstat -nao > netstat-a-n-o.txt**

Και το αποτέλεσμα που προκύπτει είναι η Εικόνα 9:

```
Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
TCP    127.0.0.1:50176        127.0.0.1:50177        ESTABLISHED
TCP    127.0.0.1:50177        127.0.0.1:50176        ESTABLISHED
TCP    127.0.0.1:50178        127.0.0.1:50179        ESTABLISHED
TCP    127.0.0.1:50179        127.0.0.1:50178        ESTABLISHED
TCP    192.168.21.111:139     0.0.0.0:0              LISTENING
```

Εικόνα 9: Ενεργές συνδέσεις ή ανοιχτές θύρες (ports)

Για να εντοπίσουμε την δικτυακή δρομολόγηση των πακέτων και τυχόν τροποποίηση της διαδρομής, δίνουμε τις ακόλουθες εντολές:

c:\> **route print > route_PRINT.txt**
c:\> **netstat -r > netstat-r.txt**

Για να καταγράψουμε τις ανοικτές πόρτες για TCP/IP και UDP δίνουμε την ακόλουθη εντολή:

c:\> **cports /stext cports.txt**

Για να καταγράψουμε τα URL πρωτόκολλα, που έχουν χρησιμοποιηθεί, στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **urlprotocolview /stext urlprotocolview.txt**

Για να καταγράψουμε όλες τις δικτυακές συνδέσεις στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **net sessions > net_sessions.txt**

Και το λαμβανόμενο αποτέλεσμα είναι η Εικόνα 10:

```
Computer              User name            Client Type       Opens Idle time
-------------------------------------------------------------------------------
\\192.168.21.111      userVictim                                1 00:00:19
```

Εικόνα 10: Εγκατεστημένες συνδέσεις NetBIOS

Το NetBIOS είναι ένα πρωτόκολλο που χρησιμοποιείται από τα Windows, το οποίο συνήθως λειτουργεί σε TCP/IP και δίνει τη δυνατότητα στα συστήματα να επικοινωνούν στο ίδιο τοπικό δίκτυο. Για να γίνει αυτό, το NetBIOS εκχωρεί έναν αριθμό ταυτοποίησης σε κάθε σύστημα. Ως εκ τούτου, μπορεί να γίνει προσβάσιμο μέσα από το δίκτυο μέσω του όνοματός του ή της IP των διαμοιρασμένων πόρων του συστήματος. Το NetBIOS σε TCP/IP πραγματοποιεί την αντιστοίχηση ονόματος υπολογιστή στη διεύθυνση IP, καθώς και την ανάλυση του ονόματος. Υπάρχουν τέσσερις μέθοδοι ανάλυσης ονόματος NetBIOS σε TCP/IP: b-node, p-node, m-node και h-node.

Το NetBIOS αποθηκεύει προσωρινά τα ονόματα όλων των αντιγραμμένων αρχείων μέσω του πρωτοκόλλου αυτού σε έναν πίνακα. Για να καταγράψουμε όλα τα αρχεία που έχουν ανοίξει μέσω δικτύου στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **net file > net_file.txt**

Και το λαμβανόμενο αποτέλεσμα είναι η Εικόνα 11:

```
ID          Path                                          User name          # Locks
-------------------------------------------------------------------------------
3           c:\temp\                                      userVictim          0
6           c:\temp\for.txt                               userVictim          0
The command completed successfully.
```

Εικόνα 11: Προσφάτως μεταφερθέντα αρχεία μέσω του NetBIOS

Για να καταγράψουμε όλα τα αρχεία που διαμοιράζονται μέσω δικτύου (network shared files) στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **net share > net_share.txt**

Για να συγκεντρώσουμε πληροφορίες σχετικά με την διαχείριση αρχείων, αρχεία σε αναμονή, ανοικτά αρχεία ή κοινόχρηστα αρχεία, δίνουμε τις παρακάτω εντολές:
c:\> **pendmoves /AcceptEula > pendmoves.txt**
c:\> **net use > net-use.txt**

c:\> **net view > net-view.txt**
c:\> openfiles /query /fo csv >openfiles.csv

Το NetBIOS αποθηκεύει κάθε πρόσβαση σε έναν πίνακα. Για να τον δούμε, χρησιμοποιούμε το **nbtstat** ή την εντολή **net**. Για να καταγράψουμε τα προσωρινά αποθηκευμένα δεδομένα του NETBIOS (cache) over TCP στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **nbtstat -c > nbtstat-c.txt**

Για να καταγράψουμε όλες τις συνόδους του NETBIOS over TCP στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **nbtstat -s > nbtstat-s.txt**

Για να καταγράψουμε όλες τις δικτυακές συνδέσεις στον υπό εξέταση υπολογιστή, δίνουμε την ακόλουθη εντολή:
c:\> **tcpvcon -a -c /accepteula > tcpvcon-a-c.txt**

Μπορούμε να ανακτήσουμε την σχέση μεταξύ των ανοιχτών εφαρμογών και των θυρών δίνοντας της ακόλουθη εντολή:
c:\> **netstat -anob > netstat-anob.txt**

Άλλες εντολές συλλογής δικτυακών πληροφοριών:
c:\> **type %SystemRoot%\system32\drivers\etc\hosts > hosts.txt**
c:|> type %windir%\System32\drivers\etc\networks > networks.txt

Άλλα εργαλεία

tcpview	https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx
Fport	http://www.mcafee.com/es/downloads/free-tools/fport.aspx

Καταγραφή των Εκτελούμενων διεργασιών.

Για να ανακτήσουμε την λίστα των διεργασιών που “τρέχουν” στον υπό εξέταση υπολογιστή, μπορούμε να χρησιμοποιήσουμε το εργαλείο **pslist** και πληκτρολογούμε την ακόλουθη εντολή (εάν είναι 64 bit):

c:\> ***pslist64.exe*** **/accepteula > pslist64.txt**

Ωστόσο μπορούμε να χρησιμοποιήσουμε και άλλα εργαλεία για να ανακτήσουμε τις διεργασίες που “τρέχουν” στο υπό εξέταση σύστημα, οι εντολές και τα εργαλεία είναι τα ακόλουθα:
c:\> **cprocess /stext cprocess.txt**
c:\> **procinterrogate -ps > procinterrogate-ps.txt**
c:\> **procinterrogate -list -md5 -ver -o procinterrogate-list-md5-ver-o.txt**
c:\> **wmic process list status > process-list-status.txt**
c:\> **wmic process list memory > process-list-memory .txt**

Για να εμφανίσουμε τις διεργασίες σχετιζόμενες με το Path του εκτελέσιμου

και επιπλέον πληροφορίες – (Extended and long information) χρησιμοποιούμε το εργαλείο pv.exe (είναι το εργαλείο γραμμής εντολών του prcView) και δίνουμε την εντολή:

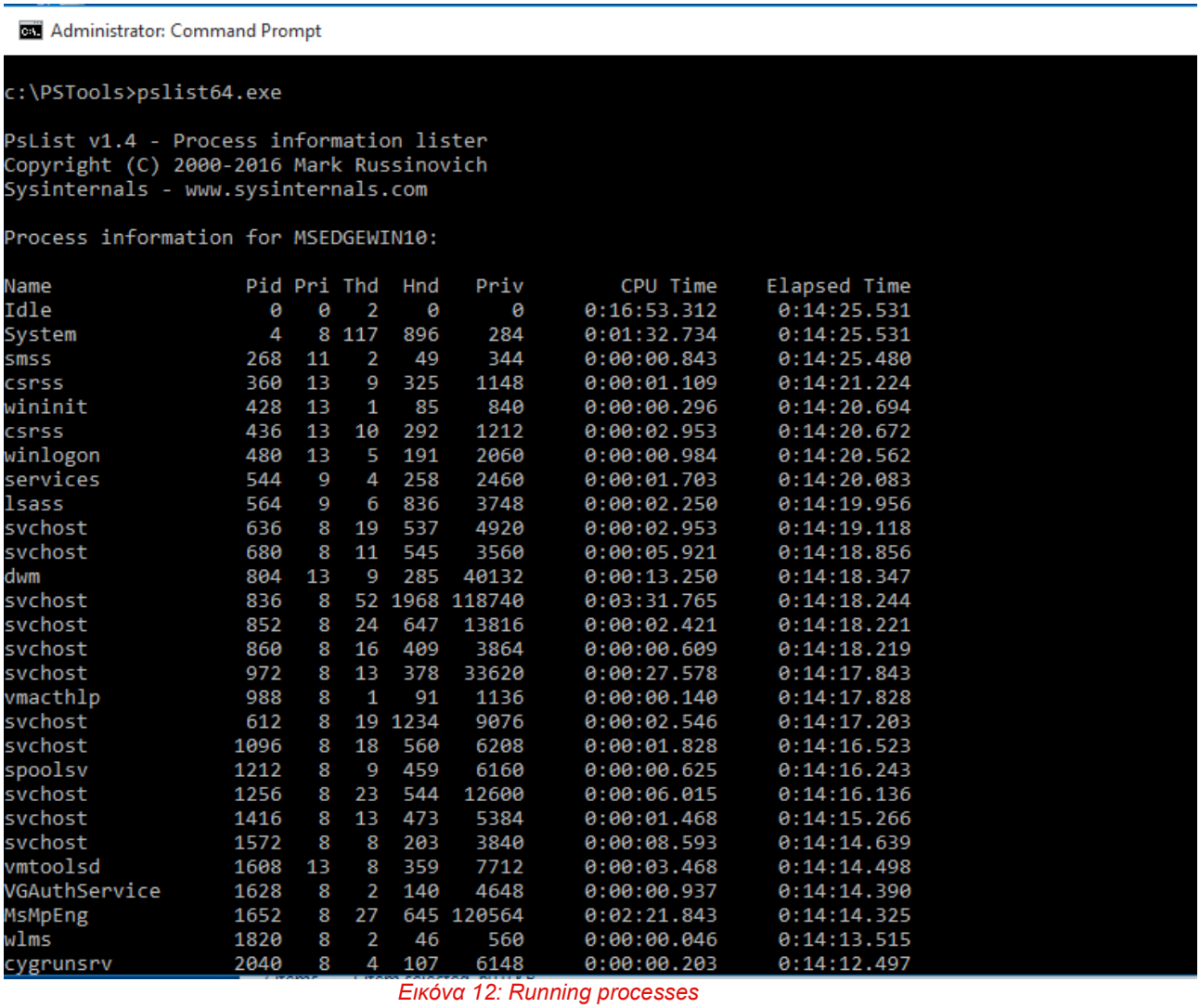
c:\> ***PrcView/pv.exe -el > pv-e-l.txt***

Για να εμφανίσουμε τις διεργασίες σχετιζόμενες με το Path του εκτελέσιμου– (Extended) χρησιμοποιούμε το εργαλείο pv.exe (είναι το εργαλείο γραμμής εντολών του prcView) και δίνουμε την εντολή:

c:\> ***PrcView/pv.exe -e > pv-e.txt***

Για να ανακτήσουμε την λίστα των διεργασιών που "εκτελούνται" με την χρήση εργαλείων του συστήματος, μπορούμε να χρησιμοποιήσουμε το εργαλείο **taskslist** και δίνουμε την εντολή:

c:\> ***tasklist -V > tasklist-V.txt***



Εικόνα 12: Running processes

Για να καταγράψουμε την γραμμή εντολών για κάθε διεργασία, δίνουμε την εντολή:
c:**> tlist -c > tlist-c.txt**

Για να συλλέξουμε σε δενδροειδή μορφή τις διεργασίες, δίνουμε την εντολή:
c:**> tlist -t >tlist-t.txt**

Για να καταγράψουμε τις υπηρεσίες που είναι ενεργές σε κάθε διεργασία, δίνουμε την εντολή:
c:**>tlist -s > tlist-s.txt**

Για να καταγράψουμε όλες τις βιβλιοθήκες που φορτώνουν σε κάθε διεργασία, δίνουμε την εντολή:
c:**>listdlls /accepteula > listdlls.txt**

Για να καταγράψουμε όλες τις συναρτήσεις που χρησιμοποιούν οι βιβλιοθήκες που φορτώνουν σε κάθε διεργασία, δίνουμε την εντολή:
c:**>dllexp /stext dllexp.txt**

Για να καταγράψουμε όλες τις βιβλιοθήκες (dll) που που γίνονται inject σε κάθε διεργασία, δίνουμε την εντολή:
c:**>injecteddll /stext injecteddll.txt**

Για να καταγράψουμε όλους τους οδηγούς (drivers) που φορτώνουν στο υπό εξέταση σύστημα, δίνουμε τις παρακάτω εντολές:
c:**>driverview /stext driverview.txt**
c:**>wmic /output:Loaded_system_drivers_wmic.txt sysdriver list full**

Για να καταγράψουμε όλα τα ανοικτά handles για κάθε διεργασία, δίνουμε την εντολή:
c:**>handle /accepteula > handle.txt**

Για να καταγράψουμε όλα τα αρχεία που είναι ανοικτά στον υπό εξέταση υπολογιστή, δίνουμε την εντολή:
c:**> openedfilesview /stext openfilesview.txt**

Άλλα εργαλεία

Pslist	http://technet.microsoft.com/es-es/sysinternals/bb896682.aspx
Volatility	http://www.volatilityfoundation.org/releases
CurrProcess	http://www.nirsoft.net/utils/cprocess.html
PrcView	http://www.majorgeeks.com/mg/getmirror/process_viewer_for_windows_(prcview),1.html

Σημείωση

Σε ειδικές περιπτώσεις, κυρίως εκείνων που σχετίζονται με ιομορφικό λογισμικό, θα ήταν ίσως χρήσιμο να λάβουμε αντίγραφο της μνήμης μιας τρέχουσας διεργασίας που θεωρούμε ως ύποπτη και πιθανός να χρησιμοποιείται από το ιομορφικό λογισμικό. Διαφορετικά εργαλεία μπορούν να χρησιμοποιηθούν για το σκοπό αυτό, όπως το **ADPlus.vbs, Procdump, PMDump** ή το **Process Dumper**, ή στα Windows 10, μπορεί να δημιουργηθεί ένας φάκελος όπου μπορούμε να πάρουμε αντίγραφο της μνήμης μίας διεργασίας μέσα από τον task manager ως administrator.

Για να χρησιμοποιήσουμε τον Windows Task Manager και να δημιουργήσουμε ένα αντίγραφο της μνήμης μιας διεργασίας, στα Windows 10, ακολουθούμε τα εξής βήματα:

- Ξεκινάμε τη Διαχείριση εργασιών (Task Manager). Για να το κάνουμε αυτό, πιέζουμε τον συνδυασμό πλήκτρων CTRL + SHIFT + ESC.
- Κάνουμε κλικ στην καρτέλα Διεργασίες (Processes tab).
- Κάνουμε δεξί κλικ στο όνομα της διεργασίας που θέλουμε, και στη συνέχεια κάνουμε κλικ στην επιλογή Δημιουργία αρχείου ένδειξης σφαλμάτων (Create Dump Συγκέντρωση πληροφοριών συστήματος. Εντολές: File).

Θα εμφανιστεί το User Account Control. Εάν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογούμε τον κωδικό πρόσβασης ή κάνουμε κλικ στο κουμπί συνέχεια (Continue).

Ένα αρχείο ένδειξης σφαλμάτων για τη διαδικασία δημιουργείται στον ακόλουθο φάκελο:Drive:\Users\UserName\AppData\Local\Temp
Όταν λάβουμε ένα μήνυμα που αναφέρει ότι το αρχείο ένδειξης σφαλμάτων δημιουργήθηκε με επιτυχία, κάνουμε κλικ στο OK.

Καταγραφή των Εκτελούμενων Υπηρεσιών (Services-Υπηρεσίες που έχουν εκκινήσει) .

Για να ανακτήσουμε την λίστα των υπηρεσιών που “εκτελούνται” στον συγκεκριμένο υπολογιστή μπορούμε να χρησιμοποιήσουμε το εργαλείο **psservice**.

Για να το κάνουμε αυτό, πληκτρολογούμε την ακόλουθη εντολή (εάν είναι 64 bit):

c:**> *psservice64.exe*** > ***psservice64.txt***

Και το αποτέλεσμα που προκύπτει είναι η Εικόνα 13:

```
c:\PSTools>PsService64.exe

PsService v2.25 - Service information and configuration utility
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their
own bundled routers will be unable to run.
        TYPE               : 20 WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                             (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
                             (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

Εικόνα 13: Running services

Για να ανακτήσουμε τις υπηρεσίες που εκτελούνται και τις σχετιζόμενες διεργασίες, δίνουμε την εντολή:

c:\>tasklist /SVC

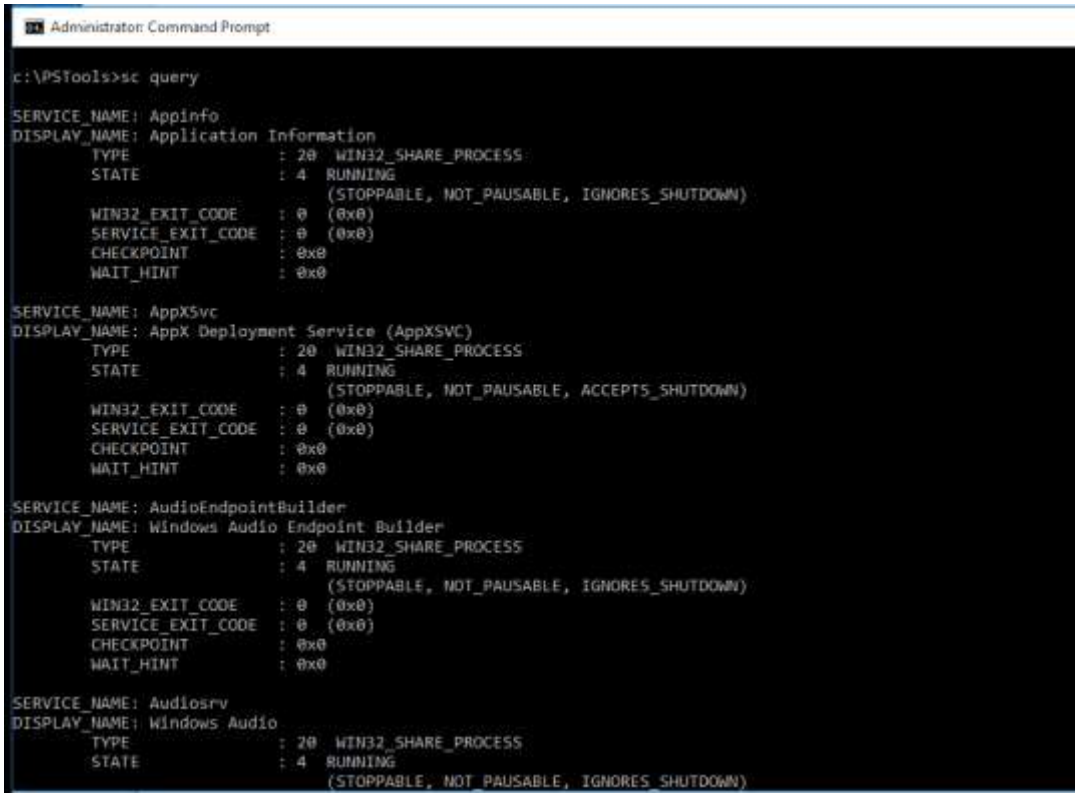
```
c:\PSTools>tasklist /SVC

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       268 N/A
csrss.exe                      368 N/A
wininit.exe                    436 N/A
csrss.exe                      444 N/A
winlogon.exe                   504 N/A
services.exe                   552 N/A
lsass.exe                      572 SamSs, VaultSvc
svchost.exe                    644 BrokerInfrastructure, DcomLaunch, LSM,
                                   PlugPlay, Power, SystemEventsBroker
svchost.exe                    696 RpcEptMapper, RpcSs
dwm.exe                        800 N/A
svchost.exe                    840 Appinfo, BITS, Browser, DoSvc, iphlpsvc,
                                   LanmanServer, lfsvc, ProfSvc, Schedule,
                                   SENS, ShellHWDetection, Themes,
                                   UserManager, UsoSvc, Winmgmt, wuauserv
svchost.exe                    920 AudioEndpointBuilder,
                                   DeviceAssociationService, NcbService,
                                   PcaSvc, SysMain, TrkWks
svchost.exe                    936 Audiosrv, Dhcp, EventLog,
                                   HomeGroupProvider, lmhosts, Wcmsvc, wscsvc
svchost.exe                    952 FDResPub, SSDPSRV, TimeBroker, wcncsvc
vmacthlp.exe                  1008 VMware Physical Disk Helper Service
svchost.exe                    660 EventSystem, fdPHost, FontCache,
                                   LicenseManager, netprofm, nsi,
                                   WdiServiceHost, WinHttpAutoProxySvc
svchost.exe                   1128 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc
spoolsv.exe                   1220 Spooler
```

Εικόνα 14: Running services

Για να ανακτήσουμε την λίστα των υπηρεσιών που “εκτελούνται” με την χρήση εργαλείων του συστήματος, μπορούμε να χρησιμοποιήσουμε το εργαλείο **sc** και δίνουμε την εντολή:

c:\> ***sc query***



Εικόνα 15: Running services

Επίσης για να ανακτήσουμε την λίστα των υπηρεσιών που “εκτελούνται” με την χρήση εργαλείων του συστήματος, μπορούμε να χρησιμοποιήσουμε το εργαλείο **wmic** και δίνουμε την εντολή:
c:\> ***wmic service list config > service-list-config.txt***

Άλλα εργαλεία

PsService	http://technet.microsoft.com/es-es/sysinternals/bb897542.aspx
Volatility	http://www.volatilityfoundation.org/releases
serviwin.exe	http://www.nirsoft.net/utils/serviwin.html

Συνδέσεις χρηστών στον υπό εξέταση υπολογιστή.

Για να αποκτήσουμε τη λίστα με τους χρήστες που έχουν συνδεθεί κατά το παρών αλλά και το παρελθόν με τον συγκεκριμένο υπολογιστή, υπάρχουν διαθέσιμα διάφορα εργαλεία, όπως το **netusers**. Για να δούμε ποιοι είναι συνδεδεμένοι στον υπολογιστή, πληκτρολογούμε οποιαδήποτε από τις ακόλουθες εντολές:

c:\> **netusers.exe > netusers.txt**
c:\> **psloggedon /accepteula > psloggedon.txt**

Με το ίδιο εργαλείο (**netusers.exe)**, μπορούμε να εντοπίσουμε χρήστες που είχαν πραγματοποιήσει μία σύνοδο/σύνδεση (session) στον συγκεκριμένο

υπολογιστή σε κάποια άλλη χρονική στιγμή και πότε ήταν η τελευταία φορά που το έκαναν. Για να συλλέξουμε αυτές τις πληροφορίες, πληκτρολογούμε την ακόλουθη εντολή:
c:**> netusers /local /history > netusers_local_history.txt**

Για να καταγράψουμε τις τρέχουσες συνδέσεις χρηστών, δίνουμε την εντολή:
c:**> logonsessions /accepteula > logonsessions.txt**

Για να καταγράψουμε τις συνδέσεις και τις αποσυνδέσεις των χρηστών (users logged on/off), δίνουμε την εντολή:

c:**> winlogonview /stext winlogonview.txt**

Άλλα εργαλεία

Netuser.exe	http://www.systemtools.com/download/netusers.zip
Psloggedon	http://technet.microsoft.com/es-es/sysinternals/bb897545.aspx
LogonSessions	http://technet.microsoft.com/es-es/sysinternals/bb896769.aspx

Πληροφορίες χρηστών στον υπό εξέταση υπολογιστή.

Για την συγκέντρωση πληροφοριών που αφορούν λογαριασμούς χρηστών του υπό εξέταση συστήματος, δίνουμε τις παρακάτω εντολές:

c:**> net localgroup administrators > administrators.txt**
c:**> Net user > net_user.txt**
c:**> whoami > whoami.txt**
c:**> wmic useraccount list > wmic-useraccount-list.txt**
c:|> showpriv SeLockMemoryPrivilege (for Win2k3)
c:**> showpriv SeSecurityPrivilege (for Win2k3)**
c:**> showpriv SeTakeOwnershipPrivilege (for Win2k3)**

Πληροφορίες συστήματος

Για να συγκεντρώσουμε γενικές πληροφορίες που αφορούν τον υπό εξέταση υπολογιστή δίνουμε τις παρακάτω εντολές:

C:**>WinAudit.exe /r=gsoPxuTUeERNtnzDaIbMpmdcSArCHGBLJF**
C:**>Systeminfo > systeminfo.txt**
C:**>psinfo /accepteula > psinfo.txt**
C:**>hostname > hostname.txt**
c:**> set > set.txt**

Για να συγκεντρώσουμε πληροφορίες που αφορούν τους δίσκους του υπό εξέταση υπολογιστή δίνουμε τις παρακάτω εντολές:

C:\>**psinfo -d /accepteula > psinfo-d.txt**

Για να συγκεντρώσουμε πληροφορίες που αφορούν εγκατεστημένο λογισμικό στον υπό εξέταση υπολογιστή δίνουμε τις παρακάτω εντολές:

C:**> psinfo -s /accepteula > psinfo-s.txt**
C:**> wmic /output:Installed_software.txt product get Name, Version**
C:**> wmic /output:list-Installed_software.txt product list**

Για να συγκεντρώσουμε μία λίστα με τα hotfixes που είναι εγκατεστημένα στον υπό εξέταση υπολογιστή δίνουμε τις παρακάτω εντολές:

C:**>psinfo -h /accepteula > psinfo-h.txt**
C:**> wmic qfe get Hotfixid > hotfixes-id.txt**
C:**> wmic qfe list > hotfixes-list.txt**

Για να συγκεντρώσουμε μία λίστα με τις ενημερώσεις (updates) που είναι εγκατεστημένες στον υπό εξέταση υπολογιστή δίνουμε τις παρακάτω εντολές:

C:**>wul /stext wul.txt**

Για να συγκεντρώσουμε πληροφορίες που αφορούν την πολιτική που εφαρμόζεται στον υπό εξέταση υπολογιστή δίνουμε τις παρακάτω εντολές:

C:**> gplist > gplist.txt**
C:**> gpresult /Z > gpresult_Z.txt**

Για να συγκεντρώσουμε πληροφορίες που αφορούν τις ωρικές ζώνες στις οποίες έχει αλλάξει ο υπό εξέταση υπολογιστής δίνουμε την παρακάτω εντολή:

C:**>turnedontimesview /stext turnedontimesview.txt**

Ανάλογα με τον τύπο του περιστατικού είναι σημαντικό να γνωρίζουμε τις τελευταίες αναζητήσεις στις κυριότερες μηχανές αναζήτησης. Για να συλλέξουμε αυτές τις πληροφορίες, ένα από τα εργαλεία που μπορούμε να χρησιμοποιήσουμε είναι το **MyLastSearch**, το οποίο ανακτά όλες τις αναζητήσεις που έγιναν με τη χρήση των κύριων μηχανών αναζήτησης (Google, Yahoo και MSN), καθώς επίσης και των κύριων κοινωνικών δικτύων, όπως το Twitter, το Facebook, το MySpace, κλπ. Συνεπώς για να συγκεντρώσουμε πληροφορίες που αφορούν τις αναζητήσεις οι οποίες έχουν πραγματοποιηθεί στον υπό εξέταση υπολογιστή, δίνουμε την παρακάτω εντολή:

C:**>mylastsearch /stext mylastsearch.txt**

Μπορούμε να καταγράψουμε τα τελευταία γεγονότα που έχουν συμβεί στο παραβιασμένο σύστημα με την χρήση του εργαλείου **LastActivityView.** Η εντολή που δίνουμε είναι:

c:\>lastactivityview /stext lastactivityview.txt

Για να καταγράψουμε το Serial number και γενικότερα πληροφρίες για το υλικό του συστήματος, δίνουμε τις εντολές:

C:**> wmic csproduct get name > name.txt**
C:**> wmic bios get serialnumber > bios-serialnumber.txt**
C:**> wmic computersystem get manufacturer > manufacturer.txt**

Για να καταγράψουμε το Λειτουργικό σύστημα του υπολογιστή, δίνουμε τις εντολές:

C:\>systeminfo | findstr /B /C:"OS Name" /C:"OS Version" – CREDIT > os-version.txt

C:**>ver > Ver.txt**

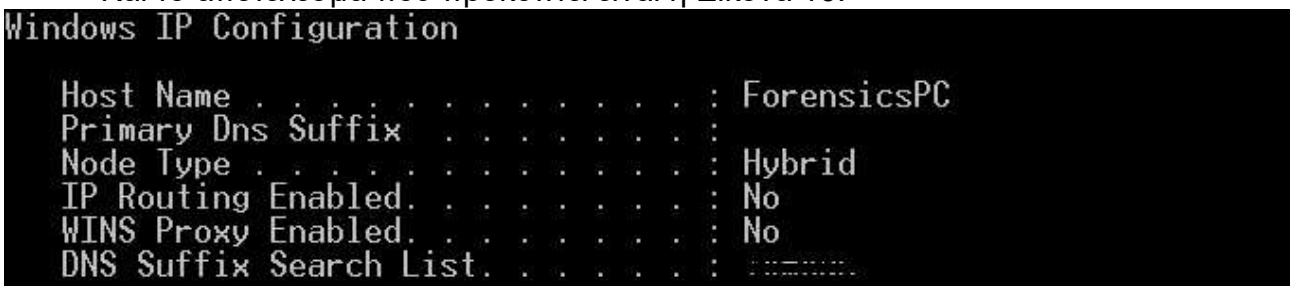
Πληροφορίες που αφορούν τους προσαρμογείς του δικτύου (network's adaptors) του συστήματος

Για να καταγράψουμε τους προσαρμογείς του δικτύου (network's adaptors), τη διαμόρφωσή τους, κλπ, χρησιμοποιούμε την εντολή **ipconfig**. Για να το κάνουμε αυτό, πληκτρολογούμε τις ακόλουθες εντολές:

c:**> ipconfig /all > ipconfig_all.txt**

c:**> ipconfig /allcompartments /all > ipconfig_all_comp.txt**

Και το αποτέλεσμα που προκύπτει είναι η Εικόνα 16:



Εικόνα 16

Το πρωτόκολλο DNS (Domain Name System) συσχετίζει τις IP διευθύνσεις με τα ονόματα των domain, καθώς τα τελευταία είναι πιο εύκολο να τα θυμόμαστε. Η DNS cache αποθηκεύει την προαναφερθείσα συσχέτιση όσον αφορά τα domains που έχουν γίνει προσβάσιμα από το σύστημα. Αυτή η λίστα μπορεί να ληφθεί χρησιμοποιώντας την εντολή **ipconfig**. Για να το κάνουμε αυτό, πληκτρολογούμε την ακόλουθη εντολή:

c:**> ipconfig /displaydns > ipconfig_displaydns.txt**

Και το αποτέλεσμα που προκύπτει είναι η Εικόνα 17:

Εικόνα 17: Περιεχόμενο DNS cache

Για να καταγράψουμε την MAC Address του υπολογιστή (NIC), δίνουμε τις ακόλουθες εντολές:

C:\>wmic nicconfig get description,IPAddress,MACaddress
C:\>getmac > getmac.txt

Για να καταγράψουμε την MAC Address του default gateway, δίνουμε την παρακάτω εντολή:

C:\>for /f "tokens=2 delims=:" %i in ('ipconfig ^| findstr /i "Default gateway" ^|findstr [0-9]') do arp -a %i

Για να συγκεντρώσουμε πληροφορίες που αφορούν όλες τις δικτυακές διεπαφές (network interfaces) στον υπό εξέταση υπολογιστή, δίνουμε την παρακάτω εντολή:

C:**>networkinterfacesview /stext networkinterfacesview.txt**

Σημείωση

Μία από τις δυνατότητες που έχουν οι κακόβουλοι χρήστες όταν παραβιάσουν ένα σύστημα είναι και να θέσουν την κάρτα δικτύου σε promiscuous mode, με άλλα λόγια, μπορούν να λαμβάνουν και να παρακολουθούν την κίνηση ολόκληρου του δικτύου. Για την ανίχνευση αυτού του είδους της πρακτικής, μπορούμε να χρησιμοποιήσουμε εργαλεία όπως το Promiscdetect.

Για να το κάνουμε αυτό, πληκτρολογούμε την ακόλουθη εντολή:

c:**> promiscdetect.exe > promiscdetect.txt**

Promiscdetect	http://ntsecurity.nu/downloads/promiscdetect.exe

Συλλογή συνθηματικών

Σε ορισμένα περιστατικά, είναι χρήσιμο να γνωρίζουμε τα διάφορα ονόματα χρηστών και τους κωδικούς πρόσβασης που είναι αποθηκευμένα στο σύστημα, γι' αυτό συνιστάται να τα συλλέξουμε, εφόσον μας έχει χορηγηθεί ρητή άδεια εκ των προτέρων και διατηρείται η συμμόρφωση με την ισχύουσα νομοθεσία όσον αφορά την προστασία των δεδομένων. Τα συνθηματικά μπορεί να χρησιμοποιηθούν για να αποκρυπτογραφηθούν τυχόν κρυπτογραφημένα δεδομένα ή και όπου χρειαστεί κατά την διάρκεια της διαδικασίας της ψηφιακή σήμανσης.

Υπάρχει ένας αριθμός από κωδικούς πρόσβασης που θα μπορούσαν να αποθηκευτούν στο σύστημα, από διάφορες υπηρεσίες, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, ηλεκτρονικές τραπεζικές συναλλαγές, υπηρεσίες εμπορίου, κλπ., καθώς και ένας μεγάλος αριθμός προγραμμάτων για τη συλλογή τους. Υπάρχουν αρκετά εργαλεία συλλογής συνθηματικών, μερικά θα τα παρουσιάσουμε εδώ.

Για να συλλέξουμε το σύνολο των συνθηματικών, θα χρησιμοποιήσουμε το project Lazagne (https://github.com/AlessandroZ/LaZagne/releases/download/2.0/Windows.zip)

Η εντολή που δίνουμε είναι:
c:\>laZagne.exe all > laZagne-passwords.txt

Για να ανακτήσουμε τα συνθηματικά από διάφορους email clients, δίνουμε την εντολή:
c:\>mailpv /stext mailpv.txt

Για να ανακτήσουμε τα συνθηματικά που βρίσκονται πίσω από τους αστερίσκους, δίνουμε την εντολή:
c:\>bulletspassview /stext bulletspassview.txt

Για να ανακτήσουμε τα συνθηματικά που έχουν αποθηκευτεί από τις διάφορες δικτυακές προσβάσεις χρησιμοποιούμε το **netpass (Network Password Recovery)** , που συλλέγει κωδικούς που αντιστοιχούν στους πόρους του δικτύου που ο τρέχων χρήστης είναι συνδεδεμένος. Εντολή:
c:\>netpass /stext netpass.txt

Για να ανακτήσουμε τα συνθηματικά από διάφορους web browsers, δίνουμε την εντολή:
c:\>webbrowserpassview /stext webbrowserpassview.txt

Το **WebBrowserPassView**: Συλλέγει τους κωδικούς πρόσβασης που αποθηκεύονται στα κύρια προγράμματα περιήγησης (browsers): Internet Explorer (Εκδόσεις 4.0 – 10.0), Mozilla Firefox (όλες οι εκδόσεις), Google Chrome, Safari και Opera.

Το **laZagne.exe**: Συλλέγει τους κωδικούς πρόσβασης που αποθηκεύονται στα κύρια προγράμματα περιήγησης (browsers): Internet Explorer, Mozilla Firefox (όλες οι εκδόσεις), Google Chrome, Safari και Opera. Εντολή:
c:\>laZagne.exe browsers > webbrowserpass.txt

Για να ανακτήσουμε τα συνθηματικά που έχουν αποθηκευτεί από τις διάφορες ασύρματες δικτυακές προσβάσεις, δίνουμε την εντολή:
c:\>wirelesskeyview /stext wirelesskeyview.txt

Για να ανακτήσουμε τα συνθηματικά που έχουν αποθηκευτεί από τις διάφορες απομακρυσμένες δικτυακές συνδέσεις (RDP-Remote Desktop Connections), δίνουμε την εντολή:
c:**>rdpv /stext rdpv.txt**

Συλλογή διαφόρων σχετικών πληροφοριών

Μπορούμε να συγκεντρώσουμε και άλλες χρήσιμες πληροφορίες από τον υπό εξέταση υπολογιστή .

Για να συγκεντρώσουμε πληροφορίες για τις προγραμματισμένες εργασίες (schedule tasks), δίνουμε την ακόλουθες εντολές:
c:**>at > at.txt**
c:**>schtasks /query /fo list /v > schtasks_query_fo_list_v.txt**
c:**>wmic job list brief> job-list-brief.txt**

Πληροφορίες που θα μπορούσαν να ενδιαφέρουν τον ελεγκτή είναι και αυτές που αποθηκεύονται στο πρόχειρο, όπως διευθύνσεις URLs, κωδικοί πρόσβασης, αποσπάσματα κειμένου, κλπ. Γι' αυτό συνιστάται να ελέγχουμε το περιεχόμενό του. Για να γίνει αυτό, μπορούν να χρησιμοποιηθούν εργαλεία όπως το **InsideClipboard** ή το **pclip** Για να συγκεντρώσουμε αυτές τις πληροφορίες που βρίσκονται στο πρόχειρο (clipboard), δίνουμε τις ακόλουθες εντολές:
c:**>pclip > pclip.txt**
c:**>InsideClipboard /stext InsideClipboard.txt**

Για να συγκεντρώσουμε πληροφορίες σχετικά με τις εφαρμογές που ξεκινούν κατά την εκκίνηση του υπολογιστή, δίνουμε τις ακόλουθες εντολές:
c:**>autorunsc /accepteula > autorunsc.txt**
c:**>wmic startup list brief > startup.txt**

Για να συλλέξουμε πληροφορίες για το MS-DOS Windows code page (Αριθμός που αντιστοιχεί στη γλώσσα του υπολογιστή), δίνουμε την εντολή:
c:\> chcp > chcp.txt

Για να συλλέξουμε συνολικές πληροφορίες για το MS-DOS Windows code page (Αριθμός που αντιστοιχεί στη γλώσσα του υπολογιστή), δίνουμε την εντολή:
c:\> chcp > chcp.txt

Για να συλλέξουμε πληροφορίες που αφορούν τους δίσκους που είναι συνδεδεμένοι στον υπό εξέταση υπολογιστή, δίνουμε τις παρακάτω εντολές:
c:\> wmic.exe diskdrive list brief /format:list > diskdrive.txt
c:\> wmic.exe logicaldisk where "drivetype!=4" get name > logicaldisk.txt
c:\> wmic.exe logicaldisk where "drivetype!=4" get size, caption > logicaldisk-size.txt

Για να συλλέξουμε πληροφορίες που αφορούν κρυφά αρχεία στον δίσκο (homedrive) του υπό εξέταση υπολογιστή, δίνουμε την εντολή:
c:\> dir /s /b /ahd "%HOMEDRIVE%\" > hidden-files.txt

Για να συλλέξουμε πληροφορίες που αφορούν Alternate Data Streams στον δίσκο (homedrive) του υπό εξέταση υπολογιστή, δίνουμε την εντολή:
c:\>streams.exe –a /accepteula > streams.txt

Για να συλλέξουμε πληροφορίες που αφορούν τον χρόνο κατά τον οποίο ο υπό εξέταση υπολογιστής λειτουργεί, δίνουμε την εντολή:
c:\>uptime.exe > uptime.txt

Το σύνολο των κακόβουλων χρηστών, όλο και ποιο συχνά χρησιμοποιεί εργαλεία κρυπτογράφησης, προκειμένου να αποκρύψει ενοχοποιητικές πληροφορίες. Είναι σημαντικό για έναν ερευνητή που εντοπίζει έναν υπολογιστή σε λειτουργία, να γνωρίζει άμεσα εάν έχει κρυπτογραφηθεί ο σκληρός ή μέρος του σκληρού με κάποιον γνωστό κρυπταλγόριθμο. Για τον εντοπισμό κρυπτογραφημένων δίσκων ή φακέλων μπορούμε να χρησιμοποιήσουμε το εργαλείο EDD (**Encrypted Disk Detector).** Το συγκεκριμένο εργαλείο εντοπίζει

γνωστούς κρυπταλγορίθμους ή προγράμματα κρυπτογράφισης, όπως το TrueCrypt, το PGP®, το Safeboot, ή το BitLocker®. Για να εντοπίσουμε τυχόν κρυπτογράφηση, πληκτρολογούμε την ακόλουθη εντολή:
c:**> EDD.exe > disk-encryption.txt**

Για να συλλέξουμε επιπλεόν πληροφορίες που αφορούν κρυπτογραφημένους φακέλους στον δίσκο του υπό εξέταση υπολογιστή, δίνουμε την εντολή:
c:**>cipher /q > cipher.txt**

Πληροφορίες για το firewall

Για να συγκεντρώσουμε πληροφορίες που αφορούν το δίκτυο του συστήματος. Και συγκεκριμένα εάν υπάρχει ενεργοποιημένο firewall, ποια είναι η πολιτική του και ποια τα logs του, δίνουμε τις παρακάτω εντολές:

C:\>netsh advfirewall show allprofiles
C:\>netsh advfirewall export "c:\advfirewallpolicy.wfw**"**
C:\>copy %windir%\System32\Logfiles\Firewall*.log

Ιστορικό της γραμμής εντολών.

Εάν κατά τη διεξαγωγή της διαδικασίας συλλογής αποδεικτικών στοιχείων υπάρχει ένα παράθυρο ανοιχτό της γραμμής εντολών (command interpreter), το ιστορικό των εκτελεσθέντων εντολών μπορεί να ληφθεί μέσω της ακόλουθης εντολής:
c:**>doskey /history > cmd-history.txt**

Εγγραφές σε αναμονή (Pending recordings)

Από τα Windows XP και μετά, τα λειτουργικά συστήματα έχουν την ικανότητα εγγραφής των CDs χωρίς την ανάγκη πρόσθετου λογισμικού. Η λειτουργία αυτή πρέπει να ληφθεί υπόψη σε ορισμένα περιστατικά, όπως εκείνα που σχετίζονται με την κλοπή/αντιγραφή πληροφοριών, ειδικότερα εάν ο δράστης πιαστεί «επ' αυτοφώρω». Η υποκλοπή μπορεί να γίνει μέσω USB drives, ωστόσο η υποκλοπή δεδομένων μέσω CD/DVD, δεν θα πρέπει να αποκλειστεί. Για το λόγο αυτό, εάν διαπιστώσουμε την ύπαρξη εγγραφών σε αναμονή (Pending recordings) θα πρέπει να ελεγχθούν, με σκοπό να είμαστε σε θέση να εντοπίσουμε, ποια αρχεία επρόκειτο να εγγραφούν.

Για να γίνει αυτό, εκτελούμε την ακόλουθη εντολή από ένα παράθυρο γραμμής εντολών, η οποία εξάγει τη λίστα των αρχείων εγγραφής που εκκρεμούν.

Στα Windows XP

dir %UserProfile%\Local Settings\Application Data\Microsoft\CD Burning > CD_Burning_info.txt

Στα Windows 7/8/10

dir %UserProfile%\AppData\Local\Microsoft\Windows\Burn > CD_Burning_info.txt

Σημείωση

Είναι δυνατόν να υποκαταστήσουμε τη ρύθμιση μεταβλητής %User Profile% με τη διαδρομή που αντιστοιχεί στον κατάλογο του προφίλ του χρήστη.

Αποτυπώσεις/Καταγραφές οθόνης (Screen captures)

Στην περίπτωση που απαιτηθεί από τον ερευνητή να ληφθεί μία εικόνα της επιφάνειας εργασίας (screenshot), τότε μπορεί να χρησιμοποιήσει από την γραμμή εντολών εργαλεία, όπως το boxcutter ή το CmdCapture. Οι εντολές που μπορεί να δώσει είναι:
c:\> boxcutter -f screenshot.bmp

ΤΜΗΜΑ 18
WINDOWS REGISTRY (Το μητρώο των Windows)

Η registry (μητρώο) περιέχει πληροφορίες που ανατρέχουν συνεχώς τα Windows κατά τη διάρκεια της λειτουργίας τους, όπως για παράδειγμα το προφίλ του κάθε χρήστη, τις εφαρμογές που είναι εγκατεστημένες στον υπολογιστή και τους τύπους των εγγράφων που ο κάθε χρήστης μπορεί να δημιουργήσει, τις ρυθμίσεις των ιδιοτήτων που αφορούν τα εικονίδια φακέλων και εφαρμογών, το υλικό που υπάρχει στο σύστημα και τις πόρτες που χρησιμοποιούνται από τις διάφορες εφαρμογές. Η registry (μητρώο) αποθηκεύει πληροφορίες μεγάλου ενδιαφέροντος για έναν εγκληματολογικό ερευνητή (προγράμματα που εκτελούνται όταν το σύστημα είναι ενεργοποιημένο, προφίλ χρηστών, πρόσβαση στις διαμορφώσεις ασύρματων δικτύων, ιστορικό των συνδεδεμένων συσκευών USB με το σύστημα, κλπ.), και για αυτό είναι απαραίτητο να δημιουργήσουμε ένα αντίγραφό του για μεταγενέστερη ανάλυση.

Η registry είναι μία ιεραρχική βάση δεδομένων όπου τα Windows αποθηκεύουν σχεδόν τα πάντα, όπως, ρυθμίσεις λειτουργικού συστήματος, ρυθμίσεις Υλικού (hardware), προτιμήσεις Χρηστών και ρυθμίσεις Εφαρμογών (Application Settings).

Η registry αποτελείται από δύο τμήματα ρυθμίσεων – πληροφοριών. Πρόκειται για τ**ις γενικές ρυθμίσεις του συστήματος** που αφορά υλικό και λογισμικό **και τις ρυθμίσεις χρηστών** που περιλαμβάνουν τις προσωπικές ρυθμίσεις του καθενός**.**

Η Windows registry περιέχει τις κυψέλες (Hives) οι οποίες χρησιμοποιούνται για να αποθηκεύουν δεδομένα της. Οι Κυψέλες (Hives) αποθηκεύονται σε διαφορετικά αρχεία τα οποία εξαρτώνται από την έκδοση των Windows.

Στον πίνακα που ακολουθεί, μπορούμε να δούμε τα κλειδιά του μητρώου (registry keys) μαζί με τις πληροφορίες που περιέχουν.

Registry Keys (Όνομα Κλειδιού)	Σύντμευση	Πληροφορίες που περιέχει
HKEY_CLASSES_ROOT	HKCR	Εξασφαλίζει ότι όταν 'ανοίγει' ένα αρχείο με τον Windows Explorer, θα χρησιμοποιηθεί το σωστό πρόγραμμα.
HKEY_CURRENT_USER	HKCU	Περιέχει τις προσωπικές ρυθμίσεις του χρήστη που είναι συνδεδεμένος στο σύστημα.
HKEY_LOCAL_MACHINE	HKML	Περιέχει πληροφορίες για τις γενικές ρυθμίσεις του υλικού του υπολογιστή.
HKEY_USERS	HKU	Περιέχει όλες τις ρυθμίσεις όλων των χρηστών του υπολογιστή.
HKEY_CURRENT_CONFIG	HKCC	Πληροφορίες σχετικές με το προφίλ του υλικού (hardware) που χρησιμοποιήθηκε από το τοπικό σύστημα, όταν το σύστημα 'ανοίγει' (switched on).

Πίνακας 2: Καταχωρήσεις μητρώου (registry entries) και οι πληροφορίες που περιέχουν

Για την εξαγωγή της registry και των πληροφοριών που περιέχει, θα πρέπει να εκτελέσουμε τις ακόλουθες εντολές:
Η γενική εντολή είναι:
c:\> **reg export Keyname Filename**

Παράδειγμα:
c:\>reg export HKLM\Software\MyApp MyAppBkUp.reg

Για να εξάγουμε το σύνολο της registry, **όταν ο υπολογιστής είναι σε λειτουργία**, μπορούμε να χρησιμοποιήσουμε εργαλεία, όπως το **forecopy_handy**, **rawcopy** και οι εντολές που δίνουμε είναι:
c:\>forecopy_handy -g Registry_Dir

Για να χρησιμοποιήσουμε το rawcopy θα πρέπει να του υποδείξουμε που είναι αποθηκευμένα τα αρχεία της registry. Εντολή:
c:\>RawCopy.exe /FileNamePath:C:\WINDOWS\system32\config\SYSTEM /OutputPath:E:\Registry_output

Στην registry υπάρχουν αρχεία που λειτουργούν και ως αντίγραφα ασφαλείας αυτών.
Στον πίνακα που ακολουθεί, μπορούμε να δούμε σημαντικά αρχεία της registry και αντίγραφα αυτών, καθώς και άλλα σχετικά με αυτά τα αρχεία.

Αρχεία Μητρώου	Σχετικά αρχεία
HKEY_CURRENT_CONFIG	System, System.log, System.alt, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav

HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.log, System.alt, System.sav
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav

Πίνακας 3: Αρχεία μητρώου (registry files) και συσχετισμένα με αυτά αρχεία

Τα αρχεία της registry είναι αποθηκευμένα στον φάκελο (διαδρομή): **%SystemRoot%\System32\Config** (για τα Windows NT/2000/XP) ή στο **%SystemRoot%\System32\Config\Regback** (για τα Windows 7/8/10).
Τα αρχεία ***Ntuser.dat*** και ***Ntuser.dat.log*** μπορούν να βρεθούν στο **%HomePath%**.

Το **USRCLASS.DAT** μας δίνει πληροφορίες σχετικά με την εκτέλεση προγραμμάτων και επίσης μπορεί να μας δώσει πληροφορίες σχετικά με ποιους φακέλους έχει ανοίξει ο χρήστης.
Το USRCLASS.DAT το βρίσκουμε στην διαδρομή:
C:\users\<username>\AppData\Local\Microsoft\windows\USRCLASS.DAT
(win7 & win8 & win10)
Στον πίνακα που ακολουθεί περιγράφονται τα αρχεία της registry και σε πια διαδρομή ή φάκελο βρίσκονται:

Όνομα αρχείου	Τοποθεσία/διαδρομή	περιεχόμενο
Ntuser.dat Εάν υπάρχουν πολλαπλοί χρήστες, τότε κάθε χρήστης έχει Ntuser.dat Ntuser.dat.log Ntuser.ini στην διαδρομή: c:\Users\user_name	C:\Users\USER_NAME.	Προστατευμένη περιοχή για τον χρήστη. Πιο πρόσφατα χρησιμοποιημένα αρχεία του χρήστη(MRU). Προσωπικές ρυθμίσεις
Default	\Windows\system32\config	Ρυθμίσεις συστήματος
SAM	\Windows\system32\config	Διαχείριση λογαριασμού χρηστών και ρυθμίσεις ασφαλείας
Security	\Windows\system32\config	Ρυθμίσεις ασφαλείας
Software	\Windows\system32\config	Όλα τα εγκατεστημένα προγράμματα και οι ρυθμίσεις τους
system	\Windows\system32\config	Ρυθμίσεις συστήματος
USRCLASS.dat	C:\Users\YourUserName\AppData\Local\Microsoft\Windows\	Πληροφορίες σχετικά με την δράση του χρήστη

Πίνακας 4: Αρχεία μητρώου (registry files) και σχετική διαδρομή (path)

Μπορούμε να εξάγουμε την registry και από ένα αντίγραφο του σκληρού δίσκου του υπό εξέταση συστήματος. Σε αυτή την περίπτωση μπορούμε να χρησιμοποιήσουμε και εργαλεία με γραφικό περιβάλλον, όπως το **ftk imager**.

Ίσως να **μην** είναι απαραίτητο, ανάλογα με το περιστατικό, να εξάγουμε ολόκληρο το μητρώο (registry), αλλά με την εξαγωγή συγκεκριμένων κλειδιών να ολοκληρώσουμε την υπόθεσή μας.

Για να αντιγράψουμε το **ntuser.dat** για κάθε χρήστη δίνουμε την εντολή:
Για windows XP:
c:\>for /F %%i in ('dir /b "c:\Documents and Settings"') do rawcopy.exe "c:\Documents and Settings\%%i\NTUSER.dat" "ntuser_%%i.dat"

Για win7/8/10
c:**> for /F %%i in ('dir /b c:\Users') do rawcopy.exe "c:\Users\%%i\NTUSER.dat" "ntuser_%%i.dat"**

Για να αντιγράψουμε το **USRCLASS.dat** για κάθε χρήστη δίνουμε την εντολή:
Για win7/8/10
c:**> for /F %%i in ('dir /b c:\Users') do rawcopy.exe "C:\Users\%%i\AppData\Local\Microsoft\Windows\USRCLASS.dat" "USRCLASS_%%i.dat"**

Άλλα εργαλεία

RegRipper	https://code.google.com/p/regripper
RegFileExport	http://www.nirsoft.net/utils/registry_file_offline_export.html
Forensic Registry EDitor (fred)	https://www.pinguin.lu/index.php
Registry Decoder	https://code.google.com/p/registrydecoder

Σημαντικό

Πρέπει να γνωρίζουμε την φύση της υπόθεσης ώστε να συλλέγουμε μόνο τις πληροφορίες που είναι σχετικές και όχι το σύνολο των πληροφοριών που σε μερικές υποθέσεις μπορεί να έχουν τεράστιο όγκο.

Ακολούθως περιγράφονται μερικά σημαντικά αποδεικτικά στοιχεία που μπορούν να εξαχθούν από το μητρώο (registry). Είναι σημαντικό να γνωρίζουμε που μπορούμε να βρούμε την πληροφορία που αναζητάμε, ώστε να επικεντρωνόμαστε σε αυτή την πληροφορία και όχι να συγκεντρώνουμε πληθώρα στοιχείων που θα μας δυσκολέψουν στην ανάλυση.

Παραδείγματα τιμών - πληροφοριών που υπάρχουν στην Registry

- Όνομα υπολογιστή (Computer Name)

- Πότε έκλεισε ο υπολογιστής τελευταία φορά (Last Shutdown Time)
- Ποια προγρματα ή οδηγοί εκκινούν (Startup Drivers / Programs)
- Τα ονόματα και οι λογαριασμοί χρηστών (User Account Names)
- Ρυθμίσεις εφαρμογών (Application Settings)
- Σελίδα εκκίνησης του Internet Explorer (IE Start Page)
- Skype Username
- Πρόσφατη προσπέλαση, Προγραμμάτων (Programs), Ιστοσελίδων (Web Pages) και Αρχείων (Files)
- Πρόσφατα συνδεδεμένα Ασύρματα δίκτυα (Wireless Networks) και USB συσκευές (Drives)

Συνδεδεμένες συσκευές USB

Με κάθε σύνδεση μιας νέας συσκευής USB στο σύστημα, δημιουργείται μια αντίστοιχη εγγραφή μητρώου (registry record). Στην συγκεκριμένη εγγραφή μπορούμε να εντοπίσουμε πληροφορίες όπως ο κατασκευαστής της συσκευής, τον μοναδικό σειριακό αριθμό (unique serial number), το γράμμα σύνδεσης, τον χρήστη που άνοιξε την συσκευή και το Globally Unique Identifier (GUID). Για να συγκεντρώσουμε όλες αυτές τις πληροφορίες, εργαζόμαστε ως ακολούθως:

Έχουμε αντιγράψει την registry και μπορούμε να βρούμε τις πληροφορίες που αναζητάμε ως εξής:

Για να καταγράψουμε τον κατασκευαστή, το προϊόν και την έκδοση (Vendor,Product,Version), τα αναζητούμε στην διαδρομή:
SYSTEM\CurrentControlSet\Enum\USBSTOR

Για να καταγράψουμε το σειριακό αριθμό (Serial Number), το αναζητούμε στην διαδρομή:
SYSTEM\CurrentControlSet\Enum\USBSTOR

Για να καταγράψουμε το γράμμα που αντιστοιχεί στον οδηγό φόρτωσης(Drive Letter Device Mapped To) το αναζητούμε με βάση τον σειριακό αριθμό (Serial Number) στην διαδρομή:
SOFTWARE\Microsoft\Windows Portable Devices\Devices

Για να καταγράψουμε το Volume GUIDs (Globally Unique Identifier) το αναζητούμε στην διαδρομή με βάση τον σειριακό αριθμό (Serial Number) :
SYSTEM\MountedDevices

Για να καταγράψουμε τον χρήστη που χρησιμοποίησε την συγκεκριμένη συσκευή, πάμε στην διαδρομή και κάνουμε αναζήτηση με βάση το GUID της συσκευής:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Για να καταγράψουμε τον τελευταίο χρόνο που συνδέθηκε η συσκευή, τον αναζητούμε στην διαδρομή με βάση τον σειριακό αριθμό (Serial Number):
SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Για να καταγράψουμε την πρώτη φορά που συνδέθηκε η συσκευή, την αναζητούμε στην διαδρομή με βάση τον σειριακό αριθμό (Serial Number):
C:\Windows\inf\setupapi.dev.log

Συνεπώς για τους παραπάνω λόγους αντιγράφουμε από την Registry, το **System.dat**, το **Software.dat** και το **Ntuser.dat**. Από τα μητρώα καταγραφής συμβάντων (log files) αντιγράφουμε τα **Setupi.log** (Plug & play log) και τα **Event Logs.**

Για να συλλέξουμε τις παραπάνω πληροφορίες πρέπει να εκτελεστούν οι παρακάτω εντολές:
c:\> RawCopy.exe /FileNamePath:C:\WINDOWS\system32\config\SYSTEM /OutputPath:E:\system
c:\> RawCopy.exe /FileNamePath:C:\WINDOWS\system32\config\SOFTWARE /OutputPath:E:\software

Για να αντιγράψουμε το ntuser.dat για κάθε χρήστη δίνουμε την εντολή:
Για windows XP:
c:\>for /F %%i in ('dir /b "c:\Documents and Settings"') do rawcopy.exe "c:\Documents and Settings\%%i\NTUSER.dat" "ntuser_%%i.dat"

Για win7/8/10
c:\> for /F %%i in ('dir /b c:\Users') do rawcopy.exe "c:\Users\%%i\NTUSER.dat" "ntuser_%%i.dat"

Για να αντιγράψουμε το Setupi.log, δίνουμε την εντολή:
c:\> RawCopy.exe /FileNamePath:C:\Windows\inf\setupapi.dev.log /OutputPath:E:\setupi.dev.log
c:\> RawCopy.exe /FileNamePath:C:\Windows\setupapi.log /OutputPath:E:\setupi.log **(windows XP)**

Για να αντιγράψουμε τα **Event Logs**, δίνουμε την εντολή:
c:\> forecopy_handy -e event_log_Dir

Άλλα εργαλεία

USBView	https://msdn.microsoft.com/en-us/library/windows/hardware/ff560019(v=vs.85).aspx
USBDeviceForensics	http://www.woanware.co.uk/downloads/USBDeviceForensics.v1.0.14.zip
USB History Dump	http://sourceforge.net/projects/USBhistory/

Λίστα των δικτύων Wi-Fi με τα οποία έχει συνδεθεί το σύστημα

Στην περίπτωση ενός υπό εξέταση υπολογιστή, μπορεί να είναι σημαντικό

να για τον ερευνητή να εντοπίσει με ποια ασύρματα δίκτυα (κατά κύριο λόγο Wi-Fi) έχει συνδεθεί και ποιες είναι οι ρυθμίσεις τους. Μπορούμε να αναζητήσουμε πληροφορίες στην registry. Ένα εργαλείο που μπορεί να μας δώσει πληροφορίες σχετικά με τις συνδέσεις στα ασύρματα δίκτυα είναι και το WifiHistoryView. Εντολή:
c:\> **WifiHistoryView /stext WifiHistoryView.txt**

Στα Windows XP, με την χρήση των παρακάτω εντολών μπορούμε μέσα από τις αντίστοιχες εγγραφές μητρώου (registry records), να εξάγουμε τις πληροφορίες που αναζητούμε:
c:\> **reg export HKLM|SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces**
c:\> **reg export HKLM|SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards**

Τα αναγνωριστικά (Identifiers) για οποιαδήποτε ασύρματο δίκτυο που το σύστημα είχε συνδεθεί, βρίσκονται αποθηκευμένα στο ακόλουθο κλειδί της registry:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless

Αυτό το κλειδί, δεν είναι τίποτα άλλο από μια λίστα με τα αναγνωριστικά για κάθε ένα από τα ασύρματα δίκτυα που το σύστημα έχει συνδεθεί.

Συνεπώς δίνουμε την εντολή:
c:\> **reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless**

Περισσότερες πληροφορίες σχετικά με κάθε ένα από αυτά τα ασύρματα δίκτυα, όπως τη διεύθυνση MAC, την προεπιλεγμένη πύλη (default gateway), DNS suffix και SSID μπορούν επίσης να βρεθούν εντός του μητρώου (registry). Αυτό μπορεί να γίνει χρησιμοποιώντας το αναγνωριστικό από το προηγούμενο κλειδί και κάνοντας αναζήτηση στο κλειδί:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
Αυτό το κλειδί περιέχει σημαντικές πληροφορίες για τα δίκτυα γενικά.

Συνεπώς δίνουμε την εντολή:
c:\> **reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged**

Επιπλέον, το μητρώο των Windows (registry) περιέχει σημαντικές πληροφορίες για τον ερευνητή όσο αφορά τα ασύρματα δίκτυα. Οι πληροφορίες αυτές περιλαμβάνουν την ημερομηνία που δημιουργήθηκε η σύνδεση και την τελευταία φορά που συνδέθηκε ο υπολογιστής. Οι ημερομηνίες- πληροφορίες αυτές βρίσκονται στο κλειδί:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{Wireless – Identifier}

Συνεπώς δίνουμε την εντολή:
c:\>**reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{Wireless – Identifier}**

Επίσης στην περίπτωση των Windows 7/8/10, υπάρχουν πληροφορίες για τα ασύρματα δίκτυα σε αρχεία με κατάληξη XML που είναι αποθηκευμένα στον δίσκο και βρίσκονται στον φάκελο:
%SYSTEMDRIVE%\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}\{Random-GUID}.xml
Συνεπώς αντιγράφουμε το περιεχόμενο με την εντολή **copy.**

Οι πληροφορίες που αποθηκεύονται στον παραπάνω φάκελο, περιλαμβάνουν το SSID, μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης, μαζί με τα κλειδιά κρυπτογράφησης και τα συνθηματικά.

Μπορούμε να συλλέξουμε πληροφορίες για τα ασύρματα δίκτυα με τις παρακάτω εντολές:
c:\> Netsh WLAN show profiles > wlan_profiles.txt
c:\> Netsh WLAN show all > wlan_show_all.txt
c:\> Netsh WLAN show interfaces > wlan_interfaces .txt
c:\> Netsh WLAN show drivers > wlan_drivers.txt
c:\> Netsh WLAN export profile

Άλλα εργαλεία

WifiHistoryView	http://www.nirsoft.net/utils/wifi_history_view.html
WirelessNetConsole	http://www.nirsoft.net/utils/wireless_net_console.html

Διαμόρφωση του Windows Security Center / Windows Action Center

Η Microsoft, από τα Windows XP Service Pack 2 και μετά, συμπεριέλαβε το Security Center (Κέντρο Ασφαλείας), το οποίο στις επόμενες εκδόσεις του λειτουργικού συστήματος συνεχίστηκε για να ονομαστεί Action Center (Κέντρο Ενεργειών). Αυτό το κέντρο αποτελεί μία διεπαφή, όπου τα κύρια θέματα που σχετίζονται με την ασφάλεια του συστήματος μπορούν να προβληθούν και να ρυθμιστούν: τείχος προστασίας (firewall), αυτόματες αναβαθμίσεις (automatic upgrades), ειδοποιήσεις (notifications), κλπ.

Η διαμόρφωση/ρύθμιση αυτού του κέντρου είναι αποθηκευμένη στο μητρώο (registry). Μπορεί να απαιτηθεί από τον ερευνητή να συλλέξει το σύνολο των πληροφοριών που περιλαμβάνονται σε αυτό το κλειδί της registry, ανάλογα πάντα με την υπόθεση. Η εντολή που δίνουμε είναι:

Στα Windows XP:
c:\> reg export HKLM\SOFTWARE\Microsoft\Security Center\ Security_Center.reg

Στα Windows 7/8/10:
c:\> reg export HKLM\SOFTWARE\Microsoft\Security Center\ Security_Center.reg
c:\> reg export HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center Action_Center.reg

Διαμόρφωση του τείχους προστασίας (firewall) των Windows

Στη διαμόρφωση του τείχους προστασίας των Windows αποθηκεύονται οι επιτρεπόμενες εφαρμογές, οι ανοιχτές θύρες και άλλες πληροφορίες σχετικά με το ίδιο το τείχος προστασίας.

Για να εξάγουμε αυτές τις πληροφορίες, εκτελούμε την ακόλουθη εντολή:

c:\> reg export HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy FirewallPolicy.reg

Προγράμματα που εκτελούνται όταν το λειτουργικό σύστημα είναι ενεργοποιημένο

Για να ξεκινήσει ένα πρόγραμμα όταν το λειτουργικό σύστημα εκκινεί (boot), θα πρέπει να έχει μεταξύ άλλων και μία εγγραφή στην registry. Τα βασικά μονοπάτια (path) της registry, όπου μπορούμε να εντοπίσουμε τις λίστες των προγραμμάτων που εκτελούνται όταν το λειτουργικό σύστημα εκκινεί, είναι τα ακόλουθα:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager

Γι' αυτό, ανάλογα με την υπόθεση και ειδικότερα σε υπόθεση παραβίασης ενός υπολογιστή, επιβάλλεται να αντιγράψουμε / εξάγουμε αυτά τα registry keys μέσω των παρακάτω εντολών:

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders" HKCU_Software_Microsoft_Windows_CurrentVersion_Explorer_Shell_Folders.reg

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" HKCU_Software_Microsoft_Windows_CurrentVersion_Explorer_User_Shell_Folders.reg

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" HKCU_Software_Microsoft_Windows_CurrentVersion_Run.reg

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce" HKCU_Software_Microsoft_Windows_CurrentVersion_RunOnce.reg

reg export "HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows" HKCU_Software_Microsoft_WindowsNT_CurrentVersion_Windows.reg

reg export "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders" HKLM_Software_Microsoft_Windows_CurrentVersion_Explorer_Shell_Folders.reg

reg export "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" HKLM_Software_Microsoft_Windows_CurrentVersion_Explorer_User_Shell_Folders.reg

reg export "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" HKLM_Software_Microsoft_Windows_CurrentVersion_Policies_Explorer.reg

reg export "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" HKLM_Software_Microsoft_Windows_CurrentVersion_Run.reg

reg export "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce" HKLM_Software_Microsoft_Windows_CurrentVersion_RunOnce.reg

reg export "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager" HKLM_SYSTEM_CurrentControlSet_Control_Session_Manager.reg

Άλλα εργαλεία

Autoruns	http://technet.microsoft.com/es-es/sysinternals/bb963902.aspx
WhatInStartup	http://www.nirsoft.net/utils/what_run_in_startup.html

Οι τύποι αρχείων και τα σχετικά/αντίστοιχα προγράμματα που χρησιμοποιούνται για να τα ανοίξουμε.

Τα Windows αποθηκεύουν, στη registry, τις αντιστοιχίες μεταξύ των τύπων των αρχείων και τα προγράμματα που πρέπει να χρησιμοποιηθούν για να τα ανοίξουν. Σε ορισμένα περιστατικά, κυρίως εκείνα που σχετίζονται με ιομορφικό λογισμικό, ο κακόβουλος χρήστης έχει την δυνατότητα να τροποποιήσει αυτές τις εγγραφές, ώστε κάθε φορά που καλείται ένα πρόγραμμα να ανοίξει ένα αρχείο, ταυτόχρονα να εκτελεί και το ιομορφικό λογισμικό.

Σαν συνέπεια αυτής της τεχνικής θα πρέπει ο ερευνητής να αντιγράφει αυτές τις εγγραφές για περαιτέρω ανάλυση. Οι εντολές που θα χρειαστεί να δώσουμε είναι:

Εκτελούμε το παρακάτω batch file:

@echo off
for %%i in (batfile cmdfile comfile exefile htafile https JSEfile piffile regfile scrfile txtfile VBSfile WSFFile) do (reg export "HKEY_CLASSES_ROOT\%%i\shell\open\command" "HKCR-%%i.reg")

for %%i in (batfile comfile exefile piffile) do (reg export "HKEY_LOCAL_MACHINE\software\Classes\%%i\shell\open\command" "HKLM-%%i.reg")

ή τις επιμέρους εντολές όπως παρακάτω:

reg export "HKEY_CLASSES_ROOT\batfile\shell\open\command" "HKCR-batfile.reg"

reg export "HKEY_CLASSES_ROOT\cmdfile\shell\open\command" "HKCRcmdfile.reg"

reg export "HKEY_CLASSES_ROOT\comfile\shell\open\command" "HKCRcomfile.reg"

reg export "HKEY_CLASSES_ROOT\exefile\shell\open\command" "HKCRexefile.reg"

reg export "HKEY_CLASSES_ROOT\htafile\shell\open\command" "HKCRhtafile.reg"

reg export "HKEY_CLASSES_ROOT\https\shell\open\command" "HKCRhttps.reg"

reg export "HKEY_CLASSES_ROOT\JSEfile\shell\open\command" "HKCRJSEfile.reg"

reg export "HKEY_CLASSES_ROOT\piffile\shell\open\command" "HKCRpiffile.reg"

reg export "HKEY_CLASSES_ROOT\regfile\shell\open\command" "HKCRregfile.reg"

reg export "HKEY_CLASSES_ROOT\scrfile\shell\open\command" "HKCRscrfile.reg"

reg export "HKEY_CLASSES_ROOT\txtfile\shell\open\command" "HKCRtxtfile.reg"

reg export "HKEY_CLASSES_ROOT\VBSfile\shell\open\command" "HKCRVBSfile.reg"

reg export "HKEY_CLASSES_ROOT\WSFFile\shell\open\command" "HKCRWSFFile.reg"

reg export "HKEY_LOCAL_MACHINE\software\Classes\batfile\shell\open\command" "HKLMbatfile.reg"

reg export "HKEY_LOCAL_MACHINE\software\Classes\comfile\shell\open\command" "HKLMcomfile.reg"

reg export "HKEY_LOCAL_MACHINE\software\Classes\exefile\shell\open\command" "HKLMexefile.reg"

reg export "HKEY_LOCAL_MACHINE\software\Classes\piffile\shell\open\command" "HKLMpiffile.reg"

Συσχετισμός αρχείων με φίλτρα (Image File Execution Options)

Το χαρακτηριστικό των Windows, **Image File Execution Options** (IFEO) χρησιμοποιείται για αποσφαλμάτωση (debugging). Το ιομορφικό λογισμικό ελέγχει εάν υπάρχουν σε λειτουργία debuggers και ταυτόχρονα εκμεταλλεύεται το συγκεκριμένο χαρακτηριστικό για να εκκινεί τον εαυτό του (το ιομορφικό λογισμικό). Οι ρυθμίσεις του IFEO είναι αποθηκευμένες στην registry. Ο Σκοπός του Image File Execution Options registry key είναι να δώσει την δυνατότητα στους developers να βρουν τυχόν σφάλματα στον κώδικά τους. Αυτό γίνεται μέσα από το συγκεκριμένο κλειδί της registry και μπορούμε να επισυνάψουμε ένα πρόγραμμα σε ένα εκτελέσιμο (.exe). Η διαδικασία είναι απλή στο path του κλειδιού, προσθέτουμε ένα πρόγραμμα, όπως στο παράδειγμα που ακολουθεί:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\{name of the executable}
προσθέτουμε στο path του debugger όποιο ιομορφικό λογισμικό θέλουμε
“Debugger”=”{full path to the malware}”

Αυτό σημαίνει πως κάθε φορά που θα καλούμε το exe θα εκτελείται και το malware. Συνεπώς ο ερευνητής θα πρέπει να λαμβάνει αντίγραφο του συγκεκριμένου κλειδιού της registry για ανάλυση δίνοντας την εντολή:
reg export "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options" "HKLM-IFEO.reg"

Browser Helper Objects (BHO)

Ένα Βοηθητικό αντικείμενο προγράμματος περιήγησης (BHO-Browser

Helper Object (BHO)) είναι ένα DLL που έχει σχεδιαστεί ως ένα plugin για τον φυλλομετρητή (web browser) Internet Explorer της Microsoft για να παράσχει πρόσθετες λειτουργίες. Τα BHOs εισήχθησαν τον Οκτώβριο του 1997 με την απελευθέρωση της έκδοσης 4 του Internet Explorer. Τα περισσότερα BHOs φορτώνονται μία φορά σε κάθε νέα σύνοδο λειτουργίας του Internet Explorer. Ωστόσο, στην περίπτωση του Windows Explorer, ένα νέο στιγμιότυπο ξεκινά κάθε φορά που ανοίγει ένα νέο παράθυρο.

Κάθε φορά που ξεκινά μια νέα σύνοδο λειτουργίας του Internet Explorer, τότε ελέγχεται η registry εάν υπάρχει το κλειδί **HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Object**s. Εάν ο Internet Explorer βρει αυτό το κλειδί στο μητρώο, αναζητά το κλειδί της μορφής CLSID. Τα κλειδιά CLSID που βρίσκονται στα Browser Helper Objects λένε στον φυλλομετρητή ποια BHOs να φορτώσει. Εάν διαγράψουμε το κλειδί δεν θα φορτώνονται τα BHOs και έτσι θα εμποδίσουμε και τυχόν ιομορφικά λογισμικά. Με λίγα λόγια οι κακόβουλοι χρήστες μπορούν να χρησιμοποιήσουν τα BHOs για να εκκινήσουν ιομορφικό λογισμικό. Συνεπώς ο ερευνητής θα πρέπει να αντιγράψει το συγκεκριμένο κλειδί για περαιτέρω ανάλυση. Η εντολή που πρέπει να δώσουμε είναι:

reg export "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects" "BHOs.reg"

UserAssist

Τα προγράμματα με γραφικό περιβάλλον τα οποία ανοίγονται από την επιφάνεια εργασίας (desktop), καταγράφονται στην registry στο UserAssist κλειδί. Το συγκεκριμένο κλειδί βρίσκεται στην διαδρομή:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

Συνεπώς έχοντας αντιγράψει πιο πάνω το ntuser.dat έχουμε συλλέξει και την συγκεκριμένη πληροφορία. Μπορούμε να το εξάγουμε δίνοντας την εντολή:

c:**> reg export “HKCU\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\“ “UserAssist .reg”**

MUICache

Κάθε φορά που ένας χρήστης εκτελεί ένα πρόγραμμα/εφαρμογή για πρώτη φορά, το όνομα του προγράμματος καταχωρείται σε συγκεκριμένο κλειδί στην registry. Το κλειδί βρίσκεται στη διεύθυνση:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache στα Windows XP.

- HKEY_CURRENT_USER\Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache στα Windows 7/8/10.

Για να εξάγουμε το συγκεκριμένο κλειδί για περαιτέρω ανάλυση, δίνουμε τις ακόλουθες εντολές:

Στα Windows XP
reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache" "HKCU-Muicache.reg"

Στα Windows 7/8/10

reg export "HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" "HKCU-Muicache.reg"

Άλλα εργαλεία

MUICacheView	http://www.nirsoft.net/utils/muicache_view.html
RegRipper	https://github.com/keydet89/RegRipper2.8

RunMRU

Κάθε φορά που ένας χρήστης χρησιμοποιεί το Start -> Run για να εκτελέσει μία εντολή, τότε αυτή αποθηκεύεται στην registry στο RunMRU. Το συγκεκριμένο κλειδί το βρίσκουμε στην διαδρομή:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Συνεπώς το αντιγράφουμε ή το εξάγουμε με την εντολή:

c:**> reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" "RunMRU.reg"**

LastVisitedMRU / LastVisitedPidlMRU

Το LastVisitedMRU Windows Registry κλειδί καταγράφει τις πρόσφατα χρησιμοποιημένες εφαρμογές και το τελευταίο μονοπάτι (path) αυτών των εφαρμογών που χρησιμοποιήθηκαν για να ανοίξουν ένα αρχείο. Χρησιμοποιείται από το windows λειτουργικό σύστημα για να αποθηκεύει το μονοπάτι των εφαρμογών που έχουν χρησιμοποιηθεί πρόσφατα για να ανοίξουν ένα αρχείο και για να παρέξει υπηρεσίες αυτόματης συμπλήρωσης (auto-complete) στον χρήστη. Στη registry αποθηκεύεται η λίστα των πιο πρόσφατα χρησιμοποιημένων εφαρμογών. Αυτή η πληροφορία μπορεί να είναι ενδιαφέρουσα σε ορισμένους τύπους υποθέσεων, οπότε για να την εξάγουμε, πρέπει να εκτελεστεί η ακόλουθη εντολή:

Windows XP

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU" "HKCU-LastVisitedMRU.reg"

Windows 7/8/10

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU" "HKCU-LastVisitedPidlMRU.reg"

OpenSaveMRU / OpenSavePidMRU

Στην registry υπάρχουν τα κλειδιά ***OpenSaveMRU*** και **OpenSavePidMRU.** Το **OpenSaveMRU** (στα Windows XP και 2003) και το **OpenSavePidMRU** (στα Vista μέχρι τα Windows 10) καταγράφουν τα αρχεία τα οποία ο λογαριασμός του χρήστη έχει πρόσβαση μέσω του διαλόγου Open και Save As. Για να εντοπίσει ο ερευνητής πληροφορίες που αφορούν αρχεία που έχουν ανοιχτεί ή αποθηκευτεί μέσω του διαλόγου Open και Save As, θα πρέπει να δώσει την εντολή:

Στα Windows XP

reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU" "HKCU-OpenSaveMRU.reg"

Στα Windows 7/8/10

reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU" "HKCU-OpenSavePidMRU.reg"

Πρόσφατα ανοιγμένα αρχεία - RecentDocs

Τα Windows καταγράφουν με πολλές λεπτομέρειες τα κείμενα (documents) τα οποία ο χρήστης είχε πρόσβαση και αυτές οι πληροφορίες αποθηκεύονται στην registry, στο κλειδί RecentDocs. Αναλύοντας τις πληροφορίες που μας παρέχει το συγκεκριμένο κλειδί, μπορούμε να εντοπίσουμε πολλές από τις δραστηριότητες του χρήστη. Για να ανακτήσει ο ερευνητής το συγκεκριμένο κλειδί, δίνει την εντολή:

reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs" "HKCU-RecentDocs.reg"

AppCompatCache /AppCompatibility

Η βάση των Windows που αναφέρεται στην συμβατότητα των εφαρμογών

με το λειτουργικό (Windows Application Compatibility Database) χρησιμοποιείται για να αναγνωρίζει τυχόν προβλήματα συμβατότητας των εκτελέσιμων με το λειτουργικό. Καταγράφει το όνομα του εκτελέσιμου, το μέγεθος του αρχείου, πότε τροποποιήθηκε τελευταία φορά και στα Windows XP κρατά και τον τελευταίο χρόνο που ενημερώθηκε (last update time).
Όλες οι πληροφορίες αποθηκεύονται στο AppCompatCache / AppCompatibility και βρίσκεται στην διαδρομή:

Στα Windows XP
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility

Στα Windows 7/8/10
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Συνεπώς είναι σημαντικό για τον ερευνητή να αντιγράφει αυτές τις βάσεις προκειμένου να εντοπίσει την χρήση ιομορφικού λογισμικού, στον υπό εξέταση υπολογιστή.
Για να την αντιγράψουμε την βάση, δίνουμε την εντολή:
c:/> reg export "SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility" "AppCompatibility.reg"
c:/> reg export "SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache" "AppCompatCache.reg"

Εγκατεστημένο λογισμικό

Τα Windows αποθηκεύουν στην registry μια λίστα του εγκατεστημένου λογισμικού μαζί με τις πληροφορίες του. Για να εξάγουμε τις πληροφορίες αυτές, θα πρέπει να εκτελέσουμε την ακόλουθη εντολή:

reg export "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall" "HKCL-Installed-software.reg"

Πρόσφατες αναζητήσεις – ACMRU-WordWheelQuery

Οι χρήστες αναζητούν συχνά πληροφορίες με βάση το όνομα αρχείου ή κάποια λέξη κλειδί μέσα σε ένα αρχείο, στον υπολογιστή τους ή σε άλλα συστήματα ή στο διαδίκτυο. Αυτή την αναζήτηση έχουν την δυνατότητα να την κάνουν μέσα από το πλαίσιο αναζήτησης (search box) που παρέχει το ίδιο το λειτουργικό σύστημα. Όταν ο χρήστης χρησιμοποιήσει αυτή την δυνατότητα, οι αναζητήσεις, στα Windows XP καταγράφονται στο κλειδί: **HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMru**

Στα windows vista, οι πληροφορίες των αναζητήσεων καταγράφονται σε αρχείο. Ενώ στα windows 7 και πέρα, οι πληροφορίες των αναζητήσεων καταγράφονται στην registry στο κλειδί:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Για να το εξάγουμε τα συγκεκριμένα κλειδιά, δίνουμε την εντολή:

Για τα windows XP
reg export "HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMru" "HKCU-ACMru.reg"
Για τα Windows 7/8/10:

reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery" "HKCU-WordWheelQuery.reg"

Πληκτρολογημένα μονοπάτια – TypedPaths

Το TypedPaths κλειδί (Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths) καταγράφει τα μονοπάτια (paths) που ο χρήστης πληκτρολογεί στον Windows Explorer. Στα Windows 10, πληκτρολογώντας στο μικρό πλαίσιο (little box) κάτω δεξιά δίπλα από το σύμβολο των Windows εικόνα, σε αυτό που συνήθως λέει “Search the web and Windows”, τότε ενεργοποιεί το συγκεκριμένο κλειδί και καταγράφει τα δεδομένα.
Για να το εξάγουμε το συγκεκριμένο κλειδί, δίνουμε την εντολή:

reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths" "TypedPaths.reg"

ΤΜΗΜΑ 19
ΠΡΟΣΩΡΙΝΑ ΑΠΟΘΗΚΕΥΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΣΕ ΠΡΟΓΡΑΜΜΑΤΑ ΠΕΡΙΗΓΗΣΗΣ (Διευθύνσεις, Λήψη Ιστορικού)

Συλλογή πληροφοριών από φυλλομετρητές

Όλοι οι φυλλομετρητές αποθηκεύουν πληροφορίες, όπως διευθύνσεις, ιστορικό και άλλες πληροφορίες, χρήσιμες για τον ερευνητή. Για να συλλέξουμε αυτές τις πληροφορίες, υπάρχουν αρκετά εργαλεία. Κάποια από αυτά θα τα παρουσιάσουμε στην συνέχεια.

Γενικά στην ψηφιακή σήμανση, σχετικά με τους φυλλομετρητές μπορούμε να εντοπίσουμε πληροφορίες, όπως:

- **Ποιες ιστοσελίδες επισκέφτηκε ο χρήστης**
  - History --> cache --> Cookies --> Recovery folders --> Suggested sites
- **Πόσες φορές επισκέφτηκε μία ιστοσελίδα**
  - History
- **Πότε επισκέφτηκε μία ιστοσελίδα**
  - History --> cache --> Cookies --> Recovery folders
- **Τι ιστοσελίδες αποθήκευσε ο χρήστης**
  - Bookmarks
- **Αρχεία που τυχόν κατέβασε ο χρήστης**
  - Download folder → cache
- **Εντοπισμός ονόματος χρηστών**

- cache --> Cookies --> Recovery folders → autocomplete
- **Εντοπισμός των αναζητήσεων του χρήστη**
- cache → autocomplete

Για την συλλογή πληροφοριών του Internet Explorer, χρησιμοποιούμε το εργαλείο forecopy_handy και δίνουμε την εντολή:

c:**> forecopy_handy.exe -i internet_explorer_dir**

Μπορούμε επίσης να αντιγράψουμε τα δεδομένα που χρειαζόμαστε μέσα από τις ακόλουθες διαδρομές:
Internet Explorer:
• IE8-9 %USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
• IE10-11 %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Άλλα εργαλεία που μπορούμε να χρησιμοποιήσουμε είναι και τα **IECacheView, IECookiesView και IEHistoryView.** Οι εντολές που δίνουμε είναι:
c:\> **IECacheView.exe /stext IECacheView.txt**
c:**> IECookiesView.exe**
c:**> IEHistoryView.exe /stext IEHistoryView.txt**

Στην περίπτωση του Google Chrome, χρησιμοποιούμε το εργαλείο forecopy_handy και δίνουμε την εντολή:

c:**> forecopy_handy.exe -c chrome_dir**

Μπορούμε επίσης να αντιγράψουμε τα δεδομένα που χρειαζόμαστε μέσα από τις ακόλουθες διαδρομές:
chrome:
• Win7/8/10 %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default

Μπορούμε να αντιγράψουμε τα σχετικά αρχεία με τις ακόλουθες εντολές:

Στα Windows XP
copy "%UserProfile%\Local Settings\Application Data\Chrome\User Data\Default\Web Data" WebData

Στα Windows 7/8/10
copy "%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Web Data" WebData

Τα παραπάνω αρχεία αποτελούν μία βάση δεδομένων σε μορφή SQLITE που μπορούμε να δούμε μέσω διαφορετικών εργαλείων, όπως το SQLite Database Browser. Στον ίδιο κατάλογο, είναι δυνατό να εντοπίσουμε διάφορα

αρχεία που αποθηκεύουν πληροφορίες, χρήσιμες για τον ερευνητή, τις οποίες και μπορούμε να αντιγράψουμε και να αναλύσουμε στην συνέχεια.

Στην περίπτωση του Mozilla Firefox, χρησιμοποιούμε το εργαλείο forecopy_handy και δίνουμε την εντολή:

c:\> **forecopy_handy.exe -x Firefox_dir**

Μπορούμε επίσης να αντιγράψουμε τα δεδομένα που χρειαζόμαστε μέσα από τις ακόλουθες διαδρομές:

Firefox:
• v3-25 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default
• v26+ %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default

Παράδειγμα στον Firefox μπορούμε να αντιγράψουμε το αρχείο *formhistory.sqlite* μέσω της παρακάτω εντολής:

Στα Windows XP
copy "%UserProfile%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<random>.default*formhistory.sqlite*" *formhistory.sqlite*

Στα Windows 7/8/10
copy "%UserProfile\AppData\Roaming\Mozilla\Firefox\Profiles\<random>.default*formhistory.sqlite*" *formhistory.sqlite*

Η τιμή <*random*> είναι το τυχαίο όνομα που δόθηκε από τον Firefox στο φάκελο του χρήστη. Για να το γνωρίζουμε εκ των προτέρων, είναι απαραίτητο να κάνουμε μια λίστα του περιεχομένου στον κατάλογο (directory) *Profiles*. Όπως ακριβώς στα άλλα προγράμματα περιήγησης, στη διαδρομή (route) του προφίλ του χρήστη αποθηκεύονται όλα τα είδη των πληροφοριών.

Ιστορικό αναζήτησης στο Διαδίκτυο

Το ιστορικό αναζήτησης στο Διαδίκτυο αποτελεί σημαντική πληροφορία σε ορισμένα περιστατικά, κυρίως εκείνα που σχετίζονται με κάποιο είδος μόλυνσης από ιομορφικό λογισμικό που προκλήθηκε από την περιήγηση σε μολυσμένες ιστοσελίδες. Τον τελευταίο καιρό, οι δημιουργοί ιομορφικού λογισμικού έχουν εντείνει την εκμετάλλευση των τρωτοτήτων στα προγράμματα περιήγησης (και στα προγράμματα που καλούνται μέσω αυτών), στις τεχνολογίες που αναπτύσσουν ιστοσελίδες ή στους διακομιστές (servers), για να μολύνουν όσο το δυνατόν περισσότερους χρήστες. Γι' αυτό σε πολλές περιπτώσεις επιβάλλεται να ανακτήσουμε πληροφορίες σχετικά με το ιστορικό αναζήτησης, για να είμαστε σε θέση να εντοπίσουμε τη δραστηριότητα του χρήστη στο διαδίκτυο.

Λόγω της ευκολίας του, δεδομένου ότι υποστηρίζει κύρια προγράμματα περιήγησης (Internet Explorer, Mozilla Firefox, Google Chrome και Safari) και τις διάφορες εκδόσεις τους, συνιστάται να χρησιμοποιούμε εργαλεία όπως το **BrowsingHistoryView**. Η εντολή που δίνουμε είναι:
c:\> **BrowsingHistoryView /HistorySource 2 /LoadIE 1 /LoadFirefox 1 /LoadChrome 1 /LoadSafari1 /stext BrowsingHistoryView.txt**

Άλλα εργαλεία

Browser History Spy	http://securityxploded.com/browser-history-spy.php
IEHistoryView	http://www.nirsoft.net/utils/iehv.html
MozillaHistoryView	http://www.nirsoft.net/utils/mozilla_history_view.html
ChromeHistoryView	http://www.nirsoft.net/utils/chrome_history_view.html
Pasco	http://www.mcafee.com/es/downloads/free-tools/pasco.aspx
Mandiant Redline	https://www.mandiant.com/resources/download/redline

Τελευταίες αναζητήσεις

Για να καταγράψουμε όλες τις τελευταίες αναζητήσεις στους φυλλομετρητές, μπορούμε να χρησιμοποιήσουμε το πρόγραμμα **MyLastSearch** και δίνουμε την εντολή:

c:\> **MyLastSearch /stext MyLastSearch.txt**

Cookies

Τα cookies είναι μικρά αρχεία κειμένου που επιτρέπουν, μεταξύ άλλων, να διατηρείται ανοικτή μια σύνοδος (session) σε μια ιστοσελίδα, να παρακολουθείται, να αποθηκεύονται οι προτιμήσεις, κλπ. Γενικά τα cookies είναι σημαντικά στην ανάλυση για τον καθορισμό του τρόπου χρήσης του διαδικτύου. Τα Cookies είναι μικρά text αρχεία (<4KB), τα οποία μπορούν να δώσουν στον ερευνητή τις πληροφορίες, όπως:

- Σε ποια ιστοσελίδα αναφέρονται, εφαρμόζονται
- Πληροφορίες για τον τοπικό λογαριασμό χρήστη (Local user account)
- MAC times για το αρχείο cookie
- Και ότι άλλο δεδομένο περιλαμβάνουν σχετικά με την ιστοσελίδα.

Αποθηκεύονται μόνο τα persistent cookies. Πολύ δύσκολο να αποκρυπτογραφήσουμε τα cookies.

Υπάρχουν διάφορα εργαλεία που μπορούν να χρησιμοποιηθούν ανάλογα με το πρόγραμμα περιήγησης (browser), για να δούμε τα cookies με ένα απλούστερο τρόπο. Από όλα αυτά ξεχωρίζουν τα **ChromeCookiesView**, **MozillaCookiesView** και **IECookiesView**. Αυτά λειτουργούν με παρόμοιο τρόπο.

Άλλα εργαλεία

Galleta	http://www.mcafee.com/es/downloads/free-tools/galleta.aspx
Mandiant Redline	https://www.mandiant.com/resources/download/redline

ΤΜΗΜΑ 20
ΣΥΛΛΟΓΗ ΣΤΑΤΙΚΩΝ – ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (NON VOLATILE INFORMATION)

Μόλις συλλεχθούν οι πληροφορίες που μεταβάλλονται (πτητικές), είτε σε συνάρτηση με το χρόνο, είτε με την ενέργεια του χρήστη, είτε με την εκκίνηση του υπολογιστή, επόμενο βήμα είναι να συλλεχθούν οι πληροφορίες που δεν μεταβάλλονται, αλλά είναι αποθηκευμένες και μπορούν να ληφθούν ενώ ο υπολογιστής είναι εκτός λειτουργίας. Στα αποθηκευτικά μέσα (όπως σκληρός δίσκος), ο ερευνητής μπορεί να εντοπίσει πολλά και ενδιαφέροντα αποδεικτικά στοιχεία. Συνεπώς είναι σημαντική ενέργεια η δημιουργία αντιγράφου όλων των αποθηκευτικών μέσων που υπάρχουν στο υπό εξέταση σύστημα.

Όταν ερευνούμε μία συγκεκριμένη υπόθεση, ο ερευνητής θα βρεθεί σε μία από τις δύο καταστάσεις:

- Ο υπολογιστής βρίσκεται σε λειτουργία, με:
  - τα αποθηκευτικά μέσα να **μην είναι** κρυπτογραφημένα.
  - τα αποθηκευτικά μέσα να **είναι** κρυπτογραφημένα.
- Ο υπολογιστής δεν βρίσκεται σε λειτουργία.

Όταν ο υπολογιστής δεν βρίσκεται σε λειτουργία, απλά ο ερευνητής αντιγράφει τα αποθηκευτικά μέσα, δημιουργεί αντίγραφα και εργάζεται πάνω σε αυτά.

Όταν ο υπολογιστής βρίσκεται σε λειτουργία, ο ερευνητής συλλέγει τα μεταβαλλόμενα δεδομένα και στην συνέχεια εξετάζει αν τα αποθηκευτικά μέσα είναι κρυπτογραφημένα. Εάν δεν είναι κρυπτογραφημένα, σταματά την λειτουργία του υπολογιστή, αντιγράφει τα αποθηκευτικά μέσα, δημιουργεί αντίγραφα και εργάζεται πάνω σε αυτά.

Εάν τα αποθηκευτικά μέσα (σκληρός δίσκος) είναι κρυπτογραφημένα, τότε δεν σταματά την λειτουργία του υπολογιστή και κάνει αντιγραφή του σκληρού (λογικό αντίγραφο) ενώ ο υπολογιστής είναι σε λειτουργία και στην συνέχεια δημιουργεί αντίγραφα και εργάζεται πάνω σε αυτά.

Συνεπώς μπορούμε να αντιγράψουμε τα αποθηκευτικά μέσα με τρεις τρόπους:

- **Φυσικό αντίγραφο**
  - Πρόκειται για αντιγραφή bit to bit ενός σκληρού δίσκου, ενώ ο υπολογιστής είναι εκτός λειτουργίας.
- **Λογικό αντίγραφο**
  - Πρόκειται για αντιγραφή ενός σκληρού ενώ είναι σε λειτουργία ο υπολογιστής.
- **Συλλογή συγκεκριμένων - επιλεγμένων δεδομένων**, ανάλογα με την

υπόθεση, στην περίπτωση που ο όγκος των αποθηκευτικών μέσων είναι τεράστιος και δεν μπορούμε να τα αντιγράψουμε.

Αντιγραφή σκληρού δίσκου

Μερικοί παράγοντες που αξίζει να τους έχουμε κατά νου όταν συλλέγουμε τα αποδεικτικά στοιχεία είναι η ταχύτητα της εν λόγω συλλογής και η ακεραιότητά της. Σήμερα, ο όγκος των δίσκων είναι εξαιρετικά τεράστιος και έτσι η διαδικασία θα μπορούσε να είναι δαπανηρή από άποψη χρόνου και πόρων. Είναι απαραίτητο να έχουμε μια σαφή ιδέα του τι είδους αντιγραφή, πρέπει να διενεργηθεί, η οποία μπορεί να ταξινομηθεί σε τρεις τύπους:

1. Δημιουργία ενός αντιγράφου του δίσκου (bit to bit copy) και το αποθηκεύουμε σε μορφή εικονικού δίσκου (image). Με αυτό τον τρόπο δ**ημιουργούμε ένα bit stream αντίγραφο του δίσκου ή του εικονικού δίσκου (image)**: Αυτή είναι η πιο χαρακτηριστική και ταχύτερη μέθοδος. Εκτός αυτού, επιτρέπει επίσης να κάνουμε τόσα αντίγραφα όσα χρειάζονται με ένα γρήγορο και απλό τρόπο για τη φάση της ανάλυσης. Για να δημιουργήσουμε ένα bit stream αντίγραφο του δίσκου ή του image, το **FTK Imager** είναι μια καλή επιλογή (έκδοση γραμμής εντολών -command-line). Η Εντολή που χρειάζεται αν δώσουμε είναι:
c:\> **ftkimager.exe \\. \\PHYSICALDRIVE0** G:\HDImage.raw **--verify**

Παράδειγμα:
Η πρώτη εντολή που δίνουμε είναι:
c:\> **ftkimager.exe -list-drives**

Το αποτέλεσμα της εντολής θα είναι μία λίστα με τους δίσκους (φυσικούς/λογικούς) του συστήματος. Για να δημιουργήσουμε ένα αντίγραφό ενός σκληρού δίσκου ο οποίος εμφανίζεται ως \\.\PHYSICALDRIVE0 σε μορφή E01 ονομαζόμενο ως HDImage στο Drive X:\ και να το κρυπτογραφήσουμε με το συνθηματικό pass123, δίνουμε την εντολή:
c:\> ftkimager \\.\PHYSICALDRIVE0 "X:\HDImage.e01" --e01 --outpass pass123

Πολύ σημαντική ενέργεια, πριν χρησιμοποιήσουμε έναν δικό μας σκληρό δίσκο για να αποθηκεύσουμε τα αντίγραφα του υπό εξέταση σκληρού δίσκου είναι και ο καθαρισμός (Wipe) του δικού μας σκληρού δίσκου.
Έστω ο σκληρός δίσκος που θέλουμε να κάνουμε wipe βρίσκεται στην θέση F:, τότε στα Windows δίνουμε την εντολή:
SDelete /c /z F:\

Σε ένα Linux σύστημα ο υπολογιστής συνδέει (mounts) τις συσκευές στο /dev, συνεπώς το:
/dev/sda αναφέρεται στην πρώτη συνδεδεμένη συσκευή (δίσκος), ενώ το
/dev/sdb αναφέρεται στην δεύτερη συνδεδεμένη συσκευή (δίσκος)
Κάθε partition ενός σκληρού έχει την δικιά του εγγραφή.
/dev/sda1 αναφέρεται στο πρώτο partition της συνδεδεμένης συσκευής /dev/sda
/dev/sda2 αναφέρεται στο δεύτερο partition της συνδεδεμένης συσκευής /dev/sda

Σε windows περιβάλλον, ένα εργαλείο που μπορούμε αν χρησιμοποιήσουμε, από γραμμή εντολών για την δημιουργία αντιγράφου, bit to bit low level, είναι και το dd.exe. Η εντολή που δίνουμε είναι:
c:**> dd.exe if=\\.\PhysicalDrive0 of=d:\images\PhysicalDrive0.img --md5sum --verifymd5 --md5out=d:\images\PhysicalDrive0.img.md5**

Έστω ότι ο σκληρός που θέλουμε να κάνουμε wipe είναι ο /dev/sda, για να τον καθαρίσουμε δίνουμε τις εντολές, σε linux περιβάλλον:
dd if=/dev/zero of=/dev/sda bs=1M
dd if=/dev/urandom of=/dev/sda bs=1M

Για να δημιουργήσουμε ένα φυσικό αντίγραφο ενός δίσκου που έχουμε αποσπάσει από το υπό εξέταση σύστημα και τον έχουμε συνδέσει ως **read only**, σε ένα linux, μπορούμε να χρησιμοποιήσουμε διάφορα εργαλεία (**dd, dc3dd, dcfldd, ddrescue)** και οι εντολές τους είναι:

 # dd if=/dev/sda of=HDimage.img bs=4k conv=noerror,sync
 # dc3dd if=/dev/sda of=HDimage.img verb=on hash=md5 hash=sha256 hlog=dc3dd_result.hashlog log=dc3dd_result.log

 # dcfldd if=/dev/sda hash=md5,sha256 hashwindow=10G md5log=md5.txt sha256log=sha256.txt hashconv=after bs=512 conv=noerror,sync split=10G splitformat=aa of=HDimage.dd

 # ddrescue -d -r3 /dev/sda HDImage.img sda.logfile

Άλλα εργαλεία

Ftkimager (GUI)	http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.3
WinDD	http://sourceforge.net/projects/windd/
Clonezilla	http://clonezilla.org
OSFClone	http://www.osforensics.com/tools/create-disk-images.html

2. Δημιουργία ενός ένα bit stream αντίγραφο από δίσκο σε δίσκο: Είναι η μέθοδος που χρησιμοποιείται όταν δεν είναι δυνατό να κάνουμε ένα bit stream αντίγραφο από ένα δίσκο σε ένα image.

Με τον ίδιο τρόπο, όπως στην προηγούμενη μέθοδο, μπορούμε να κάνουμε τόσα αντίγραφα όσα και οι δίσκοι. Η κλωνοποίηση μέσω μιας συσκευής hardware συνεπάγεται μεγαλύτερη αξιοπιστία και ταχύτητα. Ωστόσο, όπως αναφέρθηκε προηγουμένως, σε αυτόν τον οδηγό έχουμε επιλέξει τη χρήση ελεύθερου λογισμικού με σκοπό να μειώσουμε το κόστος συλλογής πληροφοριών στο ελάχιστο.

Άλλα εργαλεία

DC3DD	http://sourceforge.net/projects/dc3dd/
OSFClone	http://www.osforensics.com/tools/create-disk-images.html
dd	Διατίθεται σε διανομές Linux
FOG	http://sourceforge.net/projects/freeghost/
AIR - Automated Image and Restore	http://sourceforge.net/projects/air-imager/

Σημείωση

Για τη δημιουργία ενός bit stream αντιγράφου από δίσκο σε image ή από δίσκο σε δίσκο, σε SSDs σκληρούς θα πρέπει να γνωρίζουμε τα παρακάτω:

Οι SSDs δεν λειτουργούν κατά τον ίδιο τρόπο όπως οι μαγνητικοί δίσκοι. Διαθέτουν δύο επιπλέον λειτουργίες για να προφυλαχτεί ο SSD και να έχει μεγαλύτερη διάρκεια ζωής. Σκοπός των λειτουργιών είναι να προστατέψουν όλη την επιφάνεια του σκληρού να έχει τον ίδιο αριθμό εγγραφών. Οι SSD έχουν περιορισμένο αριθμό εγγραφών. Οι λειτουργίες είναι:

- Wear leveling:

Πρόκειται για μία μεθοδολογία προστασίας του SSD για να διαρκέσει περισσότερο. Κατανέμει την εγγραφή και διαγραφή δεδομένων ομοιόμορφα σε όλο τον σκληρό.

- Trim:

Λειτουργία καθαρισμού των σημειωμένων για διαγραφή σελίδων (pages)

Οι κατασκευαστές εφάρμοσαν την λειτουργία TRIM που παρατείνει τη διάρκεια ζωής ενός SSD και εμποδίζει την υποβάθμιση της επίδοσης. Αυτή η εντολή ενημερώνει τον controller ποια cells δεν είναι πλέον σε χρήση, η οποία ομοίως, ειδοποιεί τον garbage controller πως θα πρέπει να διαγράψει ηλεκτρονικά το περιεχόμενο αυτών των cells και να τα προετοιμάσει για μελλοντικές λειτουργίες εγγραφής. Είναι πολύ σημαντικό να έχουμε μια σαφή ιδέα, ότι δεν είναι δυνατόν να αποφευχθεί η διαδικασία garbage collection όταν η εντολή TRIM είναι ενεργοποιημένη, ούτε καν με την αλλαγή του δίσκου SSD σε ένα άλλο σύστημα ή με την τοποθέτηση ενός write blocker, δεδομένου ότι ένας δίσκος SSD, απλώς έχοντας τροφοδοτηθεί με ρεύμα, θα ξεκινήσει αυτόματα την προαναφερθείσα διαδικασία.

Αυτό σημαίνει ότι εάν ένας χρήστης διαγράψει ένα αρχείο και η εντολή TRIM είναι ενεργοποιημένη, τα αποδεικτικά στοιχεία θα εξαφανιστούν για πάντα. Το γεγονός αυτό δεν επηρεάζει τους κρυπτογραφημένους δίσκους (volumes) όπως το Veracrypt, TrueCrypt, το BitLocker, κλπ., πράγμα που σημαίνει ότι πρέπει να συλλεχθούν για μεταγενέστερη ανάλυση.

Επίσης θα πρέπει να σημειωθεί ότι το γεγονός αυτό επηρεάζει και την προσπάθεια να εξάγουμε το hash από έναν δίσκο SDD, ο οποίος μπορεί να είναι

διαφορετικός, δεδομένου ότι η διαδικασία που ξεκινά την εντολή TRIM λειτουργεί στο παρασκήνιο και παρά το γεγονός ότι αυτός ο δίσκος δεν έχει προφανώς υποστεί τυχόν τροποποιήσεις, έχει στην πραγματικότητα υποστεί αλλαγές.

3. Δημιουργία αντιγράφου δεδομένων, σχετικών με την υπόθεση που ανήκουν σε ένα φάκελο ή αρχείο: με άλλα λόγια, διεξαγωγή ενός επιλεκτικού αντιγράφου, δεδομένου ότι σε πολλές περιπτώσεις, ανάλογα με τον τύπο του περιστατικού, μπορεί να είναι απαραίτητο ή όχι να κάνουμε αντίγραφο όλου του δίσκου και μπορεί να είναι αρκετό απλά να αντιγράψουμε ορισμένους φακέλους ή αρχεία.

Για να το κάνουμε αυτό, χρησιμοποιούμε εργαλεία όπως το **TeraCopy, Robocopy**. Ένα παράδειγμα της χρήσης του είναι το ακόλουθο:
c:\> **TeraCopy.exe Copy "D:\My Documents"** F:\Evidence
C:\>Robocopy C:\Documents\ F:\Evidence

Με το εργαλείο **TeraCopy**, είναι δυνατόν να ελεγχθεί εάν η διαδικασία αντιγραφής έχει πραγματοποιηθεί σωστά, δεδομένου ότι υπολογίζει τα hashes των αρχείων και των αντίστοιχων αντιγράφων τους και τα συγκρίνει.

Άλλα εργαλεία

Robocopy	http://technet.microsoft.com/es-es/library/cc733145(v=ws.10).aspx
Copy	Διατίθεται σε λειτουργικά συστήματα Windows.
Xcopy	Διατίθεται σε λειτουργικά συστήματα Windows.
ForensicCopy	http://sandersonforensics.com/forum/content.php?121-ForensicCopy

Σημαντικό

Στις τρεις περιπτώσεις που περιγράφονται, ανεξάρτητα από το ποια θα εφαρμόσουμε, είναι υποχρεωτικό να εργαστούμε κατά τη διάρκεια της ανάλυσης με αντίγραφα των σκληρών δίσκων και όχι με τους αυθεντικούς. Με αυτό τον τρόπο πετυχαίνουμε να διατηρούμε τις αρχικές πληροφορίες ανέπαφες και την ακεραιότητά τους σταθερή σε οποιαδήποτε στιγμή. **5.4 Συλλογή στατικών – αποθηκευμένων πληροφοριών**

Αντίγραφο του Master Boot Record (MBR)

Το MBR (Master Boot Record), είναι ένα πρόγραμμα, πού βρίσκεται στο πρώτο τμήμα του σκληρού δίσκου (Cylinder 0, Head 0, Sector 0) και καταλαμβάνει 512 bytes. Εκτελείται κατά την εκκίνηση τού υπολογιστή, πριν φορτωθεί το λειτουργικό. Το MBR, διατηρεί και το DPT (Disk Partition Table), το οποίο μπορεί να "δεχτεί" 4 πρωτεύοντα διαμερίσματα (primary partitions) και να ξεκινήσει το λειτουργικό σύστημα. Το MBR συλλέγει και πληροφορίες για τα διαμερίσματα τού σκληρού δίσκου μας. Αποθηκεύει πληροφορίες σε σχέση με το πώς να ξεκινήσει το λειτουργικό σύστημα, τι είδους κατατμήσεις (partitions) υπάρχουν στη συσκευή

και το μέγεθός τους, κλπ. Αν το MBR έχει υποστεί βλάβη, δεν θα φορτωθεί και το λειτουργικό μας.

Σε ορισμένα περιστατικά, κυρίως εκείνα που σχετίζονται με ιομορφικό λογισμικό, μπορεί να παρουσιάζει ενδιαφέρον να το εξάγουμε για μεταγενέστερη ανάλυση για να προσδιορίσουμε αν είναι μολυσμένο.

Για να γίνει αυτό, συνιστάται να χρησιμοποιούμε εργαλεία όπως το **MBRbackup ή mbrfix**, τα οποία επιτρέπουν την εξαγωγή του MBR εκτελώντας τις ακόλουθες εντολές:
c:**> mbrbackup.exe**
c:**> MbrFix /drive 0 listpartitions**
c:**> MbrFix /drive 0 savembr Backup_MBR_0.bin**

Επίσης μπορούμε να πάρουμε αντίγραφο του MBR με την χρήση εργαλείων όπως το DC3DD και dd. Παράδειγμα:
c:**> dd if=\\.\PhysicalDrive0 of=MBR.bin bs=512 count=1**

Αντίγραφο του Volume Boot Record (VBR)

Το VBR (Volume Boot Record), είναι ο πρώτος τομέας ενός διαμερίσματος (σε αντίθεση με MBR που είναι ο πρώτος τομέας του σκληρού δίσκου). Το VBR (ακριβώς όπως και το MBR) περιέχει επίσης κάποιο κώδικα και δεδομένα, αλλά είναι πολύ λιγότερο τυπικό, όσο αφορά την χρήση του, δεν είναι απαραίτητο.

Σε ορισμένα περιστατικά, κυρίως εκείνα που σχετίζονται με ιομορφικό λογισμικό, μπορεί να παρουσιάζει ενδιαφέρον να το εξάγουμε για μεταγενέστερη ανάλυση για να προσδιορίσουμε αν είναι μολυσμένο.

Για να γίνει αυτό, συνιστάται να χρησιμοποιούμε εργαλεία όπως το forecopy_handy **MBRbackup ή mbrfix**, το οποίο επιτρέπει την εξαγωγή του VBR εκτελώντας την εντολή:
c:**> forecopy_handy -f %SystemDrive%\$Boot vbr**

Αντιγραφή του MFT (Master File Table) για offline ανάλυση.

Ο Master File Table είναι ένας πίνακας που αποθηκεύει σχετικές πληροφορίες από όλα τα αρχεία και τους φακέλους μιας ενότητας (unity) ή δίσκου. Περιλαμβάνει, μεταξύ άλλων, πληροφορίες όπως το όνομα, το μέγεθος, την ημερομηνία, την ώρα, ή τις άδειες (permits), συμπεριλαμβανομένων των αρχείων που έχουν εξαλειφθεί έως τη στιγμή κατά την οποία ο χώρος αυτός καθίσταται αναγκαίος και ξαναγράφεται (overwritten). Το MFT είναι ένα αρχείο μετα-δεδομένων, που περιέχει περιγραφές άλλων αρχείων μετα-δεδομένων, και σε μερικές περιπτώσεις ολόκληρα αρχεία μετα-δεδομένων! Το MFT είναι ίσως η πιο σημαντική δομή του NTFS, καθώς είναι το μέρος που αποθηκεύεται κάθε πληροφορία για κάθε κατάλογο και κάθε αρχείο.

Για την εξαγωγή του Master File Table, μπορούν να χρησιμοποιηθούν εργαλεία όπως το Ntfswalk, ntfscopy, rawcopy, forecopy_handy

Για να ανακτήσουμε το Master File Table , πληκτρολογούμε μία από τις ακόλουθες εντολές:
c:\> **ntfscopy.exe -raw c:\$MFT c:\MFT**
c:**> rawcopy.exe c:0 c:\MFTraw**
c:**> forecopy_handy –m**

Άλλα εργαλεία

rawcopy	https://github.com/jschicht/RawCopy
ntfscopy	https://tzworks.net/prototype_page.php?proto_id=9
ntfswalk	https://www.tzworks.net/prototype_page.php?proto_id=12
analyzeMFT	https://github.com/dkovar/analyzeMFT

Εκτυπωμένα αρχεία (Printed files)

Είναι δυνατόν να ανακτήσουμε τα αρχεία που έχουν σταλεί για εκτύπωση, εάν έχει οριστεί η επιλογή του εκτυπωτή «*conserve documents after printing*». Σε αυτή την περίπτωση τα Windows δημιουργούν ενδιάμεσα αρχεία αποθήκευσης με κατάληξη (extension) *.SPL (metadata: owner, printing method, κλπ) και *.SHD (data to be printed), στο αρχείο, %WinDir%\system32\spool\printers, κάθε φορά που ένα έγγραφο αποστέλλεται για εκτύπωση. Μόλις οριστικοποιηθεί η διαδικασία εκτύπωσης, αυτά τα αρχεία διαγράφονται, εκτός αν έχει επιλεγεί να διατηρούνται. Συνεπώς στην διαδρομή %WinDir%\system32\spool\printers, μπορούμε να εντοπίσουμε τα αρχεία που έχουν σταλεί για εκτύπωση. Εντολές:
c:**> robocopy %WinDir%\system32\spool\printers*.SPL** F:\spl_files
c:**> robocopy %WinDir%\system32\spool\printers*.SHD F:\shd_files**

Μεταβλητές στις ρυθμίσεις (Variables in the settings)

Για να γνωρίζουμε όλες τις μεταβλητές στις ρυθμίσεις, με άλλα λόγια, αυτές που είναι στη διαδρομή (path), εκτελούμε την ακόλουθη εντολή:
c:**>path >path.txt**

Σημείωση
Το path είναι μία μεταβλητή περιβάλλοντος, όπου αποθηκεύονται οι διαδρομές των εκτελέσιμων αρχείων.

Αρχεία καταγραφής του συστήματος (System logs)

Τα αρχεία καταγραφής (logs) είναι αρχεία κειμένου που αποθηκεύουν σχετικές πληροφορίες, όπως απομακρυσμένες συνδέσεις, συμβάντα του συστήματος, κλπ. Υπάρχουν αρκετά αρχεία καταγραφής που έχουν μεγάλο εγκληματολογικό ενδιαφέρον και που πρέπει να συγκεντρωθούν.

Αρχεία καταγραφής συμβάντων των Windows

Τα MS Windows 2000, XP και 2003 τυπικά συντηρούν - έχουν τρία Event

Log files: Application, System, and Security:

- *AppEvent.evt(x)*: Καταχωρεί συμβάντα που σχετίζονται με τις εφαρμογές.
- *SysEvent.evt(x)*: Καταχωρεί συμβάντα που σχετίζονται με το σύστημα.
- *SecEvent.evt(x)*: Καταχωρεί συμβάντα που σχετίζονται με την ασφάλεια.

Τα βρίσκουμε στο μονοπάτι: **C:\Windows\system32\config** και μπορούν να εξαχθούν χρησιμοποιώντας προγράμματα όπως το **psloglist. Εντολές:**
c:\> **psloglist /accepteula -s -t , Apllication > ApllicationEventListing.txt**
c:\> **PsLoglist /accepteula -s -t , Security > SecurityEventListing.txt**
c:\> **PsLoglist /accepteula -s -t , System > SystemEventListing.txt**

Οι Server εκδόσεις των λειτουργικών συστημάτων διαθέτουν επιπλέον Event Logs (DNS Server.evt, Directory Service.evt, File Replication Service.evt) που εξαρτάται από την χρήση του server.

Θα πρέπει να σημειωθεί πως τα Vista, Windows 2008, Windows 7/8/10 χρησιμοποιούν διαφορετικό Windows Event Log format. Κάθε log file αποτελείται από την επικεφαλίδα (Header) και το σώμα (Body). Το σώμα (body) περιέχει Event records, την Cursor record και μη χρησιμοποιήσιμο χώρο (unused space).
Μορφή Windows XML Event Log (EVTX). Η Windows XML Event Log (EVTX) μορφή πρωτοεμφανίστηκε στα Windows Vista ως αντικατάσταση της Windows Event Log (EVT) αρχείων. Τα εντοπίζουμε στην διαδρομή: **C:\Windows\system32\winevt\logs\.**

Κάνοντας χρήση του "Event Viewer" (eventvwr.msc) ή του "Windows Events Command Line Utility" (wevtutil.exe), μπορούμε να διαχειριστούμε τα event log files. Ο Event Viewer μπορεί να παρουσιάσει τα log EVTX files και στην μορφή "general view" (ή αλλιώς formatted view) και σε αναλυτική μορφή "details view" (η οποία περιέχει και "friendly view" και "XML view"). Επιλέγουμε την αναλυτική μορφή για να αποκαλύψουμε το σύνολο των πληροφοριών.

Εάν εξάγουμε τα event logs από τον Event Viewer μπορεί να εξαχθεί και επιπλέον πληροφορία. Αυτή η πληροφορία αποθηκεύεται στο:
LocaleMetaData\%FILENAME%_%LCID%.MTA

Για να εξάγουμε τα log files, μπορούμε να χρησιμοποιήσουμε το **psloglist ε**ργαλείο. Μπορούμε ωστόσο να χρησιμοποιήσουμε και το **"Windows Events Command Line Utility" (wevtutil.exe),** δίνοντας τις ακόλουθες εντολές**:**

c:\> wevtutil epl Apllication ApllicationEventListing.txt
c:\> wevtutil epl Security SecurityEventListing.txt
c:\> wevtutil epl System SystemEventListing.txt

Μέσω του wevtutil εργαλείου μπορούμε να εξάγουμε το σύνολο των event logs και να συγκεντρώσουμε έναν μεγάλο όγκο πληροφοριών. Η εντολή που

δίνουμε είναι:
c:\> **wevtutil el**

Άλλα εργαλεία

MyEventViewer	http://www.nirsoft.net/utils/my_event_viewer.html

WindowsUpdate.log

Το αρχείο ***WindowsUpdate.log***, που βρίσκεται στο φάκελο %WinDir%, αποθηκεύει μια λίστα αναβαθμίσεων που αντιστοιχούν στο λειτουργικό σύστημα που έλαβαν χώρα στο σύστημα. Μπορούμε να το αντιγράψουμε και να συλλέξουμε αρκετές πληροφορίες που μπορεί να είναι χρήσιμες, ειδικά στην περίπτωση παραβίασης του συστήματος. Παράδειγμα, κάποιος κακόβουλος χρήστης εκμεταλλεύτηκε συγκεκριμένη αδυναμία να πάρει πρόσβαση και στην συνέχεια ενημερώνοντας τον υπολογιστή (update), αποκατάστησε το πρόβλημα (αδυναμία).
Εντολή:
c:\robocopy **c:\windows\WindowsUpdate.log WindowsUpdate.log**

pfirewall.log

Το αρχείο *pfirewall.log*, που βρίσκεται στο φάκελο %WinDir% (Windows XP) και στο %WinDir%\System32\LogFiles\Firewall (Windows 7/8/10), αποθηκεύει διαφορετικές πληροφορίες που αντιστοιχούν στο τείχος προστασίας των Windows. Πληροφορίες που μπορούμε να συλλέξουμε περιλαμβάνουν, συνδέσεις στο διαδίκτυο, κανόνες του firewall (αν έχει δημιουργηθεί κάποιος νέος), χαμένα πακέτα, δυσλειτουργία κάποιας εφαρμογής λόγου firewall, απόπειρες brute forcing και γενικά μπορούμε να εντοπίσουμε τυχόν κακόβουλη δραστηριότητα. Μπορούμε να αντιγράψουμε τα συγκεκριμένα αρχεία με την εντολή:
c:\robocopy **c:\windows\ *pfirewall.log* *pfirewall.log***
c:\robocopy **c:\windows\System32\LogFiles\Firewall*pfirewall.log* *pfirewall.log***

Powershell logs

Τα windows έχουν βελτιώσει τα μητρώα καταγραφής συμβάντων (log files) που αφορούν το powershell, ειδικότερα από την έκδοση 5. Για να δούμε ποια είναι τα log files ου καταγράφουν το powershell δίνουμε την εντολή:
C:\>wevtutil.exe el | findstr /I "powershell"

Για να εξάγουμε τα powershell logs δίνουμε την εντολή:
c:\> **wevtutil.exe epl "Windows PowerShell" powershell-logs.txt**

Άλλα αρχεία καταγραφής

Υπάρχουν και άλλα αρχεία καταγραφής συμβάντων (log files) που μπορεί να είναι αποθηκευμένα στο υπό έλεγχο σύστημα ή σε άλλα συστήματα στο δίκτυο και μπορεί να μας δώσουν τις πληροφορίες που αναζητάμε ως ερευνητές. Ως

ερευνητές οφείλουμε να γνωρίζουμε την ύπαρξή τους και να τα ανακτούμε εάν συμβάλλουν στην επίλυση της υπόθεσης. Κάποια από αυτά καταγράφουν πληροφορίες που αφορούν:

- Web servers, όπως Internet Information Server (IIS), Apache, κλπ.
- Εργαλεία απομακρυσμένης πρόσβασης, όπως WinVNC, pcAnywhere, κλπ.
- FTP clients, όπως Filezilla, WinSCP, κλπ.
- Τείχη προστασίας (Firewalls) ή συστήματα ανίχνευσης εισβολών (IDS).
- Πληροφορίες DHCP.
- Πληροφορίες προγραμμάτων ανταλλαγής μηνυμάτων, όπως Skype.
- Πληροφορίες συγχρονισμού Dropbox (.dbx).
- Πληροφορίες DNS

Για να αντιγράψουμε το ιστορικό του skype, δίνουμε την εντολή:
Στα windows XP
c:\> **copy /V C:\Documents and Settings\<username>\Application\Skype\<skype-name>* G:\Skype_backup_dir**

Στα Windows 7/8/10
c:\> **copy /V C:\%USERPROFILE%\AppData\Roaming\Skype\<skype-name>* G:\Skype_backup_dir**

Jump Lists

Στα Windows, η γραμμή εργασιών (task bar) δίνει την δυνατότητα στον χρήστη να μεταπηδά (Jump List) ή να έχει πρόσβαση σε δεδομένα/εφαρμογές που χρησιμοποίησε πρόσφατα ή χρησιμοποιεί συχνά. Δεν περιλαμβάνει μόνο αρχεία ήχου και εικόνας αλλά και πρόσφατες εργασίες. Οι πληροφορίες αποθηκεύονται στον φάκελο με τίτλο AutomaticDestinations, μέσα στον οποίο υπάρχει ένα μοναδικό αρχείο στο οποίο επισυνάπτεται το χαρακτηριστικό της κάθε εφαρμογής (AppID). Η διαδρομή του φακέλου είναι η ακόλουθη:

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Το φάκελο τον αντιγράφουμε με την εντολή:
c:\>robocopy C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations AutomaticDestinations /E

Αρχεία .PST και .OST

Τα αρχεία Personal Storage Table (.pst) είναι μία μορφή αρχείων τα οποία χρησιμοποιούνται για να αποθηκεύουμε αντίγραφα μηνυμάτων, γεγονότων ημερολογίου, καθώς και αρχεία των Microsoft Exchange Client, Windows Messaging, και Microsoft Outlook.

Τα αρχεία offline storage table (.ost), είναι μία μορφή αρχείων του Outlook και χρησιμοποιούνται από τον Microsoft Exchange Server και δίνουν την δυνατότητα στους χρήστες να διαχειρίζονται τα μηνύματά τους ακόμα και όταν η πρόσβαση στον mail server δεν είναι διαθέσιμη.

Οι κύριες διαφορές μεταξύ των δύο αυτών τύπων αρχείων δεδομένων του Outlook είναι ότι:

- Τα αρχεία PST χρησιμοποιούνται για λογαριασμούς POP3, IMAP και για εκείνους που βασίζονται στο Web και που επιτρέπουν να κάνουμε αντίγραφα ασφαλείας (backups) φακέλων του Outlook, συμπεριλαμβανομένων των λογαριασμών του Exchange.

- Τα αρχεία OST χρησιμοποιούνται σε περιπτώσεις όπου ένας λογαριασμός Exchange έχει διαμορφωθεί έτσι ώστε να είναι σε θέση να λειτουργήσει χωρίς σύνδεση στο διαδίκτυο (Internet).

Τα περισσότερα δίκτυα ηλεκτρονικού ταχυδρομείου επιτρέπουν επίσης τη δημιουργία αντιγράφων ασφαλείας (backups) σε μορφή PST. Έτσι, συνιστάται να αντιγράφουμε αυτά τα αρχεία, καθώς σε ορισμένα περιστατικά, μπορεί να είναι ενδιαφέροντα για μεταγενέστερη ανάλυση, δεδομένου ότι μπορεί να περιέχουν μια καταγραφή των συνομιλιών, την ανταλλαγή πληροφοριών, τα ίχνη διαρροών πληροφοριών, κλπ. Από προεπιλογή, στα Windows XP και Windows 7, τα αρχεία είναι αποθηκευμένα στο φάκελο My Documents στο Outlook και στα Windows 8 στο %UserProfile%\AppData\Local\Microsoft\Outlook.

Ανάλογα την έκδοση του outlook τα pst αρχεία εντοπίζονται στις ακόλουθες διαδρομές:
C:\users\username\AppData\Local\Microsoft\Outlook
C:\users\username\Documents\Outlook Files

Εντολή για την αντιγραφή των pst αρχείων:
c:**> COPY %LOCALAPPDATA%\Microsoft\Outlook*.pst G:\backup\PST /y**
c:**> COPY %USERPROFILE%\Local Settings\ApplicationData\Microsoft\Outlook*.pst G:\backup\PST /y**

Κάδος ανακύκλωσης

Ο Κάδος Ανακύκλωσης (Recycle Bin) περιέχει "Ανακυκλωμένα" (Recycled) αρχεία. Η μετακίνηση αρχείων και καταλόγων στον κάδο ανακύκλωσης είναι επίσης γνωστή και ως μαλακή διαγραφή (soft deletion), δεδομένου ότι τα αρχεία δεν αφαιρούνται από το σύστημα αρχείων. Συνεπώς είναι δυνατόν να αποκτηθούν πληροφορίες από τα δεδομένα που έχουν διαγραφεί και έχουν σταλεί στον κάδο ανακύκλωσης. Η διαδρομή του κάδου ανακύκλωσης ανάλογα με το λειτουργικό σύστημα, παρουσιάζεται στον πίνακα που ακολουθεί:

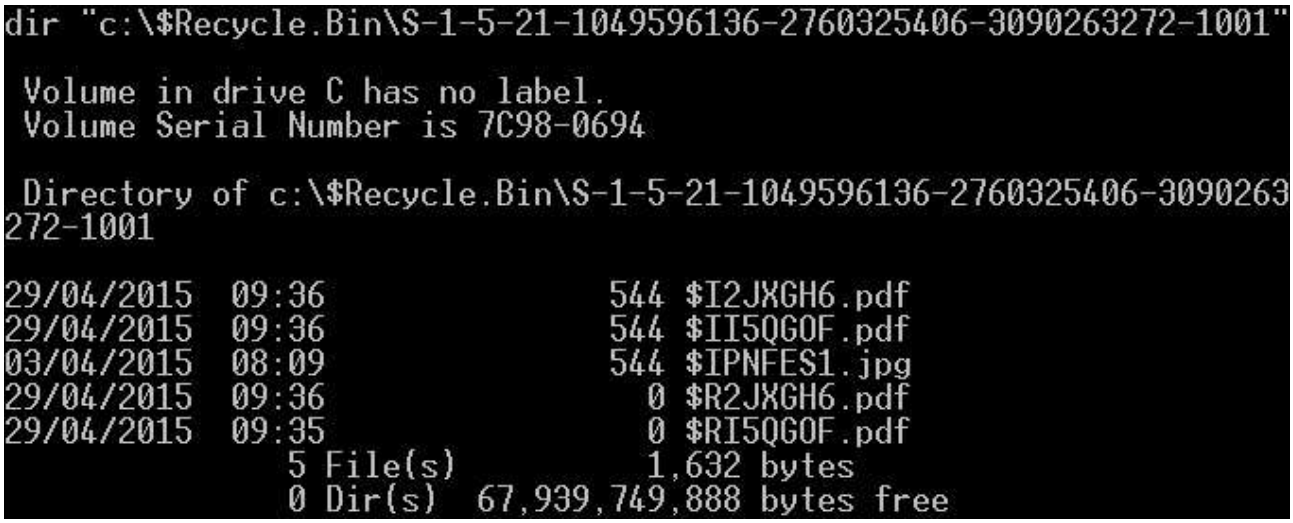
Λειτουργικό σύστημα	**Τοποθεσία**
Windows XP	%SystemDrive%\Recycler\%SID%\

Windows 7/8	%SystemDrive%\$Recycle.Bin\%SID%\

Στις διαδρομές (paths) που υποδεικνύονται, οι φάκελοι αποθηκεύονται με την ακόλουθη μορφή S-1-5-21-299502267-1677128483-839522115-1003, που αντιστοιχεί στο αναγνωριστικό ασφαλείας (SID-Security Identifier) των Windows του χρήστη που το έχει διαγράψει.

Στην περίπτωση των Windows XP, οι φάκελοι αυτοί περιέχουν τα αρχεία που έχουν μετονομαστεί, μαζί με ένα αρχείο με το όνομα INFO2 που αποθηκεύει πληροφορίες που αντιστοιχούν στην ημερομηνία διαγραφής, το μέγεθος και τη διαδρομή όπου ήταν αποθηκευμένο το αρχείο αυτό. Για να αναλύσουμε το αρχείο INFO2, χρησιμοποιούμε το εργαλείο **rifiuti**.

Στην περίπτωση των Windows 7/8/10, στους φακέλους που βρίσκονται στο %SystemDrive%\$Recycle.Bin\ για κάθε αρχείο που διαγράφεται θα υπάρχουν δύο αρχεία με το ίδιο όνομα, εκτός από το δεύτερο γράμμα, όπως μπορεί να παρατηρηθεί στην Εικόνα που ακολουθεί. Το ένα που έχει το γράμμα I ως δεύτερο γράμμα, αποθηκεύει την αρχική διαδρομή του αρχείου που έχει διαγραφεί και το άλλο που έχει το γράμμα R ως δεύτερο γράμμα, αποθηκεύει το ίδιο το αρχείο που έχει διαγραφεί.



Το εργαλείο rifiuti2, μπορεί να αναλύσει τα δεδομένα που βρίσκονται στον κάδο ανακύκλωσης.

Άλλα εργαλεία

rifiuti2	https://github.com/abelcheung/rifiuti2

Αρχείο Hosts (Hosts file)

Η λειτουργία ενός αρχείου hosts είναι η εξής: όταν ένας χρήστης εισάγει μια διεύθυνση URL στο πρόγραμμα περιήγησης, το σύστημα συμβουλεύεται πρώτα τα αρχεία hosts. Αν το αρχείο περιέχει ένα μία αντιστοιχία ανάμεσα στο URL και σε μία IP, τότε ο χρήστης θα ανακατευθυνθεί στη διεύθυνση αυτή, διαφορετικά αν η

διεύθυνση URL δεν εμφανίζεται στο αρχείο hosts θα πραγματοποιηθεί μια DNS αναζήτηση μέσω του παρόχου διαδικτύου (Internet Service Provider) για να εντοπιστεί η αντίστοιχη διεύθυνση.

Το να αντιγράψουμε και να αναλύσουμε το αρχείο hosts επιβάλλεται σε αρκετές περιπτώσεις και ειδικότερα σε περιπτώσεις μόλυνσης με ιομορφικό λογισμικό. Σε αυτή την περίπτωση το ιομορφικό λογισμικό σε αρκετές περιπτώσεις τροποποιεί το αρχείο hosts με σκοπό την παρεμπόδιση του συστήματος του χρήστη από την πρόσβαση σε ορισμένες ιστοσελίδες, κυρίως εκείνες που αντιστοιχούν σε antivirus, σουίτες ασφαλείας ή αναβαθμίσεις του λειτουργικού.

Για να αποκτήσουμε τα περιεχόμενα του αρχείου hosts, εκτελούμε την ακόλουθη εντολή:
c:**> type c:\windows\system32\drivers\etc\hosts > hosts.txt**

Έλεγχος των Ανυπόγραφων Εκτελέσιμων (Check unsigned executables)

Ανάλογα με τον τύπο του περιστατικού, και κυρίως με εκείνα που σχετίζονται με ιομορφικό λογισμικό, είναι χρήσιμο να ελέγχουμε τα ανυπόγραφα αρχεία από ορισμένους φακέλους.
Για να το κάνουμε αυτό, χρησιμοποιούμε εργαλεία όπως το **sigcheck** πληκτρολογώντας την ακόλουθη εντολή:
c:\ sigcheck -ct -h -vr -vt -s c:\Windows\ > Signed_files_windows.txt
c:\ sigcheck -ct -h -vr -vt -s c:\Windows\system32 > Signed_files_windows_system32.txt

Αρχεία LNK (LNK files)

Τα Windows δημιουργούν αυτόματα συντομεύσεις (αρχεία με LNK κατάληξη) για τα πρόσφατα αρχεία ή για οποιοδήποτε αρχείο έχουμε ανοίξει είτε τοπικά είτε απομακρυσμένα. Τα αρχεία με κατάληξη (extension) LNK (συντομεύσεις αρχείων), αποθηκεύουν μεγάλη ποσότητα πληροφοριών που μπορεί να είναι χρήσιμες για μία υπόθεση – περιστατικό. Οι πληροφορίες αυτές περιλαμβάνουν:

- Διαδρομή του αρχείου που αντιστοιχούν.
- Χρόνους MAC από το ίδιο το αρχείο και από το αρχείο με το οποίο συνδέεται.
- Πληροφορίες της μονάδας όπου είναι αποθηκευμένο (όνομα, σειριακό αριθμό, διεύθυνση MAC, κλπ.).
- Πληροφορίες του δικτύου, σε περίπτωση που κάνει αναφορά σε ένα αρχείο που είναι αποθηκευμένο σε μια απομακρυσμένη τοποθεσία.
- Μέγεθος αρχείου.

Στα Windows XP τα αρχεία .lnk δημιουργούνται στον φάκελο:
C:\%USERPROFILE%\Recent

Στα Windows 7/8/10 τα αρχεία .lnk δημιουργούνται στον φάκελο:

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent

Για να συγκεντρώσουμε όλα αυτά τα αρχεία μπορούν να χρησιμοποιηθούν διαφορετικά εργαλεία, όπως το **lnk-parser** ή το **Windows LNK Parsing Utility**. Ένα παράδειγμα της χρήσης του lnk-parser είναι το ακόλουθο:
c:\> **lnk_parser_cmd.exe -0 LinksList -w -s c:**

Ωστόσο μπορούμε να τα αντιγράψουμε δίνοντας\
τις εντολές:
c:\> **robocopy C:\%USERPROFILE%\Recent G:\Recent_XP_dir /E**
c:\> **robocopy C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\ G:\Windows_Recent_dir /E**
c:\> **robocopy C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\ G:\Office_Recent_dir /E**

Η κίνηση του δικτύου

Εκτός από τις πληροφορίες δικτύου που συγκεντρώσαμε αρχικά και περιγράφανε την κατάσταση του δικτύου, τις ενεργές συνδέσεις, κλπ., είναι επίσης σημαντικό να παρακολουθούμε την κίνηση κατά τη διάρκεια ενός περιορισμένου χρονικού διαστήματος για να την αναλύσουμε στην συνέχεια. Σκοπός αυτής της παρακολούθησης- συγκέντρωσης στοιχείων, είναι να εντοπίσουμε τα σημεία ελέγχου ενός botnet (IP επικοινωνίας - C&C servers) με την ανάλυση εκτός σύνδεσης (off-line connections) των πακέτων που συγκεντρώσαμε.

Για να γίνει αυτό, μπορούμε χρησιμοποιήσουμε εργαλεία όπως το **tshark,** το **WinDump**, ή το **dumpcap** τα οποία επιτρέπουν να παρακολουθούμε-συλλέγουμε την δικτυακή κίνηση θέτοντας την κάρτα δικτύου σε **promiscuous** κατάσταση (αν η κάρτα δικτύου το επιτρέπει). Η ενέργεια αυτή πρέπει να γίνεται σε υπολογιστή του ίδιου δικτύου, όχι σε αυτόν που κάνουμε τον έλεγχο. Μπορούμε να παρακολουθούμε την δικτυακή κίνηση του υπολογιστή που είναι υπό έλεγχο μέσω τρίτου υπολογιστή ή μέσω του δρομολογητή του συγκεκριμένου δικτύου. Υπάρχουν αρκετά εργαλεία και τεχνικές που μπορούν να εφαρμοστούν στην συγκεκριμένη φάση.

Ένα παράδειγμα της χρήσης των εργαλείων που αναφέρθηκαν σε αυτή την παράγραφο είναι:

c:\> **windump -i 2 -q -w E:\packet-capture.pcap -n -C 30 -W 10 -U -s 0**
c:\>tshark.exe -i 2 -w packet-capture.pcap
c:\> **dumpcap.exe -i 2 -w packet-capture.pcap**

Άλλα εργαλεία

Tcpdump	http://www.tcpdump.org
Wireshark	http://www.wireshark.org
Netsleuth	http://www.netgrab.co.uk
Windump	http://www.winpcap.org/windump
NetWitness	http://www.emc.com/security/rsa-netwitness.htm

Σημείωση

Για την προστασία των ευαίσθητων δεδομένων (ώστε να μην εξαχθούν εκτός δικτύου) καλό θα είναι ο υπολογιστής που βρίσκεται υπό έλεγχο να τοποθετείται λογικά σε ένα απομονωμένο VLAN χωρίς πρόσβαση στο Διαδίκτυο.

ΚΕΦΑΛΑΙΟ ΣΤ
ΑΝΑΣΚΟΠΗΣΗ

ΤΜΗΜΑ 21
ΕΠΙΛΟΓΟΣ

Όπως επισημάνθηκε στην αρχή του εγχειριδίου, η έννοια της ψηφιακής εγκληματολογικής ανάλυσης, αναφέρεται στο συνδυασμό των διαδικασιών συλλογής πληροφοριών και ανάλυσης αποδεικτικών στοιχείων που πραγματοποιούνται με σκοπό την αντιμετώπιση ενός περιστατικού που σχετίζεται με την ασφάλεια ενός υπολογιστή και, σε ορισμένες περιπτώσεις, μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία στο δικαστήριο. Μέσω αυτής της διαδικασίας, ο στόχος είναι να απαντηθούν τα ακόλουθα ερωτήματα: **Τι; Πού; Πότε; Γιατί; Ποιος; Πώς;**

Η επιστήμη αυτή λαμβάνει ένα πολύ σημαντικό ρόλο τα τελευταία χρόνια και η χρήση της επεκτείνεται, καθώς είναι συχνά τα περιστατικά που σχετίζονται με την ασφάλεια υπολογιστών, όπως παραβιάσεις συστημάτων, υποκλοπή πληροφοριών, μολύνσεις με ιούς, κλπ.

Υπάρχουν διαφορετικές μεθοδολογίες που μπορούν να υιοθετηθούν για τη ολοκλήρωση αυτής της διαδικασίας, που είναι όλες βασισμένες στην ίδια γενική ιδέα και έχουν κοινές κατευθυντήριες γραμμές και φάσεις. Μία από τις πιο σημαντικές, είναι αυτή που περιγράφεται και αναφέρεται λεπτομερώς στο έγγραφο *RFC3227*. Μεταξύ των πιο σημαντικών πτυχών που πρέπει να έχουμε κατά νου και για την οποία το *RFC3227* κάνει ειδική μνεία, είναι η σειρά της μεταβλητότητας των αποδεικτικών στοιχείων, που δείχνει ότι το πρώτο καθήκον είναι να ανακτηθούν τα αποδεικτικά στοιχεία που θα είναι διαθέσιμα μόνο για περιορισμένο χρονικό διάστημα και στην συνέχεια τα υπόλοιπα .

Σε γενικές γραμμές, λαμβάνουμε ένα αντίγραφο της μνήμης και του σκληρού δίσκου και τα αναπαράγουμε προκειμένου να εργαστούμε πάνω στα αντίγραφα, για τη λήψη των περαιτέρω αποδεικτικών στοιχείων. Ωστόσο, κατά τη διεξαγωγή της διαδικασίας, είναι πολύ σημαντικό να έχουμε σαφή ιδέα για το

συγκεκριμένο τύπο του περιστατικού, προκειμένου να εξακριβώσουμε ποιες πληροφορίες πρέπει να συλλεχθούν και πώς θα προχωρήσουμε.

Τέλος, αξίζει να υπογραμμιστεί ότι κάθε διαδικασία πρέπει να πραγματοποιείται με ένα πολύ αυστηρό και σχολαστικό τρόπο, με σκοπό τη διατήρηση της ακεραιότητας και της εγκυρότητάς της.

ΥΠΟΔΕΙΓΜΑΤΑ

(Υπόδειγμα 1)

ΣΥΣΤΗΜΑΤΑ ΠΟΥ ΕΜΠΛΕΚΟΝΤΑΙ ΣΤΟ ΠΕΡΙΣΤΑΤΙΚΟ

Α/Α	ΣΥΣΤΗΜΑ	ΜΠΟΡΕΙ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΘΕΙ ΓΙΑ ΕΞΑΓΩΓΗ ΣΤΟΙΧΕΙΩΝ	ΠΑΡΑΤΗΡΗΣΕΙΣ

(Υπόδειγμα 2)

ΛΙΣΤΑ ΕΝΕΡΓΕΙΩΝ

Α/Α	ΕΝΕΡΓΕΙΑ	ΥΛΟΠΟΙΗΣΗ	ΣΧΕΤΙΚΟ ΑΡΧΕΙΟ - ΠΑΡΑΤΗΡΗΣΕΙΣ
1	**Ώρα και ημερομηνία του συστήματος**		
2	**memory dump**		
3	**Εκτελούμενες διεργασίες**		
4	**Εκτελούμενες Υπηρεσίες**		
5	**Χρήστες που έχουν ανοίξει μια σύνοδο (session) και λίστες με λογαριασμούς χρηστών.**		
6	**Κατάσταση του δικτύου**		
7	**Εγκατεστημένες συνδέσεις NetBIOS**		
8	**Προσφάτως μεταφερθέντα αρχεία μέσω του NetBIOS**		
9	**Ενεργές συνδέσεις ή ανοιχτές θύρες**		
12	**Περιεχόμενα DNS cache**		
11	**ARP cache**		
12	**Η κίνηση του δικτύου**		
13	**Windows registry**		
14	**Συνδεδεμένες συσκευές USB**		
15	**Λίστα των δικτύων Wi-Fi με τα οποία έχει συνδεθεί το σύστημα**		
16	**Διαμόρφωση του Windows Security Center / Windows Action Center**		
17	**Διαμόρφωση του τείχους προστασίας (firewall) των Windows**		
18	**Προγράμματα που εκτελούνται όταν το λειτουργικό σύστημα είναι ενεργοποιημένο**		
19	**Τα file extensions και τα σχετικά/αντίστοιχα προγράμματα που χρησιμοποιούνται για να τα ανοίξουμε**		

./.

20	**Συσχετισμός αρχείων με φίλτρα**		
21	**Browser Helper Objects (BHO)**		
22	**MUICache**		
23	**LastVisitedMRU/ LastVisitedPidlMRU**		
24	**OpenSaveMRU**		
25	**Πρόσφατα ανοιγμένα αρχεία**		
26	**Εγκατεστημένο λογισμικό**		
27	**Κωδικοί πρόσβασης**		
28	**Προσωρινά αποθηκευμένες πληροφορίες σε προγράμματα περιήγησης (διευθύνσεις, λήψη ιστορικού)**		
29	**File and folder tree**		
30	**Ιστορικό των διερμηνειών εντολής**		
31	**Screen captures**		
32	**Clipboard**		
33	**Ιστορικό αναζήτησης στο Διαδίκτυο**		
34	**Τελευταίες αναζητήσεις**		
35	**Cookies**		
36	**Κρυπτογραφημένοι δίσκοι**		
37	**Mapping units**		
38	**Διαμοιρασμένοι φάκελοι**		
39	**Εγγραφές εν αναμονή**		
40	**Μεταποθήκευση δίσκου**		
41	**Master Boot Record**		
42	**Master File Table**		
43	**Πληροφορίες συστήματος**		
44	**Εργασίες προγράμματος**		
45	**Εκτυπωμένα αρχεία**		
46	**Μεταβλητές στις ρυθμίσεις**		
47	**System logs**		
48	**Αρχεία καταγραφής συμβάντων των Windows**		
49	**WindowsUpdate.log**		
50	**pfirewall.log**		

51	**Άλλα αρχεία καταγραφής**		
52	**Αρχεία .PST και .OST**		
53	**Φάκελος Prefetch**		
54	**Κάδος ανακύκλωσης**		
55	**Αρχείο Hosts**		
56	**Check unsigned executables**		
57	**Αρχεία LNK**		

(Υπόδειγμα 3)
ΑΛΥΣΙΔΑ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Ποιοι ήταν στο χώρο;

Τι έκαναν;

Τι έψαχναν;

Πως αντέδρασαν;

Ποιος ανακάλυψε και συγκέντρωσε τα αποδεικτικά στοιχεία;

Πότε ;

Που;

Ποιος χειρίστηκε τα αποδεικτικά στοιχεία;

Πότε ;

Που;

Ποιος φύλαγε τα αποδεικτικά στοιχεία;

Για πόσο καιρό;

Πώς τα αποθήκευε;

Εάν τα αποδεικτικά στοιχεία άλλαξαν επιμέλεια / χέρια φύλαξης/παρακολούθησης, πότε και πώς έλαβε χώρα η ανταλλαγή (συμπεριλαμβανομένου του αριθμού δελτίου παράδοσης, κλπ);

Αριθμός Υπόθεσης:

Είδος Περιστατικού:

Επηρεαζόμενη Υπηρεσία:

Διεύθυνση:

Τηλέφωνο:

Ημερομηνία και Ώρα:

Ερευνητής:

Παρατηρήσεις;

(Υπόδειγμα 4)

ΕΠΑΦΕΣ

ΛΙΣΤΑ ΕΠΑΦΩΝ
Αριθμός Υπόθεσης:
Αριθμός σελίδας:

Ονοματεπώνυμο	Email	Τηλέφωνο	Θέση

Αριθμός Υπόθεσης:

Είδος Περιστατικού:

Επηρεαζόμενη Υπηρεσία:

Διεύθυνση:

Τηλέφωνο:

Ημερομηνία και Ώρα:

Ερευνητής:

Παρατηρήσεις;

(Υπόδειγμα 5)

ΛΙΣΤΑ ΑΠΟΔΕΙΞΕΩΝ

Αριθμός Υπόθεσης:
Αριθμός σελίδας:

Αποδεικτικό Στοιχείο	Ποσότητα	Περιγραφή αντικειμένου (Μάρκα, μοντέλο, σειριακός αριθμός, κατάσταση, κ.τ.λ.)

./.