ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΨΗΦΙΑΚΗ ΔΙΚΑΝΙΚΗ ΕΝΟΣ ΔΡΟΜΟΛΟΓΗΤΗ

ΦΑΡΟΥΓΓΙΑ ΕΙΡΗΝΗ

Περιεχόμενα

ABSTRACT

An application of digital forensic and scientific knowledge to enable information to be legally retrieved from any digital devices such as computers and smart phones is digital forensics, or digital forensics. Information that is legally obtained is then presented as a piece of evidence in the courtroom. Computer forensics also refers to digital forensics. Various steps are involved in the investigation of digital crimes, such as evidence presentation and validation, search, recovery and identification. Recent research has shown the huge cascade of cyber attacks and threats, which require forensic and forensic experts to simplify the system of the digital world. digital forensics is considered to be directly related to data retrieval and research. This sector faces some technical, resource and legal challenges differently. The aim of this study is to explore new dimensions of digital forensics, such as network forensics, computer forensics and router forensics. All the findings of the research allow for a better understanding of digital forensics, which could be considered useful in forensic research. Therefore, in this thesis, the need for security is studied by analyzing the science of digital forensics in general, but specifically in the case of routers, and what methods the researchers used during an investigation.

Λέξεις κλειδιά : Ψηφιακή Εγκληματολογία, Ψηφιακή δικανική, routers, hacking, έρευνα routers, ψηφιακά δεδομένα

Κεφάλαιο 1ο

Εισαγωγή

Η σημερινή ραγδαία ανάπτυξη της τεχνολογίας, σχεδόν επιβάλλει τη ζωή μέσα σε ένα ψηφιακό κόσμο, ο οποίος έχει εισβάλει σε κάθε πτυχή της. Τα κινητά τηλέφωνα και οι ηλεκτρονικοί υπολογιστές, κατέστησαν απαραίτητα εργαλεία σχεδόν σε κάθε επαγγελματική δραστηριότητα. Η ανάπτυξη του διαδικτύου παράλληλα, επέφερε αλλαγές σε κάθε έκφανση της ανθρώπινης επαφής και της καθημερινότητας, καθώς και

των εργασιακών σχέσεων. Είναι επόμενο λοιπόν, να διεξάγονται έρευνες από πολλούς ακαδημαϊκούς φορείς και βιομηχανίες, πάνω σε αυτό το θέμα προκειμένου να ανακαλυφθούν όλες οι δυνατότητες που περιέχονται στην έννοια αυτή, να αφομοιωθούν από την ανθρωπότητα με στόχο την αύξηση της ποιότητας ζωής. Ένα σημαντικό ζήτημα που γεννιέται ωστόσο, είναι η ασφάλεια των δεδομένων τα οποία διακινούνται ανάμεσα στους ανθρώπους και τις συσκευές και κατ' επέκταση στο διαδίκτυο.

Τα εγκλήματα του ψηφιακού κόσμου είναι όμοια με αυτά του φυσικού κόσμου. Όταν λαμβάνει χώρα ένα έγκλημα στον φυσικό κόσμο, σχεδόν πάντα θα έχουν παραμείνει ίχνη, ανθρώπινο γενετικό υλικό διάφορα στοιχεία, τα οποία θα αποδεικνύουν από ποιον, πώς και γιατί διαπράχθηκε το έγκλημα. Στον ψηφιακό κόσμο αντίστοιχα, το ψηφιακό έγκλημα, αφήνει ηλεκτρονικά ίχνη, τα οποία μπορούν να οδηγήσουν στο δράστη. Στο σημείο αυτό, υπεισέρχεται και η επιστήμη της ανάλυσης και ανάκτησης ψηφιακών πειστηρίων ή αλλιώς ψηφιακής δικανικής (digital forensics), ώστε να μπορέσει να καταδειχθεί ο δράστης και να οδηγηθεί ενώπιον της δικαιοσύνης. Σύμφωνα με τον McKemmish (1999) η ψηφιακή εγκληματολογία περιγράφεται ως μια διαδικασία ανάλυσης, παρουσίασης, διατήρησης και ταυτοποίησης ψηφιακών αποδείξεων, με νομικά αποδεκτό τρόπο. Στην πράξη, εννοούνται τα πειστήρια τα οποία ανακαλύφθηκαν από τον ερευνητή μετά από μια ψηφιακή επίθεση, τα οποία μπορούν να παρουσιαστούν σε δικαστική αίθουσα με νόμιμη βάση ώστε να χρησιμοποιηθούν αναλόγως.

Δομή της εργασίας

Στο πρώτο κεφάλαιο παρουσιάζεται μια σύντομη εισαγωγή της εργασίας, μαζί με τη δομή που θα ακολουθηθεί, καθώς και του στόχους και τη συνεισφορά της εργασίας αυτής.

Στο δεύτερο κεφάλαιο παρουσιάζονται κάποιες γενικές έννοιες ασφάλειας, με επίκεντρο την ασφάλεια υπολογιστών.

Στο τρίτο κεφάλαιο παρουσιάζεται η ψηφιακή δικανική, οι μεθοδολογίες και οι κλάδοι της.

Στο τέταρτο κεφάλαιο παρουσιάζεται η απόκτηση ψηφιακών δεδομένων επικεντρωμένο στη στατική, ζωντανή απόκριση καθώς και στις μεθόδους και τα εργαλεία απόκτησης.

Στο πέμπτο κεφάλαιο παρουσιάζεται η δικανική ενός δικτύου, μια επισκόπηση των δρομολογητών (routers), το χακάρισμά τους, η διερεύνησή τους και τελικά μια απόκριση σε ένα γεγονός.
Στο έκτο κεφάλαιο παρουσιάζονται τα συμπεράσματα που εξήχθησαν από τη μελέτη αυτή.

Στόχοι της εργασίας

Οι στόχοι της διπλωματικής είναι να κατανοήσουμε την έννοια της ψηφιακής εγκληματολογίας και πιο συγκεκριμένα στην περίπτωση του router. Επιπλέον, μελετάται η δικανική δικτύου και πως συνδυαστικά με τη δικανική του router και μέσα από μελέτη συμβάντος, μπορούν να αντληθούν χρήσιμες πληροφορίες που θα οδηγήσουν στην καλύτερη ανάλυση του θέματος. Επιδιώκεται μετά από αυτή την ανάλυση ο αναγνώστης να έχει μια ολοκληρωμένη άποψη γύρω από αυτά.

Συνεισφορά της διπλωματικής εργασίας

Η συνεισφορά της διπλωματικής ορίζεται ως εξής:

1. Πραγματοποιήθηκε ανάλυση της επιστήμης της Ψηφιακής Εγκληματολογίας, της δικανικής δικτύου και router.
2. Αναλύθηκε το πώς αποκτούνται τα ψηφιακά δεδομένα.
3. Μέσα από τη χρήση της ακαδημαϊκής βιβλιογραφίας αναλύθηκαν τα βήματα της ψηφιακής δικανικής ενός router.

Κεφάλαιο 2^{ο}

Γενικές Έννοιες Ασφάλειας

2.1 Ασφάλεια υπολογιστών

Η ασφάλεια αποτελεί ένα από τα σημαντικότερα κομμάτια της καλής λειτουργίας μιας έξυπνης συσκευής, ενός υπολογιστή ή ενός δικτύου υπολογιστών. Κρύβονται πολλοί κίνδυνοι στο διαδίκτυο τόσο για τους πιο έμπειρους, αλλά και απλούς χρήστες, καθώς

και για οργανισμούς και επιχειρήσεις. Παρόλο που υπάρχουν πλέον δισεκατομμύρια κάτοχοι έξυπνων συσκευών και υπολογιστών, ελάχιστοι είναι αυτοί οι οποίοι γνωρίζουν τους κινδύνους αυτούς. Προβάλλεται λοιπόν μια αναγκαία συνθήκη συνδυαστικά με άλλες βασικές λειτουργίες όπως η απόδοση και η ποιότητα των υπηρεσιών, για να μπορέσει να λειτουργήσει ολοκληρωμένα και σωστά μια επιχείρηση ή ακόμη και η χρήση ενός προσωπικού υπολογιστή, του διαδικτύου ή του έξυπνου κινητού από έναν χρήστη.

Η προστασία των πληροφοριών, οι οποίες υπάρχουν στην κατοχή διαφόρων ατόμων από περιπτώσεις καταστροφών και αλλοιώσεων, καθώς και από παράνομη χρήση τους, χτίζει την έννοια της ασφάλειας, ενώ σχετίζονται άμεσα. Συνεπώς, η ασφάλεια στηρίζεται στο να ληφθούν μέτρα στα οποία διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών και των δεδομένων, καθώς και η συνεχής λειτουργία του υπολογιστή και του δικτύου. Πιο συγκεκριμένα υπάρχει σύνδεση της ασφάλειας με :

Πρόληψη (Prevention): Στην πρόληψη λαμβάνονται μέτρα ώστε να μπορέσουν να προληφθούν φθορές και καταστροφές σε δεδομένα ακόμα και στους υπολογιστές.

Ανίχνευση (Detection): Στην λήψη μέτρων, ανιχνεύεται από ποιον, πώς και πότε προκλήθηκε φθορά και καταστροφή.

Αντίδραση (Reaction): Η αντίδραση, αφορά τη λήψη μέτρων για να μπορέσουν να ανακτηθούν ή να αποκατασταθούν οι πληροφορίες και τα δεδομένα που πιθανώς επηρεάστηκαν.

Ένα θέμα το οποίο πρέπει να αντιμετωπίσουν οι οργανισμοί αλλά και οι χρήστες ανεξάρτητα, είναι η προστασία ενός δικτύου αισθητήρων ή υπολογιστών ακόμη και των προσωπικών υπολογιστών οι οποίοι έχουν σύνδεση στο διαδίκτυο. Ωστόσο, κατοχυρώθηκαν πλέον οι έννοιες Ακεραιότητα, Εμπιστευτικότητα και Διαθεσιμότητα, οι οποίες είναι σχετιζόμενες αρκετά στενά με την έννοια της ασφάλειας. Η ακεραιότητα, αποτελεί μια διαβεβαίωση ότι οι ληφθέντες πληροφορίες και δεδομένα τα οποία έχουν σταλεί και αποθηκευτεί, δεν υπέστησαν κάποια μετατροπή από κάποιο τρίτο μη εξουσιοδοτημένο πρόσωπο. Κάτι τέτοιο σημαίνει ότι οποιαδήποτε αλλαγή μπορεί να γίνει μόνο από εξουσιοδοτημένους χρήστες και κανέναν άλλον. Η εμπιστευτικότητα, ασχολείται με το να προληφθεί η μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες και τα δεδομένα. Από τη στιγμή που ο εισβολέας δεν μπορεί να

τροποποιήσει κάποιο σύστημα, οι επιθέσεις θεωρούνται παθητικές. Παρόλα αυτά, μπορεί να κλέψει τα αντίγραφα των πληροφοριών, οι οποίες είναι αποθηκευμένες στον υπολογιστή ή μεταδίδονται και διέρχονται μέσω του δικτύου.

Η διαθεσιμότητα, αποτελεί τη διασφάλιση ότι όλα τα προγράμματα, δεδομένα και πληροφορίες θα είναι προσβάσιμα στους χρήστες του δικτύου. Με αυτό τον τρόπο, θα μπορούν να είναι λειτουργικές όλες οι υπηρεσίες χωρίς να έχει σημασία αν υπάρξει κάποιο ατύχημα κάποια τυχαία διακοπή ρεύματος, κ.λπ. Κάτι τέτοιο βέβαια, σημαίνει ότι οι χρήστες δεν θα αντιμετωπίσουν στην περίπτωση που θελήσουν να χρησιμοποιήσουν το δίκτυο την άρνηση εξυπηρέτησης (Denial of Service). Οι επιθέσεις αυτές, δηλαδή της άρνησης της εξυπηρέτησης, θεωρούνται επιθέσεις εναντίον ενός δικτύου υπολογιστή όπου αποσκοπούν να καταστήσουν το δίκτυο ή τον υπολογιστή ανίκανο να δεχτεί άλλες συνδέσεις, έχοντας ως αποτέλεσμα να μην μπορεί να εξυπηρετήσει κανέναν. Δεν επιτρέπεται επίσης η προσπέλαση και η εκμετάλλευση πληροφοριών και δεδομένων από κανένα νόμιμο χρήστη.

Αναγκαιότητα της Ασφάλειας

Τα τελευταία χρόνια, εξαιτίας της εξάπλωσης και της ανάθεσης των διαφόρων υπηρεσιών του διαδικτύου, ηλεκτρονικών συσκευών, τεχνολογιών και του Internet of Things, αναπτύσσονται ταυτόχρονα και πολυάριθμοι κίνδυνοι. Έτσι λοιπόν, γίνεται απαραίτητη η χρήση ασφαλείας τόσο σε επίπεδο επιχειρήσεων και οργανισμών όσο και σε προσωπικό επίπεδο, καθώς έτσι μπορούν να προστατευτούν τα οικονομικά και τα σχέδια μιας επιχείρησης, τα προσωπικά δεδομένα και οι διάφορες πληροφορίες. Είναι επόμενο, όμως, όταν υιοθετούνται διάφορα μέτρα ασφαλείας να δημιουργούνται κάποια προβλήματα στη λειτουργία των υπολογιστών, των δικτύων και των έξυπνων συσκευών, όπως το κόστος λειτουργίας και εγκατάστασης μιας συσκευής ή ενός δικτύου, και η επιβάρυνση της απόδοσης.

Ο ανταγωνισμός, η τεχνολογία και οι διάφοροι εισβολείς, οι οποίοι κατέχουν συνεχώς βελτιωμένους τρόπους επιθέσεων, καθιστούν επιτακτικό να γίνονται συχνά έλεγχοι του συστήματος. Στην περίπτωση, λοιπόν, που ακολουθείται η πολιτική αυτή στις επιχειρήσεις και γενικά σε όλο τον κόσμο, μπορεί να υπάρξει μείωση των κινδύνων καθώς διορθώνεται το σύστημα ασφαλείας, ενώ εμφανίζεται και βελτιώνεται πιο έτοιμο για κάθε πιθανή επίθεση από οπουδήποτε. Υπάρχουν όμως περιπτώσεις, όπου τελικά η ασφάλεια δεν κατάφερε να αποτρέψει κάποια επίθεση ή κάποιο άλλο γεγονός

που είχε ως στόχο να βλάψει μια επιχείρηση ή κάποιον άνθρωπο. Η ανάλυση των δεδομένων και η διερεύνηση μιας επίθεσης είναι διαδικασίες οι οποίες σχετίζονται με την ψηφιακή εγκληματολογία η οποία εξετάζεται παρακάτω, και αποτελεί ένα στενά συνδεδεμένο κλάδο με την ασφάλεια.

Κεφάλαιο 3ο

Ψηφιακή δικανική

3.1 Ψηφιακή δικανική

Η ψηφιακή δικανική (Digital forensics) ορίζεται ως : Η χρήση επιστημονικά αποδεκτών μεθόδων οι οποίες έχουν ως στόχο την καταγραφή, την παρουσίαση, την ερμηνεία, την ανάλυση και την αναγνώριση ψηφιακών πειστηρίων, τα οποία προέρχονται από τα ψηφιακά μέσα, έχοντας στόχο την έγκαιρη αντιμετώπιση και

πρόληψη μη εξουσιοδοτημένων ενεργειών που αποτελούν κίνδυνο για σχεδιαζόμενες διαδικασίες ή την αναπαράσταση και ανακατασκευή εγκληματικών ενεργειών (Digital Forensics Research Workshop, 2001). Τα ψηφιακά πειστήρια μπορεί να είναι οποιοδήποτε πληροφορία είναι μεταδιδόμενη ή αποθηκευμένη σε δυαδική μορφή, κάτι το οποίο περιλαμβάνει αξιόπιστες πληροφορίες οι οποίες καταρρίπτουν ή υποστηρίζουν μια υπόθεση.

Το ψηφιακό μέσο είναι οποιαδήποτε συσκευή μπορεί να λάβει ή να στείλει, να επεξεργαστεί και να αποθηκεύσει ψηφιακές πληροφορίες. Κάτι τέτοιο δεν αναφέρεται μόνο σε επιτραπέζιους και φορητούς υπολογιστές. Οι συσκευές βίντεο, οι ηχητικές συσκευές, οι προσωπικοί ψηφιακοί βοηθοί (PDAs), τα συστήματα cloud, οι βάσεις δεδομένων, τα δίκτυα και οι κινητές συσκευές, αποτελούν επίσης ψηφιακά μέσα βρισκόμενα και αυτά εντός του πεδίου της ψηφιακής δικανικής. Ως στόχο της ψηφιακής δικανικής, αποτελεί η αποκάλυψη ψηφιακών στοιχείων και η διαμόρφωση της υπόθεσης την οποία επιδεικνύουν ως λανθασμένη η έγκυρη. Θεωρείται απαραίτητη η διαμόρφωση της υπόθεσης, καθώς οι ψηφιακές καταστάσεις και γεγονότα δεν μπορούν να εντοπιστούν άμεσα, συνεπώς τα γεγονότα δεν είναι γνωστά.

Για να μπορέσει να προσδιοριστεί η κατάσταση των ψηφιακών δεδομένων πρέπει να χρησιμοποιηθούν εργαλεία κάτι που τα καθιστά έμμεσες παρατηρήσεις. Επιπρόσθετα, κάποια άλλα χαρακτηριστικά των ψηφιακών στοιχείων, αποτελούν η μεταβλητότητα και η ευθραυστότητα, καθώς και η μη απτή φύση τους, κάτι που τους επιβάλλει ειδική μεταχείριση. Χρειάζεται επομένως ιδιαίτερη προσοχή στο υλικό και στο λογισμικό τα οποία θα χρησιμοποιηθούν για να αναλυθούν και να εξαχθούν τα ψηφιακά πειστήρια, όπως επίσης και στις διαδικασίες οι οποίες θα ακολουθηθούν, έτσι ώστε να υπάρχει εμπιστοσύνη στο κατά πόσο είναι έγκυρες για να μην απορριφθούν από κάποιο πιθανό δικαστήριο. Στην ψηφιακή δικανική παρουσιάζεται μεγάλη ποικιλία εφαρμογών. Αρχικά εφαρμόζεται στα πλαίσια εγκληματολογικών ερευνών οι οποίες περιλαμβάνουν ψηφιακά στοιχεία, έτσι ώστε να απορριφθεί ή να επιβεβαιωθεί μια υπόθεση πριν από τη δίκη. Όταν ακούει κάποιος για τέτοιες έρευνες, κατευθείαν φέρνει στο μυαλό του κλοπή ταυτότητας ή παιδική πορνογραφία, αλλά δεν περιορίζεται μόνο σε αυτού του είδους τα εγκλήματα.

Τα ηλεκτρονικά αποδεικτικά στοιχεία στο σημερινό ψηφιακό κόσμο μπορούν να βρεθούν σε οποιαδήποτε είδους εγκληματολογική έρευνα. Σε μια ληστεία, για

παράδειγμα, υπάρχει περίπτωση κάποιος από τους κακοποιούς να αφήσει το κινητό του, και να μπορέσουν έτσι να εξαχθούν στοιχεία όπως είναι κάποιες κλήσεις ή μηνύματα τα οποία να μπορέσουν να υποδείξουν και άλλους συνεργούς του. Ο κλάδος αυτός της εγκληματολογίας εφαρμόζεται επιπλέον σε κάποιες περιπτώσεις όπου δεν εμπλέκεται παραβίαση της νομοθεσίας. Μπορεί να υπάρχουν κάποιου είδους ηλεκτρονικών πληροφοριών που βρίσκονται αποθηκευμένες σε διάφορες παραβιάσεις διαδικασιών και πολιτικών. Ένας υπάλληλος, για παράδειγμα, την ώρα την οποία εργάζεται σε μια εταιρεία, μπορεί να λειτουργήσει και μια δεύτερη προσωπική επιχείρηση με τη χρήση των υπολογιστών της εταιρείας. Ενώ αυτό δεν αποτελεί παραβίαση του νόμου, μπορεί παρόλα αυτά να δικαιολογήσει μια διεξαγωγή έρευνας από την επιχείρηση.

Η Ιστορία της Ψηφιακής Εγκληματολογίας

Η πρώτη ομάδα η οποία ασχολήθηκε με ψηφιακά πειστήρια δημιουργήθηκε το 1984 από το FBI. Το όνομα αυτής της ομάδας ήταν Computer Analysis and Response Team (CART). Εκείνη την περίοδο παρόλο που τα λειτουργικά συστήματα ήταν αρκετά, η διαδικασία της ψηφιακής εγκληματολογίας δεν ήταν τόσο απαιτητική. Το NortonDiskEdit ήταν ένα από τα εργαλεία εκείνης της περιόδου (Zareen, et al. 2013). Η αρχή των λειτουργικών συστημάτων με γραφικό περιβάλλον (GUI) έγινε το 1990, ενώ το ακολούθησαν υιοθετώντας το γραφικό περιβάλλον, τα εργαλεία της ψηφιακής εγκληματολογίας όπως το EnCase. Το λειτουργικό σύστημα των Windows τη δεκαετία του 2000-2010, γνώρισε τεράστια άνθηση καταφέρνοντας να γίνει το κύριο λειτουργικό σύστημα, τόσο σε εταιρικούς όσο και σε προσωπικούς υπολογιστές. Εξαιτίας της εξέλιξης αυτής, η ψηφιακή εγκληματολογία έγινε σχετικά ευκολότερη σαν διαδικασία, καθώς οι περισσότεροι υπολογιστές έκαναν χρήση κοινού λειτουργικού συστήματος.

Ο Pollit (2010), κατέγραψε την εξέλιξη της ψηφιακής εγκληματολογίας, με εκκίνηση την προϊστορική εποχή η οποία ορίζεται πριν το 1985, όπου δεν υπήρχε ακόμη ο όρος ψηφιακή εγκληματολογία, ενώ οι υπολογιστές χρησιμοποιούνταν παρά μόνο σε μεγάλες επιχειρήσεις. Δεν μπορεί λοιπόν να θεωρηθεί παράξενο που δεν υπάρχουν πολλές αναφορές για την περίοδο εκείνη. Το 1985-1995, θεωρήθηκε μια βρεφική περίοδος, όπου ξεκίνησαν δειλά οι υπολογιστές να μπαίνουν εκτός από τις επιχειρήσεις και στα σπίτια των ανθρώπων, ενώ οι χρήστες μπορούσαν να αντιληφθούν πόσο

μεγάλο ρόλο θα παίξουν οι υπολογιστές στο μέλλον, αφού κανείς δεν έχει τη δυνατότητα να συγκεντρώσει τόσες πολλές πληροφορίες. Το 1995 ως το 2005, αποτέλεσε την παιδική περίοδο, η οποία σηματοδότησε μια έκρηξη στην επιστήμη.

Γι' αυτό υπήρχαν πολλοί λόγοι. Η έκρηξη της τεχνολογίας ωστόσο, η διακίνηση ύποπτου υλικού μέσα από τα δίκτυα και τους υπολογιστές, οι παράνομες δραστηριότητες, ακόμα και τα συμβάντα της 11/09/2001, ήταν σαφώς σημαντικότερα. Η ψηφιακή εγκληματολογία από το 2005 έως και σήμερα, διανύει την εφηβική της περίοδο, στην οποία γνώρισε την πιο μεγάλη απήχηση αναφορικά με τους επαγγελματίες, οι οποίοι ασχολούνται με την επιστήμη αυτή. Καθώς αυξάνονται οι πηγές απ' όπου μπορεί κανείς να αποσπάσει στοιχεία, προσφέρουν παραπάνω όγκο δεδομένων στον κάθε ερευνητή.

Ψηφιακά Πειστήρια (Digital Evidence)

Σημαντικό ρόλο στη διαμόρφωση ενός αποτελέσματος για μια έρευνα, παίζουν τα ψηφιακά πειστήρια ή ψηφιακά αποδεικτικά στοιχεία. Οι Carrier και Spafford (2004) σε μια μελέτη τους όρισαν τα ψηφιακά πειστήρια, ως τις πληροφορίες οι οποίες μπορούν να διαψεύσουν ή να στηρίξουν μια υπόθεση, για την κατάσταση των ψηφιακών πληροφοριών ή για ψηφιακά γεγονότα. Η συλλογή τέτοιου είδους πειστηρίων μπορεί να γίνει σε περιπτώσεις όπου εμπλέκονται ψηφιακές συσκευές οι οποίες παρέχουν τα αντίστοιχα δεδομένα. Το 2009 ο Perumal υποστήριξε πως τα ψηφιακά πειστήρια θεωρούνται οποιαδήποτε πληροφορία, η οποία μπορεί να παρέχει διασύνδεση ανάμεσα στο θύμα και στο λόγο του εγκλήματος. Τα στοιχεία αυτά, μπορούν να παράξουν μια ψηφιακή διάσταση σε μια έρευνα με τον ερευνητή, ο οποίος θα συλλέγει, να μπορέσει σε αρκετά μεγάλο βαθμό να δημιουργήσει το προφίλ ενός ατόμου.

Θεωρούνται ιδιαίτερα ευπαθή, ενώ η μορφοποίηση ή ακόμη και η καταστροφή τους μπορεί να πραγματοποιηθεί από απρόσεκτο χειρισμό. Γι' αυτό το λόγο, οφείλουν να λαμβάνονται μέτρα ασφαλείας ώστε να διατηρήσουν την αρχική τους κατάσταση. Υπάρχει ποικιλία στους τύπους πειστηρίων που ενδέχεται να εμφανιστούν. Οι έξυπνες συσκευές, τα κινητά και οι υπολογιστές, μπορούν να βρεθούν πλέον παντού σε κάθε πτυχή της καθημερινότητας. Το 2000 ο Henseler κατηγοριοποίησε τα υπολογιστικά συστήματα που περιέχουν τέτοιου είδους δεδομένα, ως εξής:

Ανοιχτά υπολογιστικά συστήματα (Open Computer Systems): αποτελούν τους κοινούς υπολογιστές, οι οποίοι χρησιμοποιούνται πλέον από πάρα πολλούς ανθρώπους, είτε για τη διασκέδασή τους είτε εξαιτίας της δουλειάς τους. Καθώς εξελίσσεται η τεχνολογία, με την πάροδο του χρόνου, εξελίσσεται και ο χώρος αποθήκευσης των σκληρών δίσκων, ο οποίος καταλήγει σε όλο και μεγαλύτερα νούμερα, κάτι που συνεπάγεται ακόμα περισσότερες πληροφορίες, οι οποίες μπορούν να χρησιμοποιηθούν ως ψηφιακά πειστήρια.

Συστήματα Επικοινωνίας (Communication Systems): τα συστήματα επικοινωνίας αποτελούνται από τηλεφωνικά συστήματα, τα οποία όπως είναι γνωστό είναι το διαδίκτυο και τα ασύρματα δίκτυα επικοινωνίας, αποτελούν συστήματα που έχουν τη δυνατότητα να παρέχουν στοιχεία τα οποία μπορεί να φανούν χρήσιμα στον ερευνητή. Ποιος ήταν ο παραλήπτης, ποιος ο αποστολέας και ποιος ο χρόνος που στάλθηκε ένα μήνυμα μέσα από το ηλεκτρονικό ταχυδρομείο ή μέσα από το κινητό, είναι μόνο κάποιες από τις πληροφορίες τις οποίες θα μπορούσαν να εκμεταλλευτεί ο εκάστοτε ερευνητής.

Ενσωματωμένα Υπολογιστικά Συστήματα (Embedded Computer Systems): τα ενσωματωμένα υπολογιστικά συστήματα, είναι οι έξυπνες κάρτες, τα κινητά τηλέφωνα οι συσκευές οι οποίες έχουν δυνατότητα στιγματοθέτησης (GPS), όπως επίσης και ότι περιέχει γενικότερα κάποιο υπολογιστικό σύστημα, προσφέροντας πληροφορίες. Υπάρχουν πλέον τα συστήματα cloud, οι έξυπνες κάρτες, τα έξυπνα αυτοκίνητα, τα έξυπνα κινητά τηλέφωνα και τα wearables, τα οποία όλα μαζί αποτελούν το Διαδίκτυο των Πραγμάτων, ενώ έχουν τη δυνατότητα της μεταξύ τους επικοινωνίας.

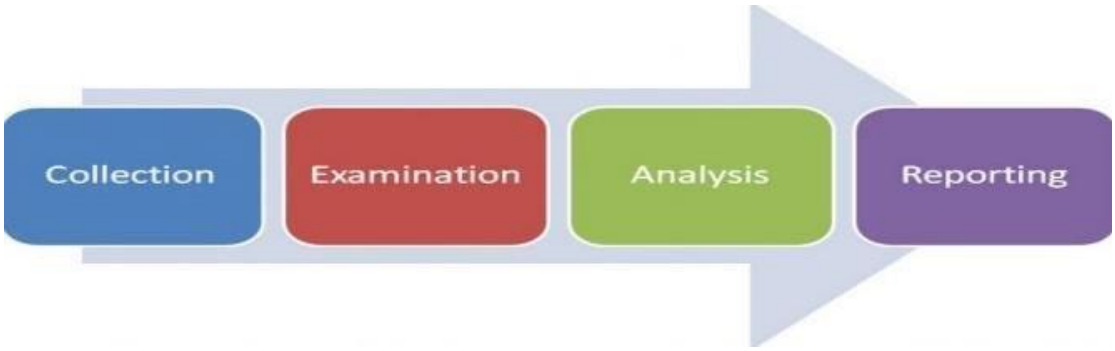
Μεθοδολογία Ψηφιακής Εγκληματολογίας

Μοντέλο του National Institute of Standards and Technology

Οι ερευνητές της ψηφιακής εγκληματολογίας χρησιμοποιούν διαφορετικές μεθοδολογίες οι οποίες ποικίλουν. Στη βιβλιογραφία προτάθηκαν κατά καιρούς πολλά μοντέλα καθώς οι περιπτώσεις δεν είναι όλες οι ίδιες, ενώ ο ερευνητής πρέπει να προσαρμόσει ανάλογα την έρευνά του. Ωστόσο, με μια προσεκτική μελέτη, μπορεί κάποιος να παρατηρήσει πως σχεδόν όλα ακολουθούν περίπου τις ίδιες διαδικασίες και βήματα με κάποιες είτε μικρές είτε μεγάλες παραλλαγές. Σύμφωνα με το National

Institute of Standards and Technology (NIST), τα πιο συνηθισμένα βήματα τα οποία μπορούν να εφαρμοστούν σε κάθε έρευνα εγκληματικής ενέργειας είναι τα εξής:

- Συλλογή Δεδομένων (Data Collection)
- Εξέταση (Examination)
- Ανάλυση (Analysis)
- Αναφορά (Reporting)



Εικόνα 1 : Μοντέλο Nist

Πηγή

Συλλογή Δεδομένων (Data Collection): η συλλογή δεδομένων αποτελεί μια από τις πρώτες κινήσεις, οι οποίες πραγματοποιούνται από τον ερευνητή, που ακολουθεί το μοντέλο του ινστιτούτου NIST, αναγνωρίζοντας έτσι τις πηγές από τις οποίες μπορεί να αποκτήσει δεδομένα και πληροφορίες, οι οποίες μπορεί να είναι και εκατοντάδες. Οι πιο κοινές που μπορεί να φανταστεί ο καθένας όπως είναι τα δίκτυα, οι εξυπηρετητές, οι φορητοί υπολογιστές και οι επιτραπέζιοι υπολογιστές. Μέσα από αυτά τα δεδομένα και τις ψηφιακές συσκευές, μπορεί ο ερευνητής να φτάσει στο σκληρό δίσκο του συστήματος καθώς και σε θύρες USB, από τις οποίες μπορεί να εξάγει πληροφορίες τις οποίες χρειάζεται να συλλέξει. Επιπλέον, οι κάρτες μνήμης, οι οπτικοί δίσκοι και τα USB sticks, περιέχουν σημαντικά δεδομένα καθώς θεωρούνται μέσα εξωτερικής αποθήκευσης.

Τα δεδομένα, εκτός από τις παραπάνω περιπτώσεις, υπάρχουν ακόμη στα αυτοκίνητα τελευταίας τεχνολογίας, στα έξυπνα ψυγεία, στις ψηφιακές κάμερες, στα iPod, στα mp3 Player και στα κινητά τηλέφωνα, όπως και γενικότερα σε συσκευές οι οποίες αποτελούν το Διαδίκτυο των Πραγμάτων. Κατά τη διάρκεια της έρευνας, ένας ερευνητής οφείλει μέσα από την προσωπική του εμπειρία να ξεχωρίσει οποιαδήποτε συσκευή έχει τη δυνατότητα να του προσφέρει πληροφορίες. Πολλά χρήσιμα δεδομένα

μπορούν να αποθηκευτούν ακόμη και στο δίκτυο ή στην μνήμη RAM του υπολογιστή, κάτι που σημαίνει πως όταν κλείσει ο υπολογιστής ή στην επόμενη επανεκκίνηση αυτά θα χαθούν, κάτι που τα κάνει να χρήζουν ιδιαίτερης προσοχής. Ο ερευνητής θα πρέπει επίσης να έχει στο νου του, κάποια σημεία τα οποία βρίσκονται εκτός του οργανισμού του οποίου ερευνάει.

Κάποια τέτοια σημεία μπορεί να είναι ο πάροχος του διαδικτύου τον οποίο χρησιμοποιεί ο οργανισμός από όπου μπορούν να αποκτηθούν τα logs, έτσι ώστε να μελετηθεί η δραστηριότητα στο διαδίκτυο. Για να γίνει κάτι τέτοιο, ωστόσο, είναι απαραίτητη η δικαστική εντολή. Για πρακτικούς λόγους, δεν είναι δυνατόν πάντα να ελεγχθούν οι πληροφορίες από τα μέσα τα οποία επιθυμεί οι ερευνητής. Θα πρέπει, λοιπόν, να είναι ικανός να ανακτήσει μόνος του κάποια δεδομένα τα οποία χρειάζεται. Καθώς η πρόληψη θεωρείται καλύτερη από τη θεραπεία, οι ειδικοί και οι εταιρείες οι οποίοι εργάζονται σε αυτές, μπορούν να λάβουν μέτρα πρόληψης, έτσι ώστε να συλλεχθούν χρήσιμα δεδομένα τα οποία θα είναι απαραίτητα σε μια ψηφιακή εγκληματολογική έρευνα, διευκολύνοντας τον ερευνητή σε περίπτωση στην οποία κριθεί απαραίτητο.

Υπάρχει η δυνατότητα της ρύθμισης καταγραφής των αλλαγών οι οποίες μπορεί να προκύψουν στις ρυθμίσεις ασφαλείας του συστήματος από τα περισσότερα γνωστά λειτουργικά συστήματα. Τα logs αυτά, στο μέλλον μπορεί να αποδειχθούν ιδιαίτερα σημαντικά για έναν οργανισμό. Βέβαια, όλα αυτά τα μέτρα θα πρέπει να είναι σχεδιασμένα βασισμένα στην ιδιωτικότητα του γενικότερου χρήστη ή και του εργαζόμενου. Από τη στιγμή που ερευνητής εντοπίσει τις πιθανές πηγές, το επόμενο βήμα είναι η απόκτηση των δεδομένων τα οποία θεωρεί απαραίτητα ώστε να τα μελετήσει. Το NIST διαχωρίζει αυτήν την διεργασία σε τρεις μικρότερες διεργασίες, οι οποίες παρουσιάζονται παρακάτω:

Σχεδιασμός: η διεργασία του σχεδιασμού αποτελεί ένα σημαντικό βήμα σύμφωνα με τις πιθανές πηγές, καθώς ο ερευνητής στο σημείο αυτό βασίζεται στα ψηφιακά μέσα τα οποία εντόπισε, ώστε να μπορέσει να τα διαχωρίσει και να τα κατηγοριοποιήσει. Λαμβάνονται υπόψη του οι παράγοντες για να μπορέσουν να τεθούν οι προτεραιότητες που έχουν να κάνουν με το πόσο χρήσιμα είναι τα δεδομένα τα οποία μπορεί να προσφέρει, καθώς και με την πιθανή αξία μιας πηγής. Σύμφωνα με την εμπειρία του

και ανάλογα με τη φύση του συμβάντος, ο ερευνητής θα μπορέσει να υπολογίσει το πόσο σημαντική είναι η κάθε πηγή.

Στη συνέχεια, ακολουθεί η ρευστότητα των δεδομένων. Η ρευστότητα μπορεί να έχει αποθηκευμένα δεδομένα τα οποία όμως αφού τερματιστεί ο υπολογιστής θα χαθούν. Συνεπώς, θα ήταν καλό η συλλογή των δεδομένων αυτών να βρίσκεται αρκετά ψηλά στη λίστα του ερευνητή και να υπάρχει προτίμησή τους έναντι των υπολοίπων δεδομένων. Ένας τρίτος παράγοντας είναι η προσπάθεια η οποία απαιτείται ώστε να συλλεχθούν οι πηγές, αφού θα είναι αρκετές και πιθανότατα θα πρέπει να εμπλακούν και άλλοι ειδικοί. Επιπλέον, απαιτείται προσπάθεια για να μπορέσει να αποκτήσει κάποιος πρόσβαση στα στοιχεία που κατέχει μόνο ο πάροχος του διαδικτύου, το οποίο μπορεί να είναι πολύ χρονοβόρα και μεγάλη διαδικασία.

Ανάκτηση Δεδομένων: προτείνεται, η ανάκτηση των δεδομένων να γίνεται με εργαλεία της ψηφιακής εγκληματολογίας ώστε να διατηρούνται στην αρχική μορφή τους. Η διαδικασία αυτή μπορεί να γίνει είτε μέσω δικτύου είτε τοπικά. Ένας από τους καλύτερους τρόπους είναι ο τοπικός καθώς και το σύστημα και οι πληροφορίες ελέγχονται καλύτερα.

Επαλήθευση των Δεδομένων: από τη στιγμή που θα ανακτηθούν τα δεδομένα, θεωρείται απαραίτητη η επαλήθευση της ακεραιότητας τους. Κάτι τέτοιο πρέπει να γίνεται για νομικούς λόγους, επιβεβαιώνοντας με αυτό τον τρόπο ότι ο ερευνητής δεν τροποποίησε ότι έχει συλλέξει. Σε αυτό το βήμα γίνεται η επαλήθευση με εργαλεία της ψηφιακής εγκληματολογίας, τα οποία συγκρίνουν γραφικά στοιχεία μέσα από τη συνάρτηση κατακερματισμού, με τα στοιχεία τα οποία απέκτησε ο ερευνητής όσο διήρκησε η έρευνα.

Εξέταση (Examination): η επόμενη φάση μετά τη φάση της συλλογής των δεδομένων είναι η εξέταση. Από τη διαδικασία αυτή, γίνεται η εξαγωγή των πληροφοριών για τα στοιχεία τα οποία αναμένουν να αξιολογηθούν. Συνήθως ο όγκος των δεδομένων είναι τεράστιος και έτσι θεωρείται δύσκολο να βρεθούν χειροκίνητα τα αποτελέσματα. Προσφέρεται λύση και σε αυτό το τμήμα από τα εργαλεία της ψηφιακής εγκληματολογίας όπως φαίνεται παρακάτω σύμφωνα με τους Zareen et al. (2013) ως εξής:

- Μέσα από την αναζήτηση με τη χρήση λέξεων κλειδιά οι οποίες μπορούν να αναγνωρίσουν κάποιο μοτίβο ή κείμενο.

- Με το φιλτράρισμα/διαχωρισμό δεδομένων βασισμένα σε διαφορετικούς τύπους δεδομένων όπως π.χ. γραφικά, βίντεο, ήχος, κείμενο κ.λπ.

Ανάλυση (Analysis): αφού ολοκληρωθεί και η εξέταση έρχεται η σειρά της ανάλυσης, στην οποία ο ερευνητής θα κάνει προσπάθεια εξαγωγής κάποιων συμπερασμάτων σύμφωνα με τις εξεταζόμενες πληροφορίες από την προηγούμενη φάση. Θεωρείται εξαιρετικά σημαντικό να γνωρίζει πότε συνέβη ένα γεγονός ή πότε δημιουργήθηκε ή τροποποιήθηκε ένας φάκελος. Με αυτό τον τρόπο θα μπορέσει να κάνει καλύτερη αναπαράσταση από την αρχή κάποιων γεγονότων στοχεύοντας στην ακόμα καλύτερη ανάλυση των γεγονότων αυτών.

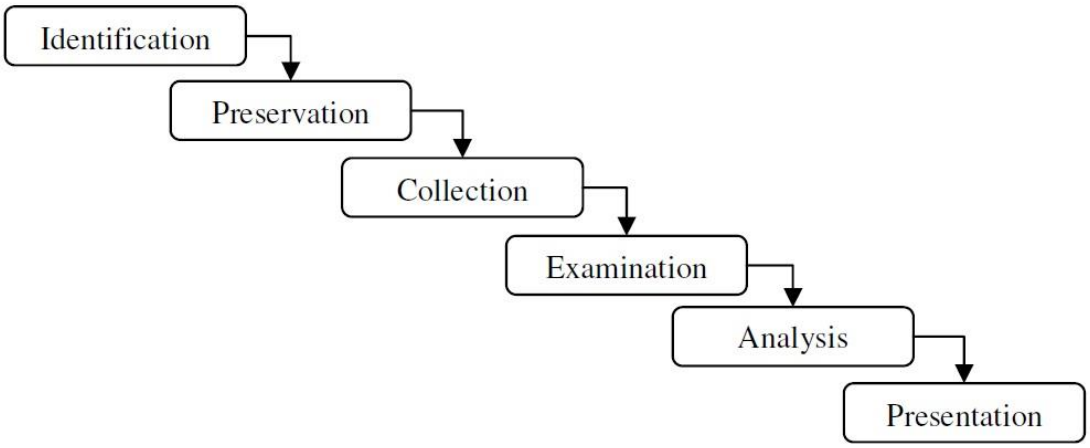
Αναφορά (Reporting): Η αναφορά των αποτελεσμάτων αποτελεί και την τελευταία φάση. Στο στάδιο αυτό, περιέχονται πληροφορίες για τα δεδομένα τα οποία απέκτησε ο ερευνητής και συνοδεύονται από την ώρα, την ημερομηνία και το μέρος που τα συνέλεξε, καθώς και τα εργαλεία και η μέθοδος τα οποία χρησιμοποιήθηκαν. Η αναφορά αυτή τις περισσότερες φορές γίνεται γραπτή και όταν ερευνητής κληθεί από το δικαστήριο προφορική. Στην περίπτωση που υπάρχουν παραπάνω από μία εξηγήσεις για ένα γεγονός, είναι στην ευθύνη του ερευνητή να αναφερθούν όλες οι εξηγήσεις, ενώ θα πρέπει να είναι πάντοτε λεπτομερής και ακριβής στην αναφορά των ευρημάτων του (Kent et al., 2006).

Επιπρόσθετα μοντέλα Ψηφιακής Εγκληματολογίας

Όπως προαναφέρθηκε, στη βιβλιογραφία συναντώνται πολλά μοντέλα εκτός από το μοντέλο του ινστιτούτου NIST, έτσι αξίζει να αναφερθούν κάποια από αυτά.

DFRWS Investigative Model

Οι ερευνητές χρησιμοποιούν συχνά το συγκεκριμένο μοντέλο, ενώ θεωρείται απόρροια του πρώτου συνεδρίου του DFRWS. Τα βήματα από τα οποία αποτελείται είναι τα εξής: Ταυτοποίηση (Identification), Διαφύλαξη (Preservation), Συλλογή (Collection), Εξέταση (Examination), Ανάλυση (Analysis) και Παρουσίαση (Presentation).



Εικόνα 2 : Μοντέλο DRFWS

Πηγή

Η ταυτοποίηση (identification) διακρίνεται στην πρώτη φάση, όπου εντοπίζεται το γεγονός, αναγνωρίζοντας κάποια ανωμαλία στο σύστημα και στην παρακολούθηση και ανάλυση ελέγχου του συστήματος. Στη συνέχεια ακολουθεί η διαφύλαξη (preservation) όπου διατηρείται η ακεραιότητα των στοιχείων τα οποία συλλέχθηκαν κατά τη διάρκεια της έρευνας. Η διαδικασία της ιεραρχίας των αποδεικτικών στοιχείων (chain of custody), εμφανίζεται στο στάδιο αυτό, σύμφωνα με την οποία καταγράφηκε σε ποια κατάσταση, σε ποιο χρονικό σημείο, πού θα μεταφερθεί αργότερα, από ποιο σημείο συλλέχθηκε ένα στοιχείο κ.λπ. αποτελεί ένα πολύ σημαντικό βήμα για τις υπόλοιπες φάσεις.

Η συλλογή (collection) ακολουθεί στη συνέχεια, στην οποία συλλέγονται οι πληροφορίες και τα δεδομένα με τη βοήθεια από συγκεκριμένα εργαλεία. Αμέσως μετά έρχεται η εξέταση (examination), η οποία αφορά την ιχνηλασιμότητα των πειστηρίων, την ανακάλυψη και εξαγωγή των κρυμμένων στοιχείων, καθώς ποιες τεχνικές φιλτραρίσματος και επικύρωσης τους. Σε όποιο σημείο υπάρχει εξόρυξη δεδομένων (datamining), με τη χρήση της ανάλυσης (analysis), πραγματοποιείται ένα χρονοδιάγραμμα, ενώ ταυτόχρονα περνά ο ερευνητής στο τελευταίο βήμα όπου είναι η παρουσίαση (presentation), στην οποία καταθέτει και τεκμηριώνει τα ευρήματά (Palmer, 2001).

Digital Forensics Investigation Model (DFIM)

Το 2011 οι Ademu et al. πρότειναν το DFIM, ένα μοντέλο το οποίο είναι χωρισμένο σε τέσσερα επίπεδα ενώ κάθε επίπεδο περιέχει επαναλαμβανόμενες διαδικασίες. Η προετοιμασία βρίσκεται στο πρώτο επίπεδο η οποία συμβαίνει καθ' όλη τη διάρκεια της έρευνας μέχρι το σημείο της παρουσίασης. Στο επίπεδο αυτό περικλείονται η επικοινωνία, η εξουσιοδότηση, η αναγνώριση και η προετοιμασία. Η φάση της αλληλεπίδρασης αποτελεί το δεύτερο επίπεδο όπου υπάρχουν οι κανόνες τεκμηρίωσης, διατήρησης και συλλογής. Στη φάση της ανοικοδόμησης περιλαμβάνονται οι κανόνες της ανάλυσης, οι διερευνητικές δοκιμές και οι κανόνες της εξέτασης. Το σύνολο αυτών οδηγούν στο τέταρτο επίπεδο, το οποίο αποτελείται από την παρουσίαση με κανόνες όπως είναι η αναφορά και το αποτέλεσμα.

Abstract Digital Forensic Model (ADFM)

Το 2002 οι Reith et al., αφού εξέτασαν διάφορα μοντέλα της ψηφιακής εγκληματολογίας, αποφάσισαν να τα χρησιμοποιήσουν ως πηγή έμπνευσης για την παρουσίαση του δικού τους μοντέλου Abstract Digital Forensic Model, το μοντέλο DFRWS. Οι δημιουργοί του μοντέλου αυτού, ισχυρίζονται πως το δικό τους μοντέλο έχει τη δυνατότητα βελτίωσης του μοντέλου DFRWS Investigative Model, αφού εμπνεύστηκε από αυτό. Αποτελείται από:

- Ταυτοποίηση (Identification): Αφορά στο καθορισμό του συμβάντος και στην αναγνώριση ενός περιστατικού. Θεωρείται μία σημαντική φάση καθώς επηρεάζει και άλλα βήματα.
- Προετοιμασία (Preparation): Περιλαμβάνει τη διαχείριση, τις τεχνικές εξουσιοδοτήσεις και την προετοιμασία εργαλείων.
- Στρατηγική Προσέγγισης (Strategy Approach): Για να μπορέσει να μεγιστοποιηθεί η συλλογή ατελών πειστηρίων από τη σκηνή του εγκλήματος, αναπτύσσεται μια προσέγγιση.
- Διατήρηση (Preservation): Εμπλέκει τη διατήρηση και ασφάλιση της κατάστασης των ψηφιακών και φυσικών αποδείξεων και την απομόνωση.
- Συλλογή (Collection): Αποτελεί το βήμα που καταγράφει τη φυσική σκηνή καθώς και την αντιγραφή των ψηφιακών στοιχείων με τη χρήση αποδεκτών και τυποποιημένων διαδικασιών.

- Εξέταση (Examination): Αποτελεί μια εις βάθος αναζήτηση για αποδείξεις σχετιζόμενες με το έγκλημα. Η εστίαση βρίσκεται στον εντοπισμό και την ταυτοποίηση των πιθανών πειστηρίων.
- Ανάλυση (Analysis): Στο στάδιο αυτό αποφασίζεται το ποια είναι η αποδεικτική αξία και πόσο σημαντικό είναι το εξεταζόμενο στοιχείο.
- Παρουσίαση (Presentation): Επεξήγηση και σύνοψη.
- Επιστροφή Αποδεικτικών Στοιχείων (Returning Evidence): Σε αυτό το στάδιο πραγματοποιείται επιστροφή της ψηφιακής και φυσικής περιουσίας στον ιδιοκτήτη.

The Integrated Digital Investigation Process Model (IDIP)

Το 2003, οι Carrier and Spafford, πρότειναν ένα μοντέλο ψηφιακής έρευνας το οποίο παρέχει ψηφιακά και φυσικά πειστήρια σε μια ενοποιημένη διαδικασία. Ο διαχωρισμός της έρευνας στον ψηφιακό και φυσικό τόπο του εγκλήματος, αποτελεί τα βασικά χαρακτηριστικά του μοντέλου αυτού. Όσα αντικείμενα βρίσκονται στη σκηνή, χειρίζονται από τον ερευνητή ως φυσικές αποδείξεις με τη χρήση παραδοσιακών μοντέλων έρευνας. Στην περίπτωση που τα αντικείμενα αυτά αποτελούν πηγές ψηφιακών αποδείξεων, η εξέτασή τους γίνεται σύμφωνα με την ψηφιακή σκηνή του εγκλήματος. Ο διαχωρισμός του μοντέλου αυτού γίνεται σε 17 φάσεις και 5 ομάδες.

A Model for Hybrid Evidence Investigation

Το 2013, οι Vlachopoulos et al., πρότειναν ένα μοντέλο το οποίο έχει δυνατότητα εφαρμογής σε περιπτώσεις όπου τα πειστήρια είναι και ψηφιακά και φυσικά. Για το λόγο αυτό ονομάστηκε υβριδικό. Μπορεί φυσικά να χρησιμοποιηθεί και σε διάφορες περιπτώσεις όπου υπάρχουν είτε φυσικές είτε ψηφιακές αποδείξεις. Το μοντέλο αποτελείται από 4 φάσεις και 12 μικρότερες.

Φάση πρώτη: Προετοιμασία (Preparation)

- Ειδοποίηση (Notification): Έρχεται η ειδοποίηση ότι διαπράχθηκε ένα έγκλημα.
- Εξουσιοδότηση (Authorization): η παροχή της γίνεται από τον οργανισμό ο οποίος ορίστηκε για να διεξάγει την έρευνα.
- Προετοιμασία (Preparation): Περιλαμβάνει την διαθεσιμότητα του προσωπικού που θα διεξάγει την έρευνα και του εξοπλισμού.

Φάση δεύτερη: Έρευνα του τόπου του εγκλήματος (Crime scene investigation)

- Διατήρηση (Preservation): Ο πρώτος ο οποίος θα φτάσει στον τόπο του εγκλήματος θεωρείται υπεύθυνος για την οργάνωση, για παράδειγμα ποιος μπορεί να πλησιάζει και ποιος όχι και την ασφάλεια της σκηνής.
- Ταυτοποίηση (Identification): Στο σημείο αυτό γίνεται από τους ειδικούς η αναγνώριση των πιθανών πειστηρίων.
- Συλλογή – Εξέταση (Collection-Examination): Ο ερευνητής ξεκινά τη συλλογή στοιχείων τα οποία σχετίζονται με το έγκλημα. Αυτά μπορεί να είναι είτε φυσικά όπως, για παράδειγμα, τα δακτυλικά αποτυπώματα, είτε και ψηφιακά. Είναι ακόμη δυνατόν να διεξαχθεί εξέταση, με τη διαφορά όμως ότι δε θα είναι με την εργαστηριακού επιπέδου. Δεν πρόκειται δηλαδή να εφαρμοστεί κανονική εξέταση των στοιχείων.
- Μεταφορά (Transportation): Αν και θεωρείται ως δευτερεύουσα διαδικασία η μεταφορά, οι Vlachopoulos et al. την θεωρούν σημαντική αναφορικά με τα μέτρα προστασίας των αποδεικτικών τα οποία οφείλει να λάβει κάποιος κατά την μεταφορά.

Φάση τρίτη: Εργαστηριακή εξέταση (Laboratory examination)

- Εξέταση (Examination): Πρόκειται για τη διαδικασία εξέτασης των στοιχείων που αποκτήθηκαν στο εργαστήριο, και που μπορούν να δώσουν απαντήσεις για την έρευνα.
- Αποθήκευση (Storage): Τα στοιχεία, μετά το πέρας της εξέτασης, θα πρέπει να αποθηκευτούν σε ασφαλή χώρο.
- Αναφορά (Report): Η αναφορά αποτελεί μια σημαντική διεργασία περιέχεται καθώς σε αυτήν περιέχεται το αποτέλεσμα της εργαστηριακής εξέτασης.

Φάση τέταρτη: Συμπέρασμα (Conclusion)

- Ανακατασκευή (Reconstruction): Είναι ευθύνη του ερευνητή παρουσιάζει τα γεγονότα αξιολογώντας τα στοιχεία η ανακατασκευή της σκηνής.
- Διάχυση (Dissemination): Αποτελεί τη τελευταία διαδικασία του μοντέλου. Στη διάχυση πραγματοποιείται μια λεπτομερής ανασκόπηση της έρευνας, ώστε να διαχυθούν οι αποκτώμενες γνώσεις, ενώ υπάρχει και η περίπτωση χρησιμοποίησής τους σε επόμενες παρόμοιες περιπτώσεις.

Προκλήσεις στην Ψηφιακή Εγκληματολογία

Όσο εξελίσσεται όλο και περισσότερο η τεχνολογία, η επιστήμη της ψηφιακής εγκληματολογίας θα υπολογίζεται όλο και πιο χρήσιμη για να επιλυθούν τέτοιες υποθέσεις. Καθώς οι πηγές είναι ποικιλόμορφες, θα απαιτείται να αναλυθούν από τους ερευνητές. Οι δυσκολίες και οι προκλήσεις σαφώς είναι πολλές, υπήρχαν και θα συνεχίσουν να υπάρχουν. Στην ενότητα αυτή παρουσιάζονται οι πιο σημαντικές σύμφωνα με τους Karie και Venter (2015).

Κρυπτογράφηση: όσο προοδεύουν οι τεχνολογίες της επικοινωνίας όπως είναι το διαδίκτυο και τα λογισμικά κρυπτογράφησης, συμπεραίνεται ότι η εξέλιξή τους γίνεται ακόμη πιο περίπλοκη από ότι ήταν. Κάτι τέτοιο μπορεί να προκαλέσει πολλές δυσκολίες στην καθημερινότητα ενός ερευνητή καθώς θα πρέπει να πραγματοποιήσει μια αποκρυπτογράφηση.

Μεγάλος όγκος δεδομένων: σημειώθηκε αρκετά μεγάλη αύξηση των μέσων αποθήκευσης των δεδομένων τόσο στα εταιρικά συστήματα όσο και στα προσωπικά. Συνεπώς, υπάρχει η δυνατότητα από κάθε χρήστη να αποθηκεύει ένα τεράστιο όγκο. Ο χρόνος ο οποίος απαιτείται για να αναλυθούν και να αποκτηθούν τα στοιχεία, αποτελεί συνέπεια της εξέλιξης αυτής.

Ασυμβατότητα μεταξύ των εργαλείων: καθώς ενδέχεται πολλά εργαλεία να έχουν διαφορετική λειτουργία, πολυπλοκότητα ή και κόστος, πολλές φορές δεν είναι εύκολο να συνεργαστούν μεταξύ τους. Κάτι τέτοιο συμβαίνει καθώς δεν είναι φτιαγμένα όλα τα εργαλεία για τον ίδιο σκοπό. Κάποια προσφέρουν μια μεγάλη γκάμα λειτουργιών ενώ κάποια άλλα μια μικρότερη.

Αστάθεια των ψηφιακών πειστηρίων: τα στοιχεία έχουν ένα από τα ιδιαίτερα χαρακτηριστικά να είναι εύθραυστα όπως αναφέρθηκε και προηγουμένως. Κάποια λειτουργία όπως είναι η απώλεια της μπαταρίας, η επανεκκίνηση ή η ενεργοποίηση, μπορούν να τα καταστρέψουν. Έρχεται λοιπόν στην αντίληψη, ότι κάθε ερευνητής, θα αντιμετωπίσει μια αρκετά σοβαρή πρόκληση στην εκκίνηση της έρευνας ενός περιστατικού.

Περιορισμοί Bandwidth: σε κάποιες περιπτώσεις στις οποίες μπορεί η αναμετάδοση των στοιχείων να είναι εξαιτίας του δικτύου πιο αργή, καθώς η υπολογιστική μηχανή η οποία περιέχει τα στοιχεία και καλείται να αντιγράψει ο ερευνητής προς το δικό του

μηχάνημα για ανάλυση, θεωρείται ήδη σε λειτουργία, μια ενδεχόμενη απενεργοποίηση θα μπορούσε να προκαλέσει ανεπανόρθωτες απώλειες και προβλήματα.

Περιορισμένη διάρκεια ζωής ψηφιακών μέσων: πλέον η ικανότητα η οποία έχουν όλα τα ψηφιακά μέσα στην αποθήκευση, όπως αναφέρθηκε προηγουμένως, έφτασε σε αρκετά μεγάλο βαθμό. Μια μακροχρόνια αποθήκευση, ωστόσο, θα πρέπει να θεωρείται δεδομένη. Αν απολεσθεί έστω και ένα bit, υπάρχει πιθανότητα να προκληθεί ολική καταστροφή των δεδομένων.

Επιτήδευση των ψηφιακών εγκλημάτων: οι ερευνητές, σύμφωνα με την ACPO, βρίσκονται συχνά αντιμέτωποι με κάποια νέα εργαλεία και λογισμικά τα οποία χρησιμοποιούν οι hackers. Κάτι τέτοιο μπορεί να προκαλέσει τις έρευνες να είναι ακόμη πιο χρονοβόρες.

Αναπτυσσόμενες Τεχνολογίες και Συσκευές: συνεχώς ξεπροβάλλουν όλα εξελισσόμενες και νέες τεχνολογίες με όλο και μεγαλύτερη ταχύτητα. Όταν υπάρχει λοιπόν ένα καινούργιο σύστημα, στην αντιμετώπιση του είτε σε επίπεδο συσκευής είτε σε επίπεδο λογισμικού, το οποίο ο ερευνητής δεν έχει ξανασυναντήσει, θα πρέπει να προσαρμοστούν τα εργαλεία του, καθώς και ο τρόπος προσέγγισης σύμφωνα με αυτά.

Περιορισμένο παράθυρο για συλλογή ψηφιακών πειστηρίων: καθώς συλλέγονται τα πειστήρια, θεωρείται σημαντικό για έναν ερευνητή να αντιληφθεί ποια στοιχεία θα πρέπει να αποκτήσει πρώτα. Ειδικά στην περίπτωση που ο χρόνος πιέζει, οι αποφάσεις πρέπει να παίρνονται πιο γρήγορα.

Τα Antiforensics: η δημιουργία της συγκεκριμένης συλλογής εργαλείων έγινε έχοντας στόχο την εμπόδιση του έργου των εργαλείων της ψηφιακής εγκληματολογίας. Κάτι τέτοιο πρακτικά έχει ως αποτέλεσμα τη δυσκολία του ερευνητή, καθώς τα εργαλεία αυτά έχουν τη δυνατότητα να διαταράξουν τις πληροφορίες.

Απόκτηση πληροφοριών από συσκευές διαφορετικές των ηλεκτρονικών υπολογιστών: το να αποκτηθούν στοιχεία από υπολογιστές θεωρείται ίσως η ευκολότερη διαδικασία συγκριτικά με την απόκτηση από έξυπνες συσκευές, κινητά τηλέφωνα, wearables καθώς και γενικότερα από αντικείμενα του διαδικτύου των πραγμάτων.

Προκλήσεις σχετιζόμενες με την τεχνολογία του "νέφους" (cloud): Οι τεχνολογίες cloud, βοήθησαν τις επιχειρήσεις στο έπακρο καθώς εξοικονομούν χρήματα για εξοπλισμό. Έχουν βοηθήσει στο έπακρο τις επιχειρήσεις, διότι τους εξοικονομούν

χρήματα για εξοπλισμό. Η θέση του ερευνητή, είναι να υπολογίσει την ετερογένεια και τη δικαιοδοσία του νέφους στην περίπτωση που χρησιμοποιήσει τέτοιες υπηρεσίες, καθώς μπορεί να προκαλέσουν εμπόδια στην έρευνα.

Εργαλεία Ψηφιακής Εγκληματολογίας

Τα εργαλεία αποτελούν ένα σημαντικό κεφάλαιο στην ψηφιακή εγκληματολογία, καθώς αποτελούν μια σημαντική μέριμνα του ερευνητή κατά τη διάρκεια της έρευνας. Τα εργαλεία αυτά μπορεί να είναι είτε ανοιχτού κώδικα και δωρεάν είτε εμπορικά. Η επιλογή τους είναι καλό να γίνεται σύμφωνα με την περίπτωση στην οποία εργάζεται ο ειδικός. Έχει δημιουργηθεί από το ινστιτούτο NIST (NIST, n.d.) μια βάση, η οποία περιέχει σχεδόν όλα τα εργαλεία τα οποία κυκλοφορούν στην αγορά. Αυτά τα εργαλεία διαχωρίστηκαν βασισμένα στις λειτουργίες τους. Παρακάτω αναφέρονται επιγραμματικά οι κατηγορίες οι οποίες εμφανίζονται στην ιστοσελίδα :

- Cloud services
- Memory capture and analysis
- Database forensics
- Mobile device acquisition, analysis & triage
- Deleted file recovery
- P2P analysis
- Disk imaging
- Password recovery
- Drone forensics
- Remote capabilities/ Remote forensics
- Email parsing
- Social media
- File Carving
- Software write block
- Forensics Boot Environment
- Steganalysis
- Forensics tool suite
- String search
- GPS forensics
- Video analytics

- Hardware write block
- VoIP forensics
- Hash analysis
- Web browser forensics
- Image analysis
- WiFi forensics
- Infotainment & vehicle forensics
- Windows registry analysis
- Instant Messenger
- Media sensitization/ drive re-use

Φαίνεται, λοιπόν, ότι είναι αρκετά μεγάλη πληθώρα των εργαλείων. Με τη χρήση αυτών, ο ερευνητής θα βρίσκεται σε θέση ανακάλυψης των ψηφιακών πειστηρίων, τα οποία θα μπορέσουν να οδηγήσουν σε ασφαλή συμπεράσματα. Παρακάτω αναφέρονται τα πιο διαδεδομένα εργαλεία.

Forensic Toolkit (FTK): Το FTK είναι ένα εργαλείο το οποίο δημιουργήθηκε από την εταιρεία AccessData. Είναι εύκολο, σταθερό και γρήγορο στην λειτουργία του χάρη στο περιβάλλον του. Καθώς χρησιμοποιεί κατανεμημένη επεξεργασία, μπορεί να αξιοποιήσει πλήρως τους πολλούς πυρήνες των υπολογιστών. Με αυτό τον τρόπο εκμεταλλεύεται πλήρως τις δυνατότητες που μπορεί να έχει ένα σύστημα για να προσφέρει καλύτερο αποτέλεσμα. Το FTK παρέχει indexing και ολοκληρωμένη επεξεργασία, ενώ ακολουθούν η αναζήτηση και το φιλτράρισμα τα οποία γίνονται γρηγορότερα. Βασίζεται σε μια βάση δεδομένων, ενώ χρησιμοποιεί και μια βάση η οποία έχει εύκολη πρόσβαση από τις ομάδες οι οποίες εργάζονται. Τα δεδομένα αποθηκεύονται όλα στην ίδια βάση και είναι ασφαλή, και έτσι μπορούν όλοι να έχουν πρόσβαση στα ίδια σημεία. Για να μπορέσουν, λοιπόν, να δημιουργηθούν πολλά σύνολα δεδομένων, με τη χρήση αυτού του τρόπου υπάρχει μείωση της πολυπλοκότητας και του κόστους. Το FTK είναι εμπορικής χρήσης, ενώ η αξία αγοράς του ανέρχεται στα $3.995 για την τελευταία έκδοση που είναι η Forensics Toolkit 6.2. (Accessdata, n.d.)

Digital Forensics Framework (DFF): αποτελεί ένα λογισμικό ανοιχτού κώδικα το οποίο είναι γραμμένο σε Python C++. Το DFF προσφέρει το αναπτυσσόμενο στο PyQt4 1 γραφικό περιβάλλον. Η χρήση του είναι κυρίως για την αποκάλυψη, διατήρηση και

συλλογή ψηφιακών πειστηρίων χωρίς να κινδυνεύσουν πληροφορίες και υπολογιστικά συστήματα. Ο χρήστης μπορεί, επιπρόσθετα, να κάνει ανάκτηση κρυφών ή ακόμα και διαγραμμένων αρχείων. υπάρχουν 3 εκδόσεις : η DFF που είναι δωρεάν, η DFF Live και η DFF. Οι δύο τελευταίες είναι εμπορικής χρήσης. Η χρήση τους μπορεί να γίνει σε λειτουργικά συστήματα Windows και Linux (Digital Forensics Framework, n.d.)

The Sleuth Kit: αποτελεί ένα λογισμικό ανοιχτού κώδικα το οποίο είναι γραμμένο σε Perl και C. Το Sleuth Kit είναι μια συλλογή και βιβλιοθήκη από εντολές οι οποίες δίνουν τη δυνατότητα εξερεύνησης του δίσκου στο χρήστη. Μία από τις βασικές λειτουργίες του προγράμματος, επιτρέπει να αναλυθεί μεγάλος όγκος στοιχείων και δεδομένων του συστήματος. Μπορεί επίσης να ενσωματωθεί και σε μεγαλύτερα εργαλεία ψηφιακής εγκληματολογίας οδηγώντας κατευθείαν στην εύρεση πειστηρίων. Μια πλατφόρμα η οποία προσφέρει γραφικό περιβάλλον για το Sleuth Kit παρέχοντας αναζήτηση λέξεων κλειδιά, διαχείριση περιπτώσεων καθώς και πολλές άλλες αυτόματες λειτουργίες, είναι το Autopsy. Χρησιμοποιείται στα λειτουργικά συστήματα Windows και Linux.

Blacklight: Το Blacklight αποτελεί ένα εργαλείο ανάλυσης το οποίο επιτρέπει στον ερευνητή να εκτελέσει γρήγορα μια ψηφιακή έρευνα. Η χρήση του μπορεί να γίνει σε συσκευές οι οποίες έχουν εγκατεστημένο λειτουργικό σύστημα MacOS, συσκευές iOS αλλά και σε συστήματα με Windows. Μπορούν να επεκταθούν οι δυνατότητες του ακόμα και στα μέσα κοινωνικής δικτύωσης και στις υπηρεσίες ανταλλαγής μηνυμάτων. Το κόστος του για έναν χρήστη ανέρχεται στα $3400. (BlackbagtechTechnologies, n.d.)

XRY: Το XRY είναι ένα λογισμικό κατασκευασμένο από την εταιρεία MSAB. Με το λογισμικό αυτό, δίνεται στο χρήστη η δυνατότητα εξαγωγής πληροφοριών και δεδομένων, τα οποία μπορούν να χρησιμοποιηθούν ως αποδείξεις από συσκευές οι οποίες μπορεί να είναι μόντεμ, tablet, GPS και έξυπνα κινητά τηλέφωνα. Η τιμή για την αγορά του είναι στα $7990 και χρησιμοποιείται για λειτουργικά συστήματα Windows (MSAB, n.d.)

Digital Evidence & Forensic Toolkit (DEFT): Το DEFT αποτελεί μια διανομή Linux. Το πρόγραμμα σύμφωνα με τον κατασκευαστή του αποτελείται από τη σουίτα Digital Advanced Response Toolkit (DART) και από GNU/Linux. Μπορεί να αποτελέσει μια

λύση η οποία βρίσκει εφαρμογή ακόμα και σε νομικές υπηρεσίες όπου διανέμεται δωρεάν (deft, n.d.).

Internet Evidence Finder (IEF): Το συγκεκριμένο εργαλείο κατασκευάζεται από την εταιρεία magnetforensics. Η έκθεση αυτού του γραφικού του περιβάλλοντος θεωρείται φιλική προς τον χρήστη. Η ικανότητα του IEF έχει να κάνει με την παρουσίαση, ανάλυση και εύρεση πειστηρίων από έξυπνα κινητά τηλέφωνα, υπολογιστές ή ακόμη και tablet. Τα στοιχεία αυτά μπορεί να είναι είτε από μέσα κοινωνικής δικτύωσης, είτε από μηνύματα ή ακόμα και από πολλές άλλες πηγές. Το κόστος του ανέρχεται στα $1700 για ένα χρήστη και υποστηρίζει τα λειτουργικά συστήματα Windows, Linux, MacOSX (Magnetforensics, n.d.).

Sans Investigative Forensics Toolkit (SIFT): Το SIFT είναι φτιαγμένο βασισμένο στο Ubuntu. Η κυρίως χρήση του είναι δωρεάν, ωστόσο κάποια plug-in κοστίζουν. Είναι πολλαπλών χρήσεων, ενώ συνοδεύεται από όλα τα εργαλεία τα οποία μπορεί να χρειαστεί κάποιος ερευνητής (Digital Forensics, n.d.).

EnCase: Το EnCase αποτελεί στο είδος του ένα από τα πιο διαδεδομένα λογισμικά. Με τη χρήση του εργαλείου αυτού, ο ερευνητής μπορεί να συλλέξει πληροφορίες από διάφορες ηλεκτρονικές συσκευές. Το περιβάλλον χρήστη είναι φιλικό, ενώ μπορεί να αναπαράγει αυτόματα την αναφορά. Μπορεί επίσης να αποκρυπτογραφήσει στοιχεία τα οποία θα φανούν χρήσιμα όσο διαρκεί μια έρευνα. Το κόστος για μία άδεια κοστίζει $3594 (EncaseForensic, n.d.).

Computer Aided Investigative Environment (CAINE): Αποτελεί μια δωρεάν διανομή Linux, είναι ένα λογισμικό ανοιχτού κώδικα, ενώ έχει φιλικό προς το χρήστη εργαλεία και περιβάλλον (CAINE, n.d.).

X-Ways forensics: Υποστηρίζει μόνο τα λειτουργικά συστήματα Windows. Μία από τις δυνατότητες του είναι ότι μπορεί να βρει διαγραμμένους φακέλους. Αναφορικά με την εγκατάσταση, οι απαιτήσεις του είναι φυσιολογικές χωρίς να απαιτείται κάτι ιδιαίτερο από άποψη υλικού. Η εκτέλεσή του γίνεται απλά από μία συσκευή USB χωρίς να υπάρξει εγκατάσταση στην περίπτωση που ο χρήστης δεν την επιθυμεί. Η τιμή για μια άδεια χρήσης κοστίζει περίπου $1065. (X-Ways, n.d.)

3.2 Μεθοδολογία Ψηφιακής Δικανικής

Απόκτηση (Acquisition)

Αφορά τη συλλογή των υπό εξέταση ψηφιακών μέσων. Αυτά, ανάλογα με το είδος που έχει κάθε έρευνα, μπορεί να είναι είτε μεμονωμένα αρχεία, chip από φορητές συσκευές, κινητά τηλέφωνα, κάρτες αποθήκευσης από φωτογραφικές μηχανές, οπτικά μέσα και σκληροί δίσκοι. Από τη στιγμή που θα γίνει συλλογή των μέσων αυτών, δημιουργείται ένα ακριβές τους αντίγραφο (Forensic duplicate) το οποίο με τα κατάλληλα εργαλεία λογισμικού υλικού, χρησιμοποιείται συνήθως μαζί με μία συσκευή write-blocking, όπου αποτρέπονται τυχόν τροποποιήσεις στα αρχικά δεδομένα. Συχνά η διαδικασία αυτή ονομάζεται και imaging.

Σημειώνεται ότι όποια εξέταση πραγματοποιείται όχι επί του πρωτοτύπου πειστηρίου αλλά επί του αντιγράφου, θα πρέπει να γίνεται ιδιαίτερα προσεκτικά, καθώς θα πρέπει να γίνει αποφυγή οποιασδήποτε μεταβολής στα αυθεντικά ψηφιακά δεδομένα, κάτι που θα καθιστούσε την έρευνα αναξιόπιστη να σταθεί σε μία δικαστική διαμάχη ως αποδεικτικό στοιχείο. Το αρχικό ψηφιακό μέσο τοποθετείται στη συνέχεια σε ένα ασφαλές μέρος για την αποφυγή αλλοιώσεων. Τέλος, για το αντίγραφο το οποίο έχει αποκτηθεί, καθώς και για το αρχικό ψηφιακό μέσο, υπολογίζεται μια κρυπτογραφική σύνοψη χρησιμοποιώντας, για παράδειγμα, τις συναρτήσεις MD5, SHA-1 και SHA-256. Γίνεται έπειτα σύγκριση των δύο τιμών που προκύπτουν, έτσι ώστε να είναι ακριβές το αντίγραφο. Με στόχο την επιβεβαίωση ότι δεν έχουν υποστεί αλλοίωση στα δεδομένα, υπολογίζεται ξανά η σύνοψη του ψηφιακού μέσου για κάποια κρίσιμα σημεία της ανάλυσης.

Ανάλυση (Analysis)

Αποτελεί στην ουσία την πραγματική εξέταση του ψηφιακού μέσου. Το περιεχόμενο των ψηφιακών αντιγράφων μετά την απόκτηση του, αναλύεται σκοπεύοντας να βρεθούν αποδείξεις που είτε αντικρούουν είτε υποστηρίζουν μια υπόθεση ή στοιχεία, τα οποία υποδεικνύουν αλλοιώσεις έχοντας στόχο την απόκρυψη δεδομένων. Το International Journal of Digital Evidence το 2002, έκανε αναφορά στο συγκεκριμένο στάδιο ως μια συστηματική αναζήτηση στοιχείων σε βάθος, τα οποία σχετίζονται με το υποπτευόμενο έγκλημα. Σε αντίθεση, το 2005 ο Brian Carrier, έκανε περιγραφή μιας πιο απαιτητικής διαδικασίας, όπου τα προφανή δεδομένα πρώτα προσδιορίζονται και μετά πραγματοποιούνται με πιο διεξοδικές αναζητήσεις, έτσι ώστε να υπάρξει κάλυψη των διαφόρων κενών (Carrier, 2005). Όσο διαρκεί μια ανάλυση, ο ερευνητής ανακτά συνήθως αποδεικτικό υλικό με τη χρήση πολλών διαφορετικών μεθοδολογιών και

εργαλείων ξεκινώντας συνήθως ανάλογα και με το είδος της έρευνας, από τις πιο συνηθισμένες τοποθεσίες.

Αν μελετάται, για παράδειγμα, η περιήγηση στον ιστό ενός χρήστη, η έρευνα θα ξεκινήσει από την προσωρινή μνήμη του περιηγητή (web browser cache), από τους σελιδοδείκτες και το ιστορικό του. Για να μπορέσουν να βοηθήσουν στην ανάκτηση και προβολή δεδομένων, οι εξεταστές χρησιμοποιούν ειδικά εργαλεία. Είναι διαφορετικό το είδος των δεδομένων το οποίο ανακτάται ανάλογα με την έρευνα, καθώς και με παραδείγματα τα οποία αποτελούνται από αρχεία κειμένου, εικόνες, ιστορικό διαδικτύου, logs συνομιλιών και e-email. Η ανάκτηση των αποδείξεων αυτών, μπορεί να γίνει όχι μόνο μέσα από τον ελεύθερο χώρο ή από τα αρχεία της λανθάνουσας μνήμης του λειτουργικού συστήματος (cache files), αλλά και από τον προσβάσιμο χώρο ενός ψηφιακού μέσου. Από τη στιγμή που γίνει ανάκτηση των στοιχείων, αναλύονται οι πληροφορίες έχοντας στόχο την αναπαράσταση ενεργειών ή γεγονότων καταλήγοντας σε συμπεράσματα.

Παρουσίαση (presentation)

Αποτελεί τη διαδικασία σύμφωνα με την οποία ένας εξεταστής μπορεί να μοιραστεί με τους ενδιαφερόμενους τα αποτελέσματα της ανάλυσης του. Κάτι τέτοιο μπορεί να περιλαμβάνει τη δημιουργία αναφοράς με τα ακολουθούμενα βήματα και τα συλλεγμένα στοιχεία καθώς και την ερμηνεία τους. Η φάση της παρουσίασης αρκετές φορές μπορεί να περιλαμβάνει και την υπεράσπιση των ευρημάτων από τον εξεταστή.

3.3 Κλάδοι Ψηφιακής Δικανικής

Ανάλογα με το εμπλεκόμενο είδος της εκάστοτε συσκευής, μπορεί να χωριστεί και η ψηφιακή δικανική σε διάφορους κλάδους. Οι κλάδοι αυτοί είναι η δικανική βάσεων δεδομένων, η δικανική κινητών συσκευών, η δικανική δικτύων και η δικανική υπολογιστών.

3.3.1 Δικανική δικτύων

Η διαδικασία ανάλυσης και ανάκτησης πληροφοριών από ένα ή περισσότερα δίκτυα υπολογιστών, στα οποία υπάρχει η υποψία ότι προσπελάστηκαν ή εκτέθηκαν από μη εξουσιοδοτημένους χρήστες, ορίζει τη δικανική δικτύων. Στις πληροφορίες αυτές περιλαμβάνονται τα φορτία δεδομένων και η κίνηση του δικτύου. Επιτρέπεται στους αναλυτές η επεξεργασία της εγκυρότητας των υποθέσεων, εξηγώντας τα αίτια και τις

συνθήκες της ενέργειας την οποία ερευνούν και το αν είναι δυνατή η παροχή αποδεικτικών στοιχείων τα οποία υποστηρίζουν την αστική ή την ποινική ευθύνη. Παρόλο που η δικανική δικτύων χρησιμοποιείται για τον προσδιορισμό του πώς έγινε κάποια παραβίαση ασφαλείας, κρίνεται απαραίτητο να ληφθούν μέτρα, έτσι ώστε να γίνει ισχυρότερη η ασφάλεια του δικτύου αποφεύγοντας έτσι τυχόν εισβολές.

Τέτοια μέτρα αποτελούν η ενημέρωση και εκπαίδευση του προσωπικού, η προστασία του δικτύου, η ισχυροποίηση μεμονωμένων υπολογιστών και η διαρκής ενημέρωση του λογισμικού. Επίσης, πρόκληση αποτελεί η ανίχνευση από συμβάντα ασφαλείας, καθώς οι εξελιγμένες επιθέσεις έχουν τη δυνατότητα να αλλάξουν πρόσωπο ώστε να δείχνουν φυσιολογικές δικτυακές δραστηριότητες. Για να είναι πιο αποτελεσματικός ο εντοπισμός ύποπτης δραστηριότητας σε ένα συγκεκριμένο δίκτυο, θεωρείται σημαντική η απόκτηση μιας εικόνας για το τι αποτελεί φυσιολογική δραστηριότητα, η κίνηση στο δίκτυο αυτό, και αν η απόκτηση της εικόνας αυτής μπορεί να γίνει μέσα από τα logs του δικτύου. Οι ειδοποιήσεις του λογισμικού προστασίας από ανωμαλίες στη δικτυακή κίνηση, μη φυσιολογική διαδικτυακή συνδεσιμότητα και οι ειδοποιήσεις του λογισμικού προστασίας από ιούς, αποτελούν πιθανά σημάδια επιθέσεων.

Αξίζει να αναφερθούν κάποιες απροσδόκητες προκλήσεις οι οποίες παρουσιάζονται καθώς διαχειρίζονται ψηφιακά αποδεικτικά ψηφία σε ένα δίκτυο, αντίθετα με την ανάκτηση στοιχείων από την επεξεργασία σκληρών δίσκων όπου θεωρείται μια καλά ορισμένη διαδικασία. Στα δικτυωμένα συστήματα, τα δεδομένα θεωρούνται μεταβλητά και δυναμικά κάνοντας έτσι δύσκολο να ληφθεί ένα στιγμιότυπο στο δίκτυο για μια δεδομένη χρονική στιγμή. Επιπρόσθετα, αντίθετα με τους, για παράδειγμα, προσωπικούς υπολογιστές, δεν θεωρείται εφικτό να κλείσει ένα δίκτυο, καθώς θα χαθούν τα περισσότερα αποδεικτικά στοιχεία τα οποία είναι αποθηκευμένα σε αυτό, αλλά και ο ερευνητής τις περισσότερες φορές έχει ευθύνη της εξασφάλισης των στοιχείων χωρίς την αποδιοργάνωση των επιχειρηματικών δραστηριοτήτων οι οποίες είναι βασισμένες στο δίκτυο αυτό.

Σε αντίθεση με τα εγκλήματα του φυσικού περιβάλλοντος, τα ψηφιακά εγκλήματα μπορούν να γίνουν σε διαφορετικά σημεία του δικτύου σε οποιαδήποτε χρονική στιγμή. Συνεπώς, κάποια αποδεικτικά στοιχεία μπορεί να έχουν διασπαρθεί σε διάφορες συσκευές ή μηχανήματα καθώς και σε διαφορετικές γεωγραφικές περιοχές, κάνοντας έτσι δυσκολότερη την απομόνωση του εγκλήματος. Ένα από τα

πλεονεκτήματα βέβαια το οποίο προκύπτει από τη διασπορά αυτή, είναι η δυσκολία στο να καταστραφούν τα αποδεικτικά στοιχεία. Σε περίπτωση που καταστραφούν τα στοιχεία σε ένα υπολογιστικό σύστημα, μπορεί να βρεθεί ένα αντίγραφό τους σε διάφορους υπολογιστές στο διαδίκτυο.

3.3.2 Δικανική κινητών συσκευών

Η δικανική κινητών συσκευών αποτελεί ακόμη ένα κλάδο της ψηφιακής δικανικής, ο οποίος είναι σχετιζόμενος με το να ανακτηθούν ψηφιακά αποδεικτικά στοιχεία ή δεδομένα από μια κινητή συσκευή. Στον όρο αυτό, δεν περιέχονται μόνο τα κινητά τηλέφωνα, αλλά κάθε ψηφιακή συσκευή η οποία έχει ταυτόχρονα δυνατότητα επικοινωνίας και εσωτερική μνήμη. Κάποια παραδείγματα αποτελούν τα tablet, τα GPS και οι συσκευές PDA. Δεν υπάρχει διαφορά από τα δεδομένα των κινητών συσκευών συγκριτικά με άλλα ψηφιακά δεδομένα, έχοντας ως αποτέλεσμα την εφαρμογή και σε αυτόν τον κλάδο των βασικών αρχών της διαχείρισης των ψηφιακών αποδεικτικών στοιχείων. Αξίζει όμως να αναφερθούν και κάποιες ιδιαιτερότητες οι οποίες υπάρχουν. Αρχικά, αν βρεθεί ανοιχτή συσκευή, πρέπει να διασφαλιστεί ότι θα παραμείνει συνδεδεμένη σε κάποια πηγή ενέργειας μέχρι να γίνει η συλλογή των δεδομένων της προσωρινής μνήμης.

Αν η συσκευή έχει συνδεθεί με υπολογιστή, θα πρέπει να αποσυνδεθεί αμέσως, καθώς έτσι αποφεύγεται πιθανός συγχρονισμός που θα μπορούσε να αντικαταστήσει δεδομένα της συσκευής. Απαραίτητη θεωρείται και η απομόνωση της συσκευής με τη χρήση για παράδειγμα, μίας σακούλας Faraday, καθώς υπάρχει πιθανότητα διαγραφής από πιθανές εισερχόμενες κλήσεις, emails και μηνύματα, καθώς και ο κίνδυνος της απομακρυσμένης διαγραφής δεδομένων από τον ύποπτο. Στην περίπτωση όμως που η απομόνωση αυτή γίνει με ανοιχτή συσκευή, αδειάζει πιο γρήγορα η μπαταρία καθώς προσπαθεί να συνδεθεί συνεχώς στο διαδίκτυο. Προτείνεται από τη NIST η χρήση μιας φορητής πηγής ενέργειας για την αντιμετώπιση του κινδύνου αυτού. Μια ακόμα δυσκολία την οποία αντιμετωπίζουν οι ερευνητές, θεωρείται η τεράστια ποικιλία λειτουργικών συστημάτων κινητών συσκευών αλλά και μοντέλων τα οποία κυκλοφορούν. Σε κάθε μία συσκευή υποστηρίζονται πολλές διαφορετικές εφαρμογές και υπηρεσίες, ενώ απαιτούνται επιπλέον διαφορετικά εξαρτήματα και καλώδια καθώς δεν υπάρχει ένα ενιαίο Hardware διεπαφών.

3.3.3 Δικανική Βάσεων Δεδομένων

Η εφαρμογή των τεχνικών έρευνας και ανάλυσης υπολογιστών, έχοντας στόχο να συλλεχθούν αποδεικτικά στοιχεία από βάσεις δεδομένων ώστε να παρουσιαστούν σε κάποιο δικαστήριο, ορίζει τη δικανική βάσεων δεδομένων.

3.3.4 Δικανική Υπολογιστών

Η Δικανική Υπολογιστών (Computer forensics) αποτελεί ένα κλάδο της επιστήμης της ψηφιακής εγκληματολογίας, ο οποίος είναι σχετιζόμενος με το να βρεθούν αποδεικτικά στοιχεία για υπολογιστές ενώ συνήθως εμπλέκονται και άλλα ψηφιακά μέσα αποθήκευσης όπως δισκέτες, DVD-ROM, CD-ROM και USB. Αποτελεί, λοιπόν, την εφαρμογή τεχνικών ανάλυσης και έρευνας, έχοντας στόχο να διατηρηθούν τα δεδομένα από μια συγκεκριμένη υπολογιστική συσκευή με κατάλληλο τρόπο έτσι ώστε να παρουσιαστούν μετέπειτα στο δικαστήριο. Έναν από τους στόχους της δικανικής υπολογιστών αποτελεί και η διεξαγωγή μιας παράλληλης διατήρησης γραπτής αλυσίδας στοιχείων και μιας δομημένης έρευνας, έχοντας στόχο τον προσδιορισμό με ακρίβεια του τι συνέβη σε μια υπολογιστική συσκευή, καθώς και ποιος ήταν ο υπεύθυνος για αυτό.

Συνήθως ακολουθείται μια συγκεκριμένη σειρά διαδικασιών στη δικανική υπολογιστών : μετά την απομόνωση της συσκευής η οποία έχει ερευνηθεί ώστε να προστατευτεί από πιθανές βλάβες, φτιάχνεται από τους ερευνητές ένα ψηφιακό αντίγραφο του περιεχομένου της συσκευής όπου στη συνέχεια κλειδώνεται σε ένα ασφαλές μέρος με στόχο τη διατήρηση της αρχικής της κατάστασης. Οι έρευνες πραγματοποιούνται και στα αυθεντικά δεδομένα, αλλά στο ψηφιακό αντίγραφο χρησιμοποιώντας ποικιλία εφαρμογών λογισμικού και τεχνικών. Αν κατά την εξέταση του αντίγραφου βρεθεί οποιοδήποτε στοιχείο, τότε αυτό καταγράφεται σε μια αναφορά. Παρακάτω γίνεται εστιασμός σε θέματα τα οποία αφορούν τη δικανική υπολογιστών ενώ περιγράφονται οι βασικές αρχές της απόκτησης ψηφιακών δεδομένων μέσα από την έρευνα της δικανικής υπολογιστών.

Κεφάλαιο 4ο

Απόκτηση Ψηφιακών Δεδομένων

4.1 Στατική Απόκτηση (Static Acquisition)

Η πραγματοποίηση της στατικής απόκτησης ψηφιακών δεδομένων γίνεται σε έναν απενεργοποιημένο υπολογιστή. Στην περίπτωση που βρεθεί υπό εξέταση υπολογιστής σε λειτουργία, τότε πραγματοποιείται απενεργοποίηση του, είτε ακολουθώντας τη

φυσιολογική διαδικασία απενεργοποίησης, είτε τραβώντας από την πρίζα το καλώδιο τροφοδοσίας. Από τη στιγμή που θα απενεργοποιηθεί, αφαιρεί το σκληρό δίσκο από το σύστημα και γίνεται η σύνδεση του ως εξωτερικού δίσκου σε ένα σταθμό Forensic και πραγματοποιείται αντιγραφή των περιεχομένων του. Η αντιγραφή αυτή δεν σημαίνει απλή αντιγραφή αρχείων. Η σημασία της είναι ότι αντιγράφεται κάθε byte του δίσκου μαζί με τον ελεύθερο χώρο (unallocated space), τα μεταδεδομένα και τον χώρο slack (slack space). Λαμβάνονται τα κατάλληλα μέτρα έτσι ώστε στον υπό εξέταση δίσκο να μην υπάρξουν τροποποιήσεις δεδομένων. Γίνεται επιστροφή του δίσκου στο αρχικό σύστημα ανάλογα με την κάθε περίπτωση, ή μπορεί ακόμη και να παραμείνει στην κατοχή του ερευνητή φυλασσόμενο ως στοιχείο.

Απενεργοποίηση

Όταν επιλέγεται η διαδικασία της απενεργοποίησης, σημαντικό ρόλο παίζουν τα προγράμματα και οι διαδικασίες τα οποία τρέχουν τη συγκεκριμένη στιγμή στον υπολογιστή, επειδή μετά από μια φυσιολογική απενεργοποίηση υπάρχει πιθανότητα να σβηστούν πιθανά στοιχεία. Τα προσωρινά αρχεία κειμένου, για παράδειγμα, αν η εφαρμογή που τα δημιούργησε σβήσει φυσιολογικά μπορεί και να διαγραφούν. Υπάρχουν επίσης προγράμματα τα οποία εκτελούνται σε φυσιολογική απενεργοποίηση, ενώ προχωρούν στο να διαγράψουν στοιχεία, για παράδειγμα, μία wipe utility. Εξαρτάται επίσης η διαδικασία απενεργοποίησης από το τι είδους λειτουργικό σύστημα εκτελείται αλλά και ποια έκδοση. Τα περισσότερα συστήματα τα οποία έχουν Microsoft Windows για παράδειγμα, μπορούν να απενεργοποιηθούν με ασφάλεια αν απλά τα βγάλει κάποιος από την πρίζα τραβώντας το καλώδιο τροφοδοσίας.

Σε αντίθεση, στα συστήματα τα οποία εκτελούν χρέη διακομιστή ενώ εκτελούνται σε αυτά εφαρμογές βάσεων δεδομένων που θεωρούνται ευαίσθητες σε μη ομαλή απενεργοποίηση, είναι προτιμότερο να ακολουθηθεί η ομαλή λειτουργία απενεργοποίησης. Ο ερευνητής για την αναγνώριση του λειτουργικού συστήματος ενός υπολογιστή, έχει τη δυνατότητα είτε να αναγνωρίσει το λειτουργικό από κάποια χαρακτηριστικά που έχει όπως, για παράδειγμα, για τα Windows XP το πράσινο κουμπί εκκίνησης το οποίο έχει το σύμβολο των Windows, είτε να απευθυνθεί στο διαχειριστή του συστήματος. Υπάρχει εναλλακτική αλληλεπίδραση με το σύστημα ώστε να μπορέσει να εξακριβώσει την ακριβή έκδοση και τύπο του λειτουργικού συστήματος.

Σε αυτήν όμως την περίπτωση, θα πρέπει η αλληλεπίδραση να γίνει με πολύ μεγάλη προσοχή καταγράφοντας επακριβώς τις ενέργειες οι οποίες πραγματοποιήθηκαν. Λόγω εμπειρίας του ερευνητή, τις περισσότερες φορές μπορεί να αναγνωρίσει αμέσως ένα λειτουργικό σύστημα καθιστώντας τέτοιες περιπτώσεις εξαιρετικά σπάνιες.

Σε περίπτωση που ακολουθηθεί η μέθοδος της αφαίρεσης της παροχής του ρεύματος, ο ερευνητής θα πρέπει να βεβαιωθεί ότι δεν υπάρχει συσκευή αδιάλειπτης παροχής ενέργειας (UPS), διαφορετικά οφείλει να διακόψει και τη λειτουργία αυτής ώστε να μπορέσει να σβήσει ο υπολογιστής ή να αφαιρεθεί το καλώδιο από το πίσω μέρος του υπολογιστή και όχι από τον τοίχο. Κάτι τέτοιο είναι εξαιρετικά σημαντικό καθώς πολλές φορές οι συσκευές αυτές συνοδεύονται από ένα λογισμικό το οποίο όταν διακοπεί το ρεύμα αποστέλλει ειδοποιήσεις (e-email, snmp κτλ.) που ενδεχομένως δεν είναι επιτρεπτό να σταλούν, καθώς επίσης δημιουργούν και συμβάντα στο αρχείο καταγραφής του συστήματος, έχοντας ως αποτέλεσμα να προκαλείται η δημιουργία νέων δεδομένων αντί να διατηρούνται αναλλοίωτα τα δεδομένα του υπολογιστή. Στην περίπτωση της διακοπής παροχής ρεύματος σε ένα φορητό υπολογιστή, πρέπει να αφαιρεθεί και η μπαταρία καθώς έχει ακόμα φορτίο ακόμα και όταν το καλώδιο τραβηχτεί από την πρίζα. Όποια μέθοδος και αν ακολουθηθεί, θα πρέπει να γίνει αναλυτική καταγραφή των βημάτων της και η αιτιολόγησή τους ώστε αν απαιτηθεί να δώσει ο ερευνητής λόγο σε ενδεχόμενη δίκη να μην υπάρχει θέμα.

Περιορισμοί

Η στατική απόκτηση μπορεί να αντιμετωπίσει ένα βασικό πρόβλημα το οποίο είναι η κρυπτογράφηση αρχείων ή δίσκου. Στην κρυπτογράφηση, όταν κρυπτογραφείται ένας δίσκος γίνεται σε όλο το δίσκο ή και το περιεχόμενο ενός τόμου του δίσκου (disk volume). Με την απενεργοποίηση του υπολογιστή, φαινομενικά ο δίσκος είναι γεμάτος με τυχαία δεδομένα, τα οποία χωρίς το κλειδί αποκρυπτογράφησης ένα αδύνατο να διαβαστούν. Η κρυπτογραφία δίσκου αποτελεί ένα προεπιλεγμένο χαρακτηριστικό από κάποια καινούργια λειτουργικά συστήματα και δεν χρησιμοποιείται μόνο από κακοποιούς οι οποίοι θέλουν να αντιμετωπίσουν την αποτελεσματικότητα της στατικής ανάλυσης. Όταν κρυπτογραφούνται αρχεία αντί για ολόκληρους τόμους ή δίσκους, αποκρυπτογραφούνται εντός των λειτουργικών συστημάτων κάποια μεμονωμένα αρχεία για παράδειγμα ένα αρχείο σε Word ή ακόμη και ένας ολόκληρος φάκελος. Ακόμη κι αν ο ερευνητής είχε στη διάθεσή του ένα ακριβώς αντίγραφο των bit ενός

κρυπτογραφημένου αρχείου ή δίσκου, αν αυτό λήφθηκε όταν ήταν απενεργοποιημένος ο υπολογιστής, είναι άχρηστο για αυτόν εκτός αν μπορέσει να το αποκρυπτογραφήσει χρησιμοποιώντας το μοναδικό κλειδί αποκρυπτογράφησης.

Για να μπορέσει ο ερευνητής να βρει το κλειδί της αποκρυπτογράφησης, θα πρέπει να στηριχθεί στο αν θα συνεργαστεί ο ύποπτος ή να χρησιμοποιήσει κάποιο εργαλείο το οποίο ανακτά κλειδιά όπως είναι το Password Recovery Toolkit. Τα δεδομένα τα οποία βρίσκονται σε έναν υπολογιστή ο οποίος είναι σε λειτουργία, και είναι προσωρινά και δυναμικά, χάνονται στην περίπτωση απενεργοποίησης του κάτι που αποτελεί ένα ακόμη σημαντικό ζήτημα. Τα περιεχόμενα της RAM, τα ανοιχτά κλειδιά και τα αρχεία της Registry όταν εκτελείται κάποια διεργασία και οι δικτυακές συνδέσεις, οι οποίες εξελίσσονται εκείνη τη στιγμή (Network Connection), είναι σημαντικά δεδομένα τα οποία μπορούν να δώσουν μια πιο πλήρη εικόνα για το πώς χρησιμοποιήθηκε το σύστημα. Σε μια υπόθεση στην οποία ο κατηγορούμενος, για παράδειγμα, ισχυρίζεται ότι το κακόβουλο λογισμικό θεωρείται υπεύθυνο για παράνομη δραστηριότητα στο σύστημα του (Trojan Defence), θεωρείται σημαντική η παροχή πληροφοριών για ενεργές διεργασίες και συνδέσεις ώστε να μπορέσει να εντοπιστεί αν έτρεχε εκείνη τη στιγμή κάποια ασυνήθιστη διεργασία, ή εάν κάποιος ο οποίος ήταν συνδεδεμένος στο σύστημα ανέβαζε αρχεία για παράδειγμα.

4.2 Ζωντανή Απόκτηση (Live Acquisition)

Για την αντιμετώπιση των αδυναμιών της στατικής απόκτησης έναντι στο χάσιμο των μεταβλητών δεδομένων και στην κρυπτογραφία, αναπτύχθηκε η τεχνική της ζωντανής απόκτησης. Η ζωντανή απόκτηση μπορεί να περιλάβει τη συλλογή δεδομένων από ένα απενεργοποιημένο σύστημα. Πραγματοποιείται είτε τοπικά με την εκτέλεση εντολών από το πληκτρολόγιο ενώ σώζονται τα δεδομένα σε κάποια δικτυακή πηγή (network share), είτε είναι απομακρυσμένα τα συνδεδεμένα στο σύστημα μέσα από το δίκτυο ενώ εκτελούν εντολές μέσα από τη σύνδεση αυτή ή σε κάποιο εξωτερικό δίσκο που περιλαμβάνει την συλλογή δεδομένων από ένα σύστημα ενώ αυτό είναι ενεργοποιημένο. Περιλαμβάνει την απόκτηση αντιγράφου ολόκληρου του σκληρού δίσκου ή/και τη συλλογή πτητικών ψηφιακών δεδομένων (volatile) ενώ το σύστημα παραμένει σε λειτουργία. Για να αποκτηθούν τα πτητικά δεδομένα, προσοχή δίνεται στο πόσο μεταβλητό θεωρείται το κάθε στοιχείο. Κάποιες πληροφορίες έχουν πολύ μικρότερη διάρκεια ζωής μέσα στο σύστημα συγκριτικά με άλλες.

Ο χρόνος για κάποιες συνδέσεις δικτύου οι οποίες δεν χρησιμοποιούνται, για παράδειγμα, μπορεί να λήξει συχνά μέσα σε μερικά λεπτά. Κάποιες από τις διεργασίες όπως είναι οι υπηρεσίες (Services) μπορούν να τρέχουν για μεγάλο χρονικό διάστημα, ενώ κάποιες άλλες να εκτελούνται γρηγορότερα ενώ εξαφανίζονται από τη μνήμη. Βασισμένοι σε αυτές τις πληροφορίες, δίνεται προτεραιότητα στο να αποκτηθούν κάποια πτητικά δεδομένα. Καλό είναι για παράδειγμα να λαμβάνονται πρώτα τα περιεχόμενα από ολόκληρη τη RAM, καθώς η χρήση οποιουδήποτε άλλου εργαλείου μπορεί να γίνει και μετά τη συλλογή θετικών δεδομένων, ενώ φορτώνεται στη μνήμη τροποποιώντας με αυτό τον τρόπο τα περιεχόμενά της. Όσο διαρκεί μια ζωντανή απόκτηση, είναι απαραίτητος ο προσδιορισμός το αν τρέχων λογαριασμός του χρήστη είναι συνδεδεμένος σε εικονικό ή πραγματικό περιβάλλον (Carvey, n.d.).

Και τα δύο περιβάλλοντα στην ουσία απαιτούν τις ίδιες τεχνικές διερευνήσεις, στην περίπτωση όμως που ο λογαριασμός είναι συνδεδεμένος σε μια εικονική μηχανή, τότε πρέπει να πραγματοποιηθεί εκτενέστερη ανάλυση έτσι ώστε να μπορέσει να αποκτηθεί και το αντίγραφο του πραγματικού μηχανήματος, όπως και από άλλα εικονικά μηχανήματα τα οποία βρίσκονται πιθανότατα στο πραγματικό σύστημα. Για να μπορέσει να ξεχωρίσει ένας ερευνητής αν το σύστημα είναι εικονικό ή πραγματικό υπάρχουν διάφορες τεχνικές όπως είναι να ψάξει για εγκατεστημένα εργαλεία ή ειδικούς οδηγούς Hardware. Αυτά δεν είναι ιδιαίτερα αξιόπιστα γιατί μπορεί να τροποποιηθούν εύκολα. Μια από τις πιο αξιόπιστες τεχνικές είναι η εγκατάσταση του λογισμικού εντοπισμού εικονικών μηχανών, κάτι όμως που μπορεί να επιδράσει αρνητικά στην ακεραιότητα των δεδομένων.

Περιορισμοί

Σχετικά με τη ζωντανή απόκτηση, δύο από τις κυριότερες ανησυχίες είναι η εξάρτηση της διαδικασίας από το λειτουργικό σύστημα του υπό εξέταση υπολογιστή και η τροποποίηση των δεδομένων κατά τη διάρκεια της απόκτησης. Η πραγματοποίηση της ζωντανής απόκτησης γίνεται με προγράμματα τα οποία εκτελούνται στο λειτουργικό σύστημα του υπολογιστή που βρίσκεται υπό εξέταση. Αν και εμφανίζονται κάποια κοινά χαρακτηριστικά, οι χρήστες των υπολογιστών μπορούν να διαμορφώσουν τα συστήματά τους βασισμένες στις προτιμήσεις τους. Συνεπώς, ένας ερευνητής οφείλει να γνωρίζει το χειρισμό μιας ποικιλίας λειτουργικών συστημάτων, λογισμικού και

υλικού. Πολλοί κακοποιοί επίσης έχουν τη δυνατότητα ρύθμισης με κατάλληλα προγράμματα του λειτουργικού συστήματος, ώστε να παρουσιάζει καμουφλαρισμένα δεδομένα στους ερευνητές (Jones, 2007). Με αυτό τον τρόπο, φαίνεται σαν ο ερευνητής να ζητάει από το κακόβουλο λειτουργικό να του επιστρέψει τα αποδεικτικά στοιχεία της ενοχής του.

Τα δεδομένα του υπολογιστή υπάρχει περίπτωση να τροποποιηθούν από οποιαδήποτε διεργασία τρέχει κατά τη διάρκεια της απόκτησης. Όταν λοιπόν ο ερευνητής βρει έναν υπολογιστή ανοιχτό, δεν μπορεί να έχει έλεγχο των διεργασιών οι οποίες τρέχουν σε αυτόν εκείνη τη συγκεκριμένη στιγμή. Οι διεργασίες αυτές μπορεί να είναι η εφαρμογή εξυπηρετητών ή χρήστη, οι οποίες μπορούν να αλλάξουν δεδομένα κατά τη διάρκεια της απόκτησης. Κάποια λάθη που μπορεί να γίνουν από τον ερευνητή κατά την απόκτηση, μπορεί να οδηγήσουν σε αλλαγές δεδομένων. Αν για παράδειγμα εκτελέσει μια εφαρμογή, τότε αλλάζει η χρονική στιγμή τελευταίας εκτέλεσης καθώς και οι υπόλοιπες λίστες πρόσφατων ενεργειών. Στην τροποποίηση του συστήματος αρχείων κατά τη διάρκεια της απόκτησης, το αντίγραφο το οποίο αποκτάται έχει τη δυνατότητα να παρουσιαστεί σαν μια σαφής εικόνα των δεδομένων του συστήματος (slurred images) (Jones, 2007;Carvey, n.d.).

Το τμήμα των μεταδεδομένων του δίσκου μπορεί να αλλάξει με οποιαδήποτε τροποποίηση, διαβάζεται όμως πρώτο κατά την απόκτηση. Αν οι αναφερόμενοι από τα μεταδεδομένα τομείς του δίσκου, που φυλάνε αρχεία, αλλάξουν πριν την απόκτησή τους, τότε θα περιέχονται προβλήματα στην ανάλυση καθώς οι τομείς του δίσκου και τα μεταδεδομένα δεν θα ταιριάζουν. Επιπλέον, εξαιτίας των τροποποιήσεων, οι τιμές κατακερματισμού (hash values) των partitions ή του δίσκου οι οποίες υπολογίστηκαν πριν αποκτηθούν, δεν μπορούν να πιστοποιήσουν την ακεραιότητα των δεδομένων που έχουν συλλεχθεί. Τα δεδομένα τροποποιούνται κατά τη διάρκεια της απόκτησης, συνεπώς τροποποιείται και η τιμή του κατακερματισμού. Τέλος, σε μια ζωντανή απόκτηση δεν μπορεί να γίνει επανάληψη δίνοντας τα ίδια ακριβώς αποτελέσματα (Nelson, 2010). Αν διατηρείται το αρχικό μέσο αποθήκευσης σε στατική απόκτηση, μια επανάληψη της διαδικασίας θα φέρει ακριβώς τα ίδια αποτελέσματα. Δεν μπορεί να γίνει αλλαγή των δεδομένων στο δίσκο όσες αποκτήσεις και αν πραγματοποιηθούν. Σε αντίθεση, με την εκτέλεση μιας δεύτερης ζωντανής απόκτησης ενώ οι υπολογιστές βρίσκονται σε λειτουργία, μπορεί να οδηγήσει στο να συλλεχθούν νέα δεδομένα εξαιτίας των δυναμικών αλλαγών που πραγματοποιούνται στο λειτουργικό σύστημα.

4.3 Μέθοδοι Απόκτησης

Ανεξάρτητα με τον τύπο της απόκτησης αν ήταν δηλαδή στατική ή ζωντανή, παρουσιάζονται 4 μέθοδοι συλλογής δεδομένων από το σκληρό δίσκο (Nelson, 2010) : η αραιή απόκτηση (sparse acquisition), η λογική απόκτηση (logical acquisition), η αντιγραφή του δίσκου σε άλλον δίσκο (disk-to-disk copy) και η αντιγραφή του δίσκου σε ένα αρχείο (disk-to-image file). Μια από τις πιο ευέλικτες και συνηθισμένες μεθόδους, είναι η αντιγραφή του δίσκου σε ένα αρχείο το οποίο μπορεί να αποθηκευτεί είτε σε CD-ROM είτε σε κάποιο άλλο σκληρό δίσκο. Η ονομασία του αρχείου συχνά είναι εικόνα του δίσκου (image), ενώ υπάρχουν πολλά εργαλεία τα οποία μπορεί να επιτρέψουν να διασπαστεί το αρχείο εικόνας σε μικρότερα μέρη, έτσι ώστε να μπορούν να χωρέσουν σε CDs ή DVDs. Στη μέθοδο αυτή, μπορούν να δημιουργηθούν ένα ή και περισσότερα sector-by-sector ακριβή αντίγραφα από όλα τα δυαδικά δεδομένα του δίσκου συμπεριλαμβάνοντας και τον ελεύθερο χώρο και τον slack space.

Στο αυθεντικό μέσο δεν θα πρέπει να υπάρχει οποιαδήποτε πληροφορία η οποία να παρουσιάζεται, αλλά όχι στο αρχείο εικόνα το οποίο δημιουργήθηκε. Για να μπορέσουν να διαβαστούν οι πιο κοινοί τύποι αρχείων εικόνας, χρησιμοποιούνται πολλά διαφορετικά εργαλεία forensics όπως τα ILook, X-Ways Forensics, SMART, EnCase, Prodiscover, FTK και Sleuth Kit, τα οποία μπορούν να διαβάσουν το αρχείο σαν να ήταν πραγματικός δίσκος. Όταν πρόκειται για παλιότερους δίσκους, συνήθως δεν μπορεί να είναι δυνατή η δημιουργία ενός αρχείου εικόνα εξαιτίας σφαλμάτων υλικού ή λογισμικού ή ασυμβατοτήτων (Nelson, 2010). Στις περιπτώσεις αυτές πρέπει να γίνει αντιγραφή των περιεχομένων του δίσκο σε έναν άλλο δίσκο (disk-to-disk copy). Έτσι, θα είναι πανομοιότυπο το πρώτο sector του αυθεντικού δίσκου με το πρώτο sector του δίσκου-προορισμού. Ο δίσκος προορισμός στη μέθοδο αυτή προτείνεται να γραφτεί με μηδενικά (wipe with zeros) πριν γίνει αντιγραφή, ώστε να μην υπάρξει κάποιο μπέρδεμα με άσχετα δεδομένα ίσως από προηγούμενη έρευνα.

Μπορεί να παρουσιαστούν κάποια προβλήματα όταν ο δίσκος προορισμός είναι μεγαλύτερος από το δίσκο πηγή, καθώς θα είναι δύσκολο ο προσδιορισμός του που ακριβώς τελειώνει το αντίγραφο του δίσκου πηγή. Μπορεί, επίσης, να προκύψουν κάποιες δυσκολίες στην περίπτωση που οι δύο δίσκοι έχουν διαφορετική γεωμετρία, καθώς πολλές δομές δεδομένων χρησιμοποιούν τη γεωμετρία για να μπορέσουν να περιγράψουν τις τοποθεσίες. Στην περίπτωση που ο διαθέσιμος χρόνος είναι

περιορισμένος, καθώς η συλλογή των δεδομένων από ένα μεγάλο δίσκο μπορεί να διαρκέσει πολλές ώρες, μπορεί να γίνει χρήση μιας αραιής ή λογικής απόκτησης αντιγράφου δεδομένων. Η αραιή απόκτηση μοιάζει με τη λογική, αλλά συλλέγει επιπλέον τμήματα του ελεύθερου χώρου, ενώ η λογική συλλέγει μόνο συγκεκριμένους τύπους αρχείων ή αρχεία. Παράδειγμα λογικής απόκτησης αποτελεί η υπόθεση η οποία αφορά e-email, στην οποία απαιτείται η συλλογή αρχείων Outlook .pst ή .ost.

Για να γίνει η επιλογή της καταλληλότερης μεθόδου απόκτησης για μια έρευνα, οφείλουν να ληφθούν υπόψη πόσος χρόνος μπορεί να διατεθεί για την απόκτηση, αν ο δίσκος πρέπει να επιστραφεί άμεσα στον ιδιοκτήτη και το μέγεθος του υπό εξέταση δίσκου. Σε περίπτωση επιστροφής του δίσκου, είναι καλό να χρησιμοποιηθεί ένα αξιόπιστο εργαλείο, το οποίο είναι αρκετά γνωστό στον ερευνητή έτσι ώστε να γίνει λήψη ενός πολύ καλό αντίγραφου καθώς δεν θα υπάρχει δεύτερη ευκαιρία να αποκτήσει τα δεδομένα. Στην περίπτωση που ο δίσκος πηγή είναι πολύ μεγάλος για παράδειγμα, 500GB ή παραπάνω, ο ερευνητής οφείλει να έχει στη διάθεσή του ένα δίσκο ο οποίος να χωράει το δημιουργούμενο αρχείο εικόνα. Σε περίπτωση που δεν διαθέτει κάποιο τέτοιο δίσκο έχει τη δυνατότητα καταφυγής σε εναλλακτικές λύσεις όπως να συμπιέσει το αρχείο εικόνα.

Συμπίεση Αρχείου-Εικόνας

Στην περίπτωση που γίνεται εγγραφή σε αρχείο των ψηφιακών δεδομένων, δίνεται πολλές φορές η δυνατότητα συμπίεσης του αρχείου αυτού, ώστε να μπορέσει να καταλαμβάνει λιγότερο χώρο. Οι μέθοδοι συμπίεσης που υπάρχουν είναι δύο, η συμπίεση με και χωρίς απώλειες (lossy και lossless compresion).

- Η συμπίεση με απώλειες έχει ως αποτέλεσμα μετά την αποσυμπίεση να παράγεται ένα τροποποιημένο αντίγραφο των δεδομένων καθώς συμπιέζει τα δεδομένα ξεχωρίζοντας μόνιμα bits πληροφορίας του αρχείου. Καθώς λοιπόν η μέθοδος αυτή αλλάζει τα αρχικά δεδομένα, δεν μπορεί να χρησιμοποιηθεί για forensics acquisitions. Όταν όμως γίνεται χρήση της συμπίεσης χωρίς απώλειες, που μειώνεται το μέγεθος του αρχείου χωρίς αλλαγή των δεδομένων, το αποτέλεσμα μετά την αποσυμπίεση είναι να παραχθεί ένα ακριβές αντίγραφο των αρχικών δεδομένων.
- Η λειτουργία της συμπίεσης χωρίς απώλειες γίνεται με την πιο αποδοτική αποθήκευση επαναλαμβανόμενων δεδομένων. Αν τα δεδομένα για παράδειγμα

έχουν 10.000 συνεχόμενες μονάδες, θα μπορούσε να περιγραφεί ένας συμπιεσμένος τύπος του αρχείου σε μερικά εκατοντάδες bits αντί για 10000 bits. Στην περίπτωση που τα δεδομένα είναι τυχαία, τότε η συμπίεση δεν θα είναι τόσο αποδοτική καθώς θα υπάρχει μια μικρή επανάληψη. Αν γίνει συμπίεση των δεδομένων τα οποία έχουν ήδη συμπιεστεί, το αποτέλεσμα δεν θα είναι ιδιαίτερα μικρότερο.

Μια εικόνα δίσκου όταν είναι συμπιεσμένη, κάθε εργαλείο το οποίο έχει χρησιμοποιηθεί για να επεξεργαστεί, θα πρέπει να υποστηρίζει τον τύπο της συμπίεσης. Στους πιο συνηθισμένους τύπους συμπίεσης απαιτείται η αποσυμπίεση ολόκληρου του αρχείου πριν τη χρήση του, όπως είναι για παράδειγμα το gzip για Unix και το Winzip για το Windows. Κάποιοι ειδικοί αλγόριθμοι συμπίεσης μπορούν να επιτρέψουν να αποσυμπιεστούν τα αρχεία και πρέπει να χρησιμοποιούνται από κάθε εργαλείο απόκτησης, ώστε να μην θεωρηθεί απαραίτητη η αποσυμπίεση ολόκληρου της εικόνας. Τα πλεονεκτήματα που παρουσιάζει η συμπίεση, είναι ότι μπορεί να γίνει αντιγραφή των περιεχομένων ενός μέσου αποθήκευσης σε μικρότερο αρχείο, αν και συνολικά εξοικονομείται το μέγεθος του χώρου από τα αρχικά δεδομένα. Τα μειονεκτήματα της συμπίεσης είναι, ότι ανάλογα με τον τύπο μπορεί να υποστηρίζεται από ένα συγκεκριμένο αριθμό εργαλείων καθώς και ότι για να γίνει η ανάλυση και η απόκτηση ίσως χρειαστεί παραπάνω χρόνος, καθώς απαιτείται αποσυμπίεση και συμπίεση του αρχείου αντίστοιχα.

Τύποι αρχείου-εικόνας

Όταν επιλεγεί ένα αρχείο για να αποθηκευτούν τα δεδομένα τα οποία συλλέχθηκαν από κάποιο δίσκο (disk-to-image), δίνεται η δυνατότητα επιλογής του τύπου του αρχείου αυτού. Υπάρχουν τρεις τύποι τέτοιων αρχείων :

Ακατέργαστος Τύπος (Raw format)

Στα αρχεία του ακατέργαστου τύπου περιέχεται ένα απλό αντίγραφο sector-by-sector από όλα τα ανεπεξέργαστα δεδομένα του δίσκου χωρίς διαγραφές ή προσθήκες. Στα πλεονεκτήματά του, είναι οι γρήγορες μεταφορές των δεδομένων, καθώς και η δυνατότητα αγνόησης αμελητέων σφαλμάτων ανάγνωσης του δίσκου. Επίσης, αρκετά

από τα εργαλεία δικανικής υπολογιστών έχουν τη δυνατότητα να διαβάσουν ότι απαιτείται, σε ίσο χώρο με το μέγεθος του δίσκου που αντιγράφεται. Ένα άλλο πρόβλημα μπορεί να αποτελέσει αδυναμία αποθήκευσης μεταδεδομένων στο αρχείο όπως είναι, για παράδειγμα, ο σειριακός αριθμός του δίσκου. Κάποια μεταδεδομένα μπορούν όμως να αποθηκευτούν σε ξεχωριστά επιπλέον αρχεία, κάτι που πρακτικά μπορεί να θέσει σε κίνδυνο το σύστημα, καθώς αυτά μπορεί να χαθούν ή να μπερδευτούν με τα μεταδεδομένα άλλων δίσκων.

Ιδιοκτησιακός Τύπος (Proprietary format)

Υπάρχουν πολλά διαφορετικά format σε αυτή την κατηγορία, καθώς τα περισσότερα από τα εμπορικά εργαλεία της δικανικής υπολογιστών, περιέχουν ένα δικό τους τύπο αρχείου εικόνας δίσκου. Στους ιδιοκτησιακούς τύπους παρέχονται συνήθως διάφορες δυνατότητες, οι οποίες δεν μπορούν να παραχθούν με την ακατέργαστη μορφή, όπως είναι η δυνατότητα να συμπιεστούν τα αρχεία εικόνας του δίσκου εξοικονομώντας χώρο, καθώς και η δυνατότητα να ενσωματωθούν τα μεταδεδομένα στο αρχείο εικόνας όπως είναι, για παράδειγμα, το όνομα του ερευνητή, λεπτομέρειες και σχόλια για την υπόθεση που ερευνάται, η ημερομηνία της απόκτησης και η τιμή κατακερματισμού (hash value). Δεν είναι πάντα δυνατό να αναλυθεί ένα τέτοιο αρχείο από ένα διαφορετικό κατασκευαστή, κάτι που αποτελεί ένα βασικό μειονέκτημα. Στο εργαλείο IXimager, για παράδειγμα, παράγονται τρεις ιδιοκτησιακοί τύποι τα IDIF, IRBF και IEIF, τα οποία μπορούν να διαβαστούν μόνο από το εργαλείο ILook (Nelson, 2010).

Ένας από τους πιο συχνά χρησιμοποιούμενος ιδιοκτησιακούς τύπους είναι το Expert Witness Format (EWF), το οποίο συχνά ονομάζεται και τύπος E01 εξαιτίας της επέκτασης του (.E01). Για το εργαλείο EnCase η προεπιλεγμένη επέκταση υποστηρίζει τη συμπίεση και τη διάσπαση εικόνας και αρχείου, καθώς και την αποθήκευση μεταδεδομένων συμπεριλαμβανομένων και των κρυπτογραφικών τιμών του αντιγράφου το οποίο έχει αποκτηθεί, σε μια δομή επικεφαλίδας που παρουσιάζεται στο πρώτο τμήμα του αρχείου εικόνας. Μπορεί να γίνει ανάλυση και παραγωγή πολλών αρχείων EWF από πολλά εργαλεία της ψηφιακής δικανικής, όπως είναι το X-Ways Forensics, το FTK και το SMART.

Τύπος AFF

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

- Δημιουργία συμπιεσμένου ή μη αρχείου.
- Δυνατότητα να αποθηκευτεί η εικόνα του δίσκου σε κάποιο αρχείο το οποίο έχει οποιοδήποτε μέγεθος ή να διασπαστεί σε πολλαπλά αρχεία.
- Αποθήκευση των μεταδεδομένων είτε σε ξεχωριστά αρχεία είτε στο ίδιο αρχείο.
- Απλός σχεδιασμός και δυνατότητες επεκτασιμότητας.
- Ανοιχτού κώδικα, διαθέσιμο για διάφορα λειτουργικά συστήματα και πλατφόρμες.
- Εσωτερικοί έλεγχοι συνέπειας αυτό να μπορεί να γίνει ανάκτηση από μέρη της εικόνας ακόμα και αν άλλα αλλοιωθούν.
- Επεκτασιμότητα των αποθηκευμένων μεταδεδομένων, έτσι ώστε να μπορεί να αποθηκευτεί άμεσα στο αρχείο εικόνας οποιαδήποτε πληροφορία για την υπόθεση.

Το AFF στο μέλλον μπορεί να αποτελέσει την τυπική μορφή ενός Forensic Image, οπότε και σύντομα θα πρέπει να συμπεριληφθεί στα περισσότερα εμπορικά εργαλεία.

4.4 Εργαλεία Απόκτησης

Στην ενότητα αυτή παρουσιάζονται κάποια εργαλεία τα οποία είναι δημοφιλή για να δημιουργηθούν αντίγραφα δίσκου. Καθώς υπάρχει μεγάλη πληθώρα τέτοιων εργαλείων είτε είναι δωρεάν είτε όχι, καθιστά αδύνατη την παρουσία όλων τους.

dd/dcfldd

Το εργαλείο dd σε όλες τις διανομές Linux είναι εγκατεστημένο από προεπιλογή, διατίθεται όμως και για Windows. Αποτελεί ένα πολύ απλό αλλά παράλληλα πολύ ισχυρό εργαλείο γραμμής εντολών, όπου η λάθος χρήση του μπορεί πολύ εύκολα να οδηγήσει στο να χαθούν δεδομένα. Δεν διαθέτονται χαρακτηριστικά τα οποία έχουν άλλα πιο μοντέρνα εργαλεία, όπως είναι η συλλογή μεταδεδομένων για το αρχείο εικόνα που μπορεί να δημιουργήσει και να διορθώσει λάθη. Τα παραγόμενα αρχεία εικόνες είναι σε ακατέργαστη μορφή (raw image file). Μια από τις εκδόσεις του dd σχεδιάστηκε ειδικά για να χρησιμοποιηθεί στην επιστήμη της ψηφιακής δικανικής και είναι το dcfldd. Μπορεί να έχει την ίδια βασική λειτουργία με το dd, παρέχει όμως και επιπλέον δυνατότητες, όπως ότι μπορεί να υπολογίσει ταυτόχρονα τις τιμές

κατακερματισμού των δεδομένων που αντιγράφει, ταυτόχρονη αντιγραφή σε παραπάνω από ένα αρχεία δίσκους καθώς και καταγραφή γεγονότων, παρέχει πιστοποίηση ότι το αρχείο εικόνα είναι ίδιο με αυτό του αρχικού δίσκου, παρουσιάζει μπάρα προόδου του αριθμού των δεδομένων που έχουν ήδη αντιγραφεί και υπολογίζει ταυτόχρονες τιμές κατακερματισμού δεδομένων.

FTK Imager

Ο FTK Imager παρέχεται από την AccessData, και είναι ένα εμπορικό (commercial) εργαλείο για να μπορέσουν να αποκτηθούν αντίγραφα ψηφιακών δεδομένων. Υποστηρίζονται συγκεκριμένοι τύποι αρχείων : ο ακατέργαστος τύπος (raw), ο AFF, ο EWF και ο SMART 2 . Έχει τη δυνατότητα δημιουργίας αρχείων και εικόνων σκληρών δίσκων και άλλων μέσων αποθήκευσης ή ακόμη και μεμονωμένων φακέλων και αρχείων. Επιτρέπει στο να προβληθεί το περιεχόμενο ενός αρχείου εικόνας όπως ακριβώς το έβλεπε ο χρήστης καθώς γινόταν εξαγωγή του φακέλου ή των αρχείων από αυτό. Δημιουργούνται επίσης τιμές κατακερματισμού για αρχεία είτε με τη συνάρτηση MD5 είτε με την SHA-1. Η εγκατάσταση του FTK Imager μπορεί να γίνει στον υπολογιστή ο οποίος θα χρησιμοποιηθεί ή μέσα από κάποια φορητή συσκευή όπως για παράδειγμα μνήμη USB, συνεπώς δεν θεωρείται απαραίτητη η εγκατάσταση στον υπό εξέταση υπολογιστή.

Μπλοκάρισμα Εγγραφής

Υπάρχει πιθανότητα να γραφούν δεδομένα στον αρχικό δίσκο κατά τη διάρκεια της απόκτησης ψηφιακών δεδομένων από το δίσκο αυτό. Κάτι τέτοιο θα μπορούσε να οδηγήσει στο να απορριφθούν τα αποδεικτικά στοιχεία από το δικαστήριο, και συνεπώς ο ερευνητής οφείλει να λάβει μέτρα ώστε να μην τροποποιηθούν τα αρχεία. Ένας από τους ευκολότερους τρόπους επίτευξης αυτού είναι με τη χρήση write blockers. Ένας write blocker μπορεί να επιτρέψει σε ένα σύστημα να διαβάσει τα δεδομένα από ένα δίσκο με τον οποίο συνδέεται εξωτερικά, ενώ ταυτόχρονα μπορεί να μπλοκάρει στον εξωτερικό δίσκο κάθε εντολή γραψίματος. Ένας υπολογιστής φυσιολογικά είτε διαβάζει δεδομένα είτε τα γράφει από μια συσκευή αποθήκευσης μέσα από συγκεκριμένες εντολές, ενώ μεταφέρει τις εντολές αυτές από την διεπαφή σύνδεσης, στον ίδιο τον υπολογιστή στη σύνδεση της συσκευής που θα αποθηκευτούν. Με τη χρήση ενός write blocker, μπορεί ο ερευνητής να αποτρέψει τον υπολογιστή ο οποίος εκτελεί την απόκτηση της γραφής δεδομένων στον υπό εξέταση σκληρό δίσκο.

Τα είδη του write blocker είναι δύο, οι write blockers λογισμικού και υλικού (Hardware/Software write blockers). Ένας write blocker λογισμικού, μπορεί να αντικαταστήσει τη διεπαφή πρόσβασης του υπολογιστή, προσθέτοντας εξωτερικές συσκευές αποθήκευσης. Με αυτό τον τρόπο, όταν δοθεί εντολή γραψίματος ή εγγραφής στον εξωτερικό δίσκο, αντί να εκτελεστεί ο κώδικας ο οποίος θα πραγματοποιούσε την εγγραφή αυτή, εκτελείται ο κώδικας του λογισμικού write blocker, ο οποίος και εξετάζει την εντολή που δόθηκε. Ένας write blocker υλικού αποτελεί μια συσκευή η οποία μπορεί να παρεμβληθεί ανάμεσα στην εξωτερική συσκευή αποθήκευσης και στον υπολογιστή, φιλτράροντας τις εντολές οι οποίες δίνονται στη διεπαφή του μέσου αποθήκευσης, αποτρέποντας έτσι να εγγραφούν δεδομένα σε αυτό.

Ένας άλλος τρόπος για να μπορέσει να μπλοκαριστεί η εγγραφή στα μέσα αποθήκευσης είναι εκκίνηση του υπολογιστή μέσα από CD/DVD/FLOPPY κ.λπ., με τη χρήση ειδικά διαμορφωμένου λειτουργικού συστήματος, το οποίο συνήθως είναι Linux ή BSD ή και DOS. Κατά την εκκίνηση κάνει προσάρτηση (mount) των αποθηκευτικών μέσων μόνο προς ανάγνωση, μην επιτρέποντας την εγγραφή σε αυτά (Nelson, 2010). Τέτοιου είδους δίσκοι φυσικά δοκιμάστηκαν πρώτα στα εργαστήρια ότι όντως δεν επιτρέπουν να γίνει εγγραφή στο μέσο. Τέτοιο λειτουργικά είναι το Caine, ένα live CD βασισμένο στο Ubuntu.

HPA και DCO

Οι HPA (Host Protected Area) και DCO (Device Configuration Overlay) αποτελούν τμήματα τα οποία βρίσκονται στο τέλος του δίσκου και έχουν τη δυνατότητα αποθήκευσης δεδομένων που δεν είναι προσβάσιμα όμως από το λειτουργικό σύστημα ή το BIOS και άρα και από το χρήστη. Κάτι τέτοιο μπορεί να τα κάνει ιδανικά για κάποιον ο οποίος θέλει να κρύψει δεδομένα και, συνεπώς, ο ερευνητής δεν πρέπει να παραλείψει να ψάξει και εκεί για δεδομένα. Στην περίπτωση όμως που ο ερευνητής χρησιμοποιεί ένα εργαλείο απόκτησης, το οποίο δεν εξετάζει την ύπαρξη τμημάτων HPA/DCO, αυτά δε θα αποκτηθούν. Υπάρχουν εργαλεία απόκτησης τα οποία ψάχνουν αυτόματα και αποκτούν HPA/DCO. Σε περίπτωση που δεν υπάρχει πρόσβαση από τον ερευνητή σε ένα τέτοιο εργαλείο θα πρέπει να καταφύγει σε άλλες τεχνικές ανίχνευσης.

Ένας από τους τρόπους εντοπισμού τμημάτων HPA/DCO είναι η σύγκριση των τομών (LBA sectors) τις οποίες βλέπει το BIOS, με αυτές οι οποίες αναγράφονται στην ετικέτα πάνω στο σκληρό δίσκο.

Σε περίπτωση που το BIOS βλέπει λιγότερους από αυτούς οι οποίοι αναγράφονται στην ετικέτα, τότε κατά πάσα πιθανότητα υπάρχει ένα τμήμα HPA ή DCO. Η τακτική αυτή δεν θεωρείται πάντα αξιόπιστη γι' αυτό καλό θα ήταν ο ερευνητής να συμβουλεύεται τη σελίδα του κατασκευαστή, ώστε να γνωρίζει περισσότερες τεχνικές λεπτομέρειες (Bunting, 2012). Μπορεί σε ένα δίσκο να συνυπάρχει χώρος HPA με DCO, αρκεί το τμήμα DCO να δημιουργήθηκε πριν το HPA (ασχέτως αν το DCO βρίσκεται χωροταξικά στο δίσκο μετά το HPA). Επίσης, μπορούν να ανιχνευθούν τμήματα HPA και DCO με την εφαρμογή hdparm για Linux, με τις εντολές "hdparm -N /dev/sda" και "hdparm –dco-identify /dev/sda" αντίστοιχα, όπου sda είναι ο δίσκος υπό εξέταση. Στην περίπτωση ανίχνευσης τμήματος HPA ή/και DCO, πρέπει να γίνει αφαίρεση του έτσι ώστε να αποκτηθεί το κρυμμένο κομμάτι του δίσκου. Κάτι τέτοιο γίνεται με την αλλαγή των ρυθμίσεων του δίσκου και πιο συγκεκριμένα αν τεθεί ο μέγιστος αριθμός των τομέων οι οποίοι είναι ορατοί από τον χρήστη, ίσος με τον πραγματικό αριθμό των τομέων τους οποίους περιλαμβάνει ο δίσκος. Αυτό γίνεται με εργαλεία όπως το hdparm ή το setmax (Carrier, 2005)

Πιστοποίηση

Από τα πιο σημαντικά ζητήματα της δικανικής υπολογιστών θεωρείται η πιστοποίηση ψηφιακών δεδομένων. Για την ευστάθεια μιας έρευνας σε ένα δικαστήριο, οφείλει να αποδειχθεί ότι δεν αλλοιώθηκαν τα πειστήρια με οποιονδήποτε τρόπο. Για να μπορέσουν να πιστοποιηθούν τα δεδομένα, γίνεται χρήση μιας κρυπτογραφικής συνάρτησης κατακερματισμού, η οποία αποτελεί μια ντετερμινιστική διαδικασία, που έχει ως είσοδο ένα μπλοκ δεδομένων τυχαίου μεγέθους όπως είναι για παράδειγμα το αρχείο του δίσκου, επιστρέφοντας ένα αλφαριθμητικό ίδιου πάντα μεγέθους. Αν υπάρχει οποιαδήποτε παραμικρή μεταβολή στα αρχικά δεδομένα ακόμα και αν αλλάξει απλά ένα γράμμα από μικρό σε κεφάλαιο, παράγεται μια εντελώς διαφορετική τιμή κατακερματισμού (hash value). Στους αλγόριθμους κατακερματισμού οι οποίοι χρησιμοποιούνται συχνά σε μία έρευνα Forensic, περιλαμβάνονται οι MD5 και SHA1.

Ο MD5 παράγει μία τιμή των 128 bit ενώ ο SHA1 των 160 bit. Εντοπίστηκαν συγκρούσεις και για τους δύο αυτούς αλγόριθμους κάτι που σημαίνει ότι δυο

διαφορετικά μπλοκ από δεδομένα έχουν την ίδια τιμή κατακερματισμού. Στη συγκεκριμένη περίπτωση, κάτι τέτοιο δεν αποτελεί ιδιαίτερο πρόβλημα καθώς στην περίπτωση υποψίας σύγκρουσης μπορεί να γίνει μια σύγκριση byte-by-byte για την επιβεβαίωση ότι όλα τα bytes είναι ίδια. Η εντολή MS-DOS Comp ή η Linux/Unix diff, πραγματοποιεί τέτοιες συγκρούσεις. Φαίνεται, λοιπόν, ότι από τις ιδιότητες των συναρτήσεων κατακερματισμού, ο τρόπος χρήσης τους στη δικανική υπολογιστών ώστε να μπορέσουν να πιστοποιηθούν τα ψηφιακά δεδομένα. Για τα αρχικά δεδομένα δημιουργείται μια τιμή κατακερματισμού όπου στη συνέχεια συγκρίνεται με την τιμή για το Forensic αντίγραφο τους.

Στην περίπτωση που οι τιμές αυτές είναι ίδιες, σημαίνει ότι δεν έχουν αλλοιωθεί τα δεδομένα. Επιπλέον, με τον υπολογισμό μιας τιμής κατακερματισμού αφού ολοκληρωθεί η εξέταση του αντίγραφου Forensic, μπορεί να αποδειχθεί ότι δεν τροποποιήθηκαν τα δεδομένα από τον ερευνητή. Άλλη μια χρήση που μπορεί να έχει η συνάρτηση κατακερματισμού, είναι να εντοπίσει γνωστά αρχεία τα οποία μπορούν να εξαιρεθούν από την έρευνα, όπως είναι, για παράδειγμα, κοινά προγράμματα ή αρχεία του λειτουργικού συστήματος ή ακόμη και ο εντοπισμός παράνομων αρχείων τα οποία κρύβονται αλλάζοντας το όνομά τους. Δημιουργήθηκε μια λίστα από τιμές κατακερματισμού από την National Software Reference Library (NSRL) για διάφορες εφαρμογές και αρχαία λειτουργικών συστημάτων.

Κεφάλαιο 5ο

Δικτυακή εγκληματολογία

Ο καλύτερος ορισμός της δικτυακής εγκληματολογίας μπορεί να παρουσιαστεί ως η ανάλυση, η καταγραφή και η ανίχνευση της κυκλοφορίας ενός δικτύου, καθώς και οι εκδηλώσεις του. Προκειμένου να ανακαλύψουν την πηγή συμβάντων επιθέσεων και ασφάλειας, ή ακόμη και κάποιων άλλων πιθανών προβλημάτων, διενεργούνται κάποιες εγκληματολογικές εξετάσεις δικτύου. Από τους βασικότερους ρόλους του ερευνητή

είναι η διαφοροποίηση των επαναλαμβανόμενων προβλημάτων από τις κακόβουλες επιθέσεις.

Η διαδικασία του Hacking

Στη διαδικασία του hacking ακολουθείται μια σταθερή μεθοδολογία. Γενικά, μπορούν να χωριστούν σε 6 φάσεις τα βήματα που μπορεί να ακολουθήσει ένας χάκερ :

1. Αναγνώριση
2. Σάρωση και απαρίθμηση
3. Απόκτηση πρόσβασης
4. Κλιμάκωση προνομίου
5. Διατήρηση της πρόσβασης
6. Κάλυψη τροχιών και τοποθέτηση κερκόπορτων

Η διαδικασία εισβολής

Η αναγνώριση θεωρείται η πρώτη φάση προεπίθεσης. Η επιδίωξη του χάκερ είναι να ανακαλύψει όσο το δυνατόν περισσότερες πληροφορίες για το θύμα. Στη δεύτερη φάση της προ επίθεσης, περιέχονται η απαρίθμηση και η σάρωση. Στο βήμα αυτό της μεθοδολογίας, πραγματοποιείται η μετακίνηση του χάκερ από την παθητική συλλογή πληροφοριών στην ενεργή συλλογή πληροφοριών. Η απόκτηση της πρόσβασης μπορεί να γίνει με πολλούς διαφορετικούς τρόπους. Μπορεί ο χάκερ να εκμεταλλευτεί την ευπάθεια ενός δρομολογητή ή ακόμη και να δημιουργήσει κάποιο εικονικό μηχανικό του γραφείου βοήθειας, ώστε να μπορέσει να πάρει τον τηλεφωνικό αριθμό ενός μόντεμ. Για την επιτυχία της πρόσβασης, απαιτείται να βρεθεί η ευπάθεια του λογισμικού του διακομιστή web.

Πιθανότατα, μια πρόσβαση σε ένα μέσο λογαριασμό χρήστη δεν θα μπορέσει να δώσει στον εισβολέα αρκετά μεγάλο έλεγχο ή την πρόσβαση στο δίκτυο. Συνεπώς, θα προσπαθήσει ο εισβολέας την κλιμάκωση των δικαιωμάτων διαχειριστή ή root. Από τη στιγμή που θα ολοκληρωθεί η κλιμάκωση του προνομίου αυτού, τότε ο εισβολέας θα το χρησιμοποιήσει, ώστε αυτό να εργαστεί για τρόπους διατήρησης πρόσβασης στα συστήματα τα οποία επιτέθηκε και παραβίασε. Καθώς οι χάκερ έχουν μεγάλες ομοιότητες με άλλους εγκληματίες, θέλουν να βεβαιωθούν ώστε να έχουν αφαιρεθεί όλα τα αποδεικτικά στοιχεία των δραστηριοτήτων τους, στα οποία μπορεί να

περιλαμβάνονται η χρήση root kit προκειμένου να καλύψουν τα ίχνη τους. Αυτό γίνεται τη στιγμή στην οποία ξεκινούν οι περισσότερες ερευνητικές δραστηριότητες.

Αναζήτηση αποδεικτικών στοιχείων

Ένας ερευνητής, οφείλει να έχει γνώση καθενός από τα βήματα της διαδικασίας hacking και κατανόηση των κινήτρων και των δραστηριοτήτων του χάκερ. Πολλές φορές θα αναγκαστούν να αναλάβουν τη χρήση μόνο κομματιών πληροφοριών και έτσι παίζοντας το ρόλο του ντετέκτιβ θα προσπαθήσουν να επανασυναρμολογήσουν τα κομμάτια του παζλ. Πληροφορίες οι οποίες βρίσκονται αποθηκευμένες σε έναν υπολογιστή, είναι δυνατόν να υπάρχουν είτε σε μία ή και περισσότερες προκαθορισμένες περιοχές. Οι πληροφορίες αυτές, έχουν τη δυνατότητα αποθήκευσης ως κρυφό, διαγραμμένο ή και κανονικό αρχείο, στον ελεύθερο ή χαλαρό χώρο. Το να κατανοηθούν αυτές οι περιοχές, ο τρόπος χειραγώγησης τους και ο τρόπος λειτουργίας τους, αυξάνεται η πιθανότητα ανακάλυψης ή εύρεσης κρυμμένων δεδομένων. Δεν είναι όλοι οι ύποπτοι σούπερ κυβερνοεγκληματίες. Αρκετά άτομα δεν θα κρύψουν καθόλου αρχεία, ενώ άλλοι θα επιχειρήσουν να χρησιμοποιήσουν απλές τεχνικές απόκρυψης σε ένα αρχείο.

Μπορεί ακόμα να βρεθούν πολλές περιπτώσεις στις οποίες οι ύποπτοι κυριεύθηκαν από τύψεις, φόβο ή και λύπη, προσπαθώντας να διαγράψουν ενοχοποιητικά στοιχεία μετά το συμβάν. Οι μέσοι χρήστες υπολογιστών, δεν μπορούν να κατανοήσουν ότι αν πετάξουν ένα αντικείμενο στον κάδο ανακύκλωσης δεν σημαίνει ότι αυτό καταστρέφεται οριστικά. Αυτές οι προσπάθειες αποφυγής της ανακάλυψης είναι μάταιες. Μπορεί να αποτρέψουν το μέσο χρήστη από το να βρει δεδομένα, αλλά δεν αποτρέπουν τον ερευνητή. Μία από τις κοινές τεχνικές απόκρυψης, είναι να τοποθετηθούν οι πληροφορίες σε μια σκοτεινή τοποθεσία όπως είναι το C:\winnt\system32\os2\dll. Αυτό όμως και πάλι, συνήθως εμποδίζει μόνο το μέσο χρήστη στην εύρεση του αρχείου. Στην τεχνική αυτή, τοποθετείται απλά η πληροφορία σε μια περιοχή της μονάδας δίσκου όπου συνήθως δεν είναι ορατή. Μια απλή αναζήτηση συστήματος θα μπορέσει να νικήσει γρήγορα τη μάταιη αυτή προσπάθεια απόκρυψης δεδομένων.

Γίνεται απλά αναζήτηση συγκεκριμένων τύπων αρχείων όπως είναι bmp, tif, doc και xls. χρησιμοποιώντας την ενσωματωμένη λειτουργία αναζήτησης στα Windows που βοηθά να βρεθεί γρήγορα αυτός ο τύπος πληροφοριών. Στην περίπτωση που γίνεται η

εξέταση σε έναν υπολογιστή Linux, χρησιμοποιείται η εντολή grep για αναζήτηση στη μονάδα δίσκου. Η χρήση χαρακτηριστικών αρχείων για να μπορέσουν να αποκρυφθούν φάκελοι ή αρχεία αποτελεί μια άλλη τεχνική. Μπορεί να γίνει απόκρυψη ενός αρχείου με το βοηθητικό πρόγραμμα ResEdit σε έναν υπολογιστή Macintosh. Τα χαρακτηριστικά στο λογισμικό των Windows, μπορούν να ρυθμιστούν ώστε να γίνεται απόκρυψη αρχείων στη γραμμή εντολών χρησιμοποιώντας την εντολή attrib. Η εντολή αυτή βρίσκεται ενσωματωμένη στο λειτουργικό σύστημά τους. Μπορεί να επιτρέψει στο χρήστη την αλλαγή των ιδιοτήτων ενός αρχείου. Η απόκρυψη του αρχείου μπορεί να γίνει με την έκδοση attrib +h secret.txt.

Η εντολή αυτή θα αποδώσει στο αρχείο μια αόρατη εμφάνιση στο περιβάλλον της γραμμής εντολών. Κάτι τέτοιο μπορεί επίσης να επιτευχθεί μέσα από το GUI κάνοντας δεξί κλικ σε ένα αρχείο, και επιλέγοντας από εκεί τον κρυφό τύπο. Υπάρχει όμως περίπτωση το αρχείο να μην είναι αόρατο στο GUI, καθώς εξαρτάται από τις διαμορφωμένες ρυθμίσεις προβολής. Ανοίγοντας ένα παράθυρο περιήγησης και επιλέγοντας εργαλεία/επιλογές φακέλου/προβολή/εμφάνιση/κρυφά αρχεία, μπορεί κάποιος να βεβαιωθεί ότι είναι επιλεγμένο το Show Hidden Files. Αυτό μπορεί να εμφανίσει όλους τους φακέλους και αρχεία ακόμη και αυτούς με το σύνολο χαρακτηριστικών +h.

Ένας άλλος τρόπος λήψης μιας πλήρης λίστας όλων των κρυφών αρχείων είναι αν εκδοθεί η εντολή attrib /s > features.txt από τον ριζικό κατάλογο. Η εντολή attrib κάνει παράθεση χαρακτηριστικών του αρχείου, η συνάρτηση /s κάνει παράθεση όλων των αρχείων σε όλους τους υποκαταλόγους ενώ το > κάνει ανακατεύθυνση της εξόδου σε ένα αρχείο κειμένου. Αυτό το αρχείο κειμένου έχει τη δυνατότητα στη συνέχεια τοποθέτησης και ανάλυσης σε ένα υπολογιστικό φύλλο, έτσι ώστε να αναλυθεί περαιτέρω. Μπορούν να ξεπεραστούν γρήγορα αυτές οι ακατέργαστες προσπάθειες.

5.1 Επισκόπηση δρομολογητών

Ένα βασικό κομμάτι του εργαλείου δικτύωσης αποτελούν οι δρομολογητές. Παρακάτω παρουσιάζεται η λειτουργία και ο ρόλος ενός δρομολογητή.

Τι είναι ένας δρομολογητής

Οι δρομολογητές μπορεί να είναι συσκευές λογισμικού υλικού οι οποίες δρομολογούν δεδομένα τα οποία περνούν από ένα τοπικό δίκτυο σε ένα διαφορετικό δίκτυο.

Θεωρούνται υπεύθυνοι για να ληφθούν αποφάσεις σχετικά με το ποια από τις διαφορετικές διαδρομές θα ακολουθηθεί από την κίνηση δικτύου ή Internet. Στην περίπτωση που υπάρχουν περισσότερες από μία διαδρομές για να μεταδοθούν τα δεδομένα, τότε ο δρομολογητής καθορίζει τη διαδρομή η οποία θεωρείται η καλύτερη για να δρομολογηθούν οι πληροφορίες.

Η λειτουργία ενός δρομολογητή

Οι δρομολογητές μπορούν να λειτουργήσουν επίσης δεσμεύοντας ανόμοια δίκτυα και ως μεταφραστές πρωτοκόλλων. Περιορίζουν τη φυσική κυκλοφορία μετάδοσης με τη λειτουργία τους στο επίπεδο 3 του μοντέλου OSI. Γίνεται χρήση συνήθως οποιονδήποτε πρωτοκόλλων δρομολόγησης, τα οποία είναι βασισμένα στην καταμέτρηση αναπήδησης ή στην κατάσταση αναπήδησης για να προσδιοριστεί η καλύτερη διαδρομή.

Ο ρόλος ενός δρομολογητή

Οι δρομολογητές βρίσκονται στο επίπεδο τρία του μοντέλου OSI, το οποίο είναι γνωστό και ως επίπεδο δικτύωσης. Από το επίπεδο δικτύου παρέχεται δρομολόγηση ανάμεσα στα δίκτυα ενώ ορίζεται η αλληλουχία πακέτων, ο έλεγχος συμφόρησης, ο έλεγχος σφαλμάτων και η λογική διευθυνσιοδότηση. Η κύρια ενασχόληση του επιπέδου αυτού, είναι ο τρόπος με τον οποίο λαμβάνονται πακέτα από το δίκτυο Α στο δίκτυο Β, όπου ορίζονται και οι διευθύνσεις IP. Οι διευθύνσεις αυτές μπορούν να δώσουν σε κάθε συσκευή στο δίκτυο μια μοναδική λογική διεύθυνση. Η οργάνωση των διευθύνσεων αυτών σε κλάσεις, οργανώνεται από τους δρομολογητές, και χρησιμοποιούνται για να προσδιοριστεί ο τρόπος μετακίνησης πακέτων από ένα δίκτυο σε ένα άλλο. Για να μπορέσουν να μεταφερθούν οι πληροφορίες από το ένα σημείο σε ένα άλλο, όλοι οι τύποι πρωτοκόλλων είναι βασισμένοι στη δρομολόγηση. Σε αυτό περιλαμβάνονται το IP, το IPX της Novell και το DDP της Apple. Συνήθως είναι δυναμική η διαμόρφωση της δρομολόγησης στο διαδίκτυο. Παρόλα αυτά, όταν δημιουργούνται στατικές διαδρομές αποτελούν μια μορφή βασικής δρομολόγησης. Τα δυναμικά πρωτόκολλα δρομολόγησης κάνουν συνεχή αναζήτηση της καλύτερης διαδρομής για να μπορέσει να μεταφερθεί η πληροφορία από την πηγή στο δίκτυο στόχο.

Πίνακες δρομολόγησης

Καθώς συνδέουν δίκτυα μεταξύ τους, οι δρομολογητές αποτελούν κάποια από τα βασικά δομικά στοιχεία των δικτύων. Κάθε δρομολογητής περιέχει δύο ή και περισσότερες διεπαφές, οι οποίες ενώνουν ξεχωριστά δίκτυα μεταξύ τους. Στην περίπτωση που ένας δρομολογητής λάβει ένα πακέτο, εξετάζεται η διεύθυνση IP, καθορίζοντας έτσι σε ποια διεπαφή θα προωθηθεί το πακέτο. Όταν το δίκτυο είναι μικρό και δεν είναι περίπλοκο, τότε μπορεί να οριστεί από έναν διαχειριστή μια σταθερή διαδρομή την οποία θα ακολουθήσει όλη η κίνηση. Συνήθως, στα πιο περίπλοκα δίκτυα δρομολογούνται πακέτα με την παρατήρηση κάποιας μορφής μέτρησης.

Οι πίνακες δρομολόγησης περιλαμβάνουν τον ακόλουθο τύπο πληροφοριών:

- Εύρος ζώνης : αποτελεί μια κοινή μέτρηση βασισμένη στη χωρητικότητα μιας σύνδεσης. Αν όλες οι υπόλοιπες μετρήσεις ήταν ίσες, τότε ο δρομολογητής θα επέλεγε τη διαδρομή με το μεγαλύτερο εύρος ζώνης.
- Κόστος : Στη διάθεση του οργανισμού μπορεί να βρίσκεται μια γραμμή ISDN και μια αποκλειστική γραμμή T1. Στην περίπτωση που η γραμμή ISDN έχει υψηλότερο κόστος, η κυκλοφορία θα δρομολογείται μέσω του T1.
- Καθυστέρηση : Η καθυστέρηση αποτελεί ακόμη μια κοινή μέτρηση, καθώς μπορεί να είναι βασισμένη σε πολλούς παράγοντες, ανάμεσα στους οποίους είναι και η συμφόρηση, το εύρος ζώνης και οι ουρές δρομολογητή.
- Απόσταση : Η μέτρηση της απόστασης υπολογίζεται σε hops, δηλαδή πόσοι δρομολογητές μακριά βρίσκεται ο προορισμός.
- Φορτίο : Η μέτρηση του φορτίου, είναι η μέτρηση του φορτίου που τοποθετείται σε ένα συγκεκριμένο δρομολογητή. Ο υπολογισμός της μπορεί να γίνει με τη χρήση της CPU ή με την εξέταση του χρόνου επεξεργασίας.
- Αξιοπιστία : Η μέτρηση της αξιοπιστίας εξετάζει τις αυθαίρετες αξιολογήσεις αξιοπιστίας. Οι υπεύθυνοι εκχώρησης αυτών των αριθμητικών τιμών σε διάφορους συνδέσμους είναι οι διαχειριστές δικτύου.

Το πρωτόκολλο της δρομολόγησης, συμβουλευμένοι τον πίνακα δρομολόγησης και εφαρμόζοντας τη μέτρηση αυτή, μπορεί να κάνει υπολογισμό της καλύτερης διαδρομής. Στο σημείο αυτό προωθείται το πακέτο στο επόμενο hop όσο συνεχίζεται το ταξίδι του προς τον προορισμό του.

Αρχιτεκτονική δρομολογητή

Η αρχιτεκτονική του δρομολογητή σχεδιάστηκε με τέτοιο τρόπο ώστε να είναι εξοπλισμένοι οι δρομολογητές στην εκτέλεση δύο κύριων λειτουργιών :

Την επεξεργασία πρωτοκόλλων δρομολόγησης, στα οποία χρησιμοποιούνται τα πρωτόκολλα δρομολόγησης για τον προσδιορισμό της καλύτερης διαδρομής. Ξεκινώντας από την επανεξέταση των δρομολογούμενων πρωτοκόλλων, το καλύτερο παράδειγμα αποτελεί η IP. Αν οριστεί με έναν πάρα πολύ απλό ορισμό η IP, είναι ότι ο ρόλος της είναι ο ταχυδρόμος του διαδικτύου. Η δουλειά της δηλαδή είναι να οργανώνει δεδομένα σε κάποιο πακέτο το οποίο απευθύνεται στη συνέχεια για παράδοση. Οφείλει να τοποθετήσει μια διεύθυνση πηγής και προορισμούς του πακέτου.

Κάτι τέτοιο θεωρείται παρόμοιο με τη διεύθυνση ενός πακέτου πριν παραδοθεί στο ταχυδρομείο. Στον κόσμο της IP, τα αντίστοιχα ταχυδρομικά τέλη είναι ένα TTL (Time-to-Live), στο οποίο τα πακέτα εμποδίζονται να διασχίσουν το δίκτυο για πάντα. Στην περίπτωση που δεν βρεθεί ο παραλήπτης, μπορεί τελικά να γίνει απόρριψη του πακέτου. Όλοι οι υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο έχουν διεύθυνση IP. Στην αναλογία με το ταχυδρομικό σύστημα η διεύθυνση αυτή μπορεί να θεωρηθεί ένας συνδυασμός οδού και ταχυδρομικού κώδικα. Η χρήση του πρώτου μισού της διεύθυνσης IP, είναι για να προσδιοριστεί ο κεντρικός υπολογιστής. Η χρήση του δεύτερου τμήματος της διεύθυνσης προσδιορίζει τον κεντρικό υπολογιστή. Αυτό συνδυαστικά επιτρέπει την επικοινωνία με οποιοδήποτε κεντρικό υπολογιστή και δίκτυο στον κόσμο το οποίο είναι συνδεδεμένο στο διαδίκτυο.

Πρωτόκολλα δρομολόγησης

Ο διαχωρισμός των πρωτοκόλλων δρομολόγησης γίνεται σε δύο βασικές κατηγορίες, στα στατικά και δυναμικά. Η στατική ή αλλιώς σταθερή δρομολόγηση, αποτελείται από έναν πίνακα ο οποίος αναπτύχθηκε από έναν διαχειριστή δικτύου και αντιστοιχίζει ένα δίκτυο. Στη στατική δρομολόγηση γίνεται καλύτερη λειτουργία όταν το δίκτυο είναι μικρό και έχει προβλέψιμη κίνηση. Το μεγαλύτερο πρόβλημα που παρουσιάζεται με τη στατική δρομολόγηση, είναι ότι όταν γίνονται αλλαγές στο δίκτυο δεν μπορεί να αντιδράσει. Όσο μεγαλώνει το δίκτυο μπορεί να γίνει και δυσκολότερη η διαχείριση των πινάκων. Αυτό μπορεί να καταστήσει ακατάλληλη τη στατική δρομολόγηση για τη χρήση σε μεγάλα δίκτυα ή στο διαδίκτυο, μπορεί όμως να χρησιμοποιηθεί σε

κάποιες ειδικές περιπτώσεις όπου συνήθως δεν λειτουργούν καλά τα πρωτόκολλα δρομολόγησης.

Στη δυναμική δρομολόγηση, χρησιμοποιούνται μετρήσεις για να καθοριστεί ποια διαδρομή πρέπει να ακολουθηθεί από το δρομολογητή, ώστε να στείλει το πακέτο προς τον προορισμό του. Τα πρωτόκολλα αυτά περιλαμβάνουν το πρωτόκολλο πρώτα η συντομότερη διαδρομή (OSPF), Interior Gateway Routing Protocol (IGRP), Interior Gateway Routing Protocol (IGRP) και πληροφοριών δρομολόγησης (RIP). Ο διαχωρισμός της δυναμικής δρομολόγησης μπορεί να γίνει σε δύο μεγάλες κατηγορίες : στα διανύσματα απόστασης ή στα πρωτόκολλα δυναμικής δρομολόγησης κατάστασης σύνδεσης.

RIP

Το RIP αποτελεί ένα από τα πιο κοινά πρωτόκολλα δρομολόγησης το οποίο χρησιμοποιεί ως κύρια μέτρηση της δρομολόγησης ένα πλήθος αναπήδησης. Θεωρείται ένα πρωτόκολλο διανυσμάτων απόστασης. Μια από τις βασικές μεθοδολογίες του πρωτοκόλλου διανυσμάτων αποστάσεις είναι η λήψη απόφασης για το ποια θεωρείται η καλύτερη διαδρομή με τον προσδιορισμό της συντομότερης διαδρομής. Συνήθως το συντομότερο μονοπάτι υπολογίζεται με hoop. Η δρομολόγηση αυτή ονομάζεται επίσης και δρομολόγηση κατά φήμη.

OSPF

Το OSPF αποτελεί ένα από τα πιο κοινά πρωτόκολλα δρομολόγησης κατάστασης σύνδεσης το οποίο χρησιμοποιείται αρκετές φορές αντικαθιστώντας το RIP. Αυτά τα πρωτόκολλα ονομάζονται σωστότερα ως αλγόριθμοι Dijkstra, καθώς αυτή είναι η υπολογιστική βάση του σχεδιασμού τους. Χρησιμοποιούν, λοιπόν, τον αλγόριθμο αυτό για να μπορέσουν να υπολογίσουν την καλύτερη διαδρομή προς ένα δίκτυο στόχο. Ο προσδιορισμός της καλύτερης διαδρομής μπορεί να γίνει από μία και περισσότερες μετρήσεις όπως είναι το εύρος ζώνης, η καθυστέρηση ή τα άλματα. Από τη στιγμή που θα καθοριστεί η διαδρομή, ενημερώνονται οι υπόλοιποι δρομολογητές από το δρομολογητή αυτό ως προς τα ευρήματά του. Με τον τρόπο αυτό, αναπτύσσονται αξιόπιστοι πίνακες δρομολόγησης οι οποίοι φτάνουν σε σύγκλιση. Πιο ισχυρή από τη δρομολόγηση πρωτοκόλλων διανυσμάτων απόστασης θεωρείται η δρομολόγηση κατάστασης. Ένας από τους λόγους είναι ούτε τα πρωτόκολλα κατάστασης έχουν τη δυνατότητα εκτέλεσης ταχύτερης δρομολόγησης ενημέρωσης του πίνακα.

5.2 Hacking Routers

Αν ελέγχεται πλήρως ένας δρομολογητής κάτι τέτοιο μπορεί να οδηγήσει και στο να ελέγχεται πλήρως και ένα δίκτυο. Για το λόγο αυτό, γίνεται στόχευση των δρομολογητών από τους εισβολείς οι οποίοι εξαπολύουν επιθέσεις εναντίον τους. Οι επιθέσεις αυτές μπορούν να επικεντρωθούν σε κάποια γνωστά τρωτά σημεία, σφάλματα διαμόρφωσης ή ακόμα και αδύναμους κωδικούς πρόσβασης.

Επιθέσεις δρομολογητή

Η επίθεση στους δρομολογητές μπορεί να γίνει είτε δηλητηριάζοντας τον πίνακα δρομολόγησης, πλημμυρίζοντας το εύρος ζώνης, εκτοξεύοντας επιθέσεις DoS και αλλάζοντας τη διαμόρφωση του αρχείου. Οι επιθέσεις αυτές μπορούν να είναι είτε hit and run, είτε επίμονες. Ο στόχος των επιθέσεων άρνησης υπηρεσίας είναι οι δρομολογητές. Αν ο εισβολέας καταφέρει να αναγκάσει το δρομολογητή, να σταματήσει να προωθεί πακέτα τότε όσοι κεντρικοί υπολογιστές βρίσκονται πίσω από το δρομολογητή ουσιαστικά απενεργοποιούνται.

Τοπολογία επίθεσης δρομολογητή

Η τοπολογία επίθεσης δρομολογητή είναι ίδια με όλες τις τοπολογίες επίθεσης. Τα βήματα περιλαμβάνουν:

1. Αναγνώριση
2. Σάρωση και απαρίθμηση
3. Απόκτηση πρόσβασης
4. Κλιμάκωση προνομίου
5. Διατήρηση της πρόσβασης
6. Κάλυψη τροχιών και τοποθέτηση κερκόπορτων

Επιθέσεις άρνησης υπηρεσίας

Οι επιθέσεις Denial-of-Service (DoS) χωρίζονται σε τρεις κατηγορίες:

- Καταστροφή. Επιθέσεις που καταστρέφουν την ικανότητα λειτουργίας του δρομολογητή.
- Κατανάλωση πόρων. Πλημμύρισμα του δρομολογητή με πολλές ανοιχτές συνδέσεις ταυτόχρονα.

- Κατανάλωση εύρους ζώνης. Επιθέσεις που προσπαθούν να καταναλώσουν το εύρος ζώνης χωρητικότητα του δικτύου του δρομολογητή.

Με τις επιθέσεις αυτές μπορεί να γίνει στόχευση είτε ενός ολόκληρου οργανισμού είτε ενός μεμονωμένου χρήστη, ενώ μπορούν να επηρεάσουν είτε τη διαθεσιμότητα ολόκληρου του δικτύου είτε τα συστήματα στόχου. Ο αντίκτυπος της επίθεσης αυτής, είναι να διακοπεί η κανονική λειτουργία και επικοινωνία. Για έναν επιτιθέμενο είναι ευκολότερο να το πετύχει αυτό ώστε να μπορέσει να αποκτήσει πρόσβαση στις περισσότερες περιπτώσεις. Για παράδειγμα, μια κοινή επίθεση DoS αποτελεί το Smurf, το οποίο κάνει εκμετάλλευση του πρωτοκόλλου Internet Control Message Protocol (ICMP), με την αποστολή ενός πλαστού πακέτου ping, απευθυνόμενο στη διεύθυνση εκπομπής, ενώ ως θύμα αναφέρεται η διεύθυνση πηγής. Ενδέχεται να υπάρξει απάντηση από πολλά συστήματα σε ένα δίκτυο πολλαπλής πρόσβασης. Σαν αποτέλεσμα της επίθεσης, είναι ότι το θύμα πλημμυρίζεται από απαντήσεις ping.

Ένα άλλο παράδειγμα επίθεσης DoS αποτελεί και το SYN flood. Η επίθεση αυτή κάνει διακοπή του πρωτόκολλο ελέγχου μετάδοσης (TCP) με την αποστολή ενός μεγάλου αριθμού πλαστών πακέτων τα οποία φέρουν το σύνολο σημαιών SYN. Η προσωρινή μνήμη στο σύστημα του θύματος γεμίζει από τον μεγάλο αριθμό μισάνοιχτων συνδέσεων TCP εμποδίζοντάς το να δεχτεί νόμιμες συνδέσεις. Τα συνδεδεμένα στο διαδίκτυο συστήματα τα οποία παρέχουν υπηρεσίες όπως είναι οι HTTP ή SMTP, θεωρούνται ιδιαίτερα ευάλωτα. Ένας δεύτερος τύπος επιθέσεων DoS, οι οποίες θεωρούνται και επιθέσεις πολλαπλών πρωτοκόλλων, είναι οι επιθέσεις DDoS. Οι επιθέσεις αυτές κάνουν χρήση των πακέτων ICMP, UDP και TCP. Από τους πιο ευδιάκριτες διαφορές ανάμεσα στους δύο αυτούς τύπους επιθέσεων, είναι ότι η επίθεση DDoS αποτελείται από δύο διακριτές φάσεις.

Στην πρώτη φάση στην προ επίθεση, οι χάκερ προσπαθούν να παραβιάσουν υπολογιστές οι οποίοι βρίσκονται διάσπαρτες στο διαδίκτυο φορτώνοντας λογισμικό στους πελάτες έτσι ώστε να βοηθήσουν στην επίθεση. Στους στόχους μιας τέτοιας επίθεσης περιλαμβάνονται κακώς διαμορφωμένα δίκτυα, οι οικιακοί χρήστες, πανεπιστήμια, κολέγια, και οι χρήστες ευρυζωνικότητας. Με την ολοκλήρωση του πρώτου βήματος ξεκινά το δεύτερο βήμα το οποίο είναι και η πραγματική επίθεση. Στο βήμα αυτό, ο εισβολέας δίνει μια εντολή στους masters να επικοινωνήσουν με τα zombies, ώστε να ξεκινήσει η επίθεση. Μπορεί να γίνει εύκολος αποκλεισμός των

πακέτων ICMP και UDP. Είναι δύσκολος όμως ο μετριασμός των πακέτων TCP. Οι βασισμένες σε TCP επιθέσεις DoS εντοπίζονται σε δύο μορφές:

- Προσανατολισμένες στη σύνδεση. Για να μπορέσουν να δημιουργήσουν μια σύνδεση, οι επιθέσεις αυτές ολοκληρώνουν τη χειραψία τριών κατευθύνσεων. Σε αυτού του τύπου τις επιθέσεις μπορεί να προσδιοριστεί η διεύθυνση IP της πηγής.
- Χωρίς σύνδεση. Είναι δύσκολη η ανίχνευση αυτών των πακέτων SYN.

Το Tribal Flood Network (TFN) αποτελεί ένα παράδειγμα εργαλείου DDOS και ήταν το πρώτο δημόσια διαθέσιμο εργαλείο DDoS βασισμένο σε UNIX. Το εργαλείο αυτό μπορεί να κάνει εκκίνηση των επιθέσεων ICMP, Smurf, UDP και SYN flood. Χρησιμοποιεί κυρίως τη θήρα UDP 31335 και τη θύρα TCP 27665. Στη συνέχεια, ακολούθησαν περισσότερο προηγμένες επιθέσεις όπως είναι το Trinoo. Το συγκεκριμένο DDoS καθώς είναι στενά συνδεδεμένο με το TFN, μπορεί να επιτρέψει στο χρήστη την εκκίνηση μιας συντονισμένης UDP flood στον υπολογιστή του θύματος, στον οποίο γίνεται υπερφόρτωση της κίνησης. Σε μια τυπική ομάδα επίθεσης περιλαμβάνονται μόνο λίγοι διακομιστές και ένας αρκετά μεγάλος αριθμός υπολογιστών πελατών όπου εκτελείται και το Trinoo. Θεωρείται αρκετά εύκολο στη χρήση από έναν εισβολέα και πολύ ισχυρό, καθώς ένας υπολογιστής μπορεί να δώσει οδηγίες σε πολλούς διακομιστές Trinoo να ξεκινήσουν μια επίθεση DoS απέναντι σε ένα συγκεκριμένο υπολογιστή.

Routing Table Poisoning

Θεωρούνται ιδιαίτερα ευάλωτες σε επιθέσεις δηλητηρίασης πίνακα δρομολόγησης ή δρομολογητές οι οποίοι εκτελούν RIPv1. Ως εγκεκριμένος τύπος επίθεσης, τροποποιεί γνήσια πακέτα ενημέρωσης διαδρομής σε άλλους κόμβους ή στέλνει ψεύτικες ενημερώσεις δρομολόγησης με τα οποία επιχειρεί ο εισβολέας να προκαλέσει άρνηση υπηρεσίας. Μπορεί να προκαλέσει μια πλήρη άρνηση εξυπηρέτησης ή να καταλήξει σε μια μη βέλτιστη δρομολόγηση ή να συμφορήσει τμήματα του δικτύου.

Hit-and-Run Attacks και Persistent Attacks

Οι επιτιθέμενοι έχουν τη δυνατότητα να εξαπολύσουν έναν από τους δύο τύπους αυτούς επιθέσεων. είναι δύσκολος ο εντοπισμός και η απομόνωση μιας επίθεσης τύπου hit and run, επειδή ο εισβολέας εκτελεί ή μόνο μία ή κάποιες κακές μορφές πακέτων. Στην προσέγγιση αυτή, ο εισβολέας οφείλει να δημιουργήσει τις επιθέσεις του με τέτοιο τρόπο ώστε να υπάρχει μια διαρκής καταστροφική επίδραση των αποτελεσμάτων του. Μια επίθεση της μορφής persistent attack, μπορεί να αυξήσει την πιθανότητα να αναγνωριστεί ο εισβολέας, καθώς υπάρχει μια συνεχόμενη ροή πακέτων προς ανάλυση. Η επίθεση αυτή, ωστόσο, μειώνει το επίπεδο της πολυπλοκότητας το οποίο θεωρείται απαραίτητο στον εισβολέα με τη χρησιμοποίηση πολύ λιγότερο εξελιγμένων επιθέσεων. Κάποιοι σύνδεσμοι πρωτοκόλλων δρομολόγησης κατάστασης όπως είναι το OSPF, θεωρούνται πιο ανθεκτικά στην περίπτωση επίθεσης δρομολόγησης από το RIP.

5.3 Διερεύνηση δρομολογητών

Καθώς διερευνώνται οι δρομολογητές, εμφανίζεται μια σειρά από ενσωματωμένες εντολές που χρησιμοποιούνται για την ανάλυση. Δεν συνιστάται να επαναφερθεί ο δρομολογητής καθώς κάτι τέτοιο μπορεί να καταστρέψει όποια στοιχεία δημιουργήθηκαν από τον εισβολέα. Οι εντολές εμφάνισης οι οποίες γράφονται παρακάτω μπορούν να χρησιμοποιηθούν για να μπορέσουν να συλλεχθούν βασικές πληροφορίες και να εγγραφεί η δραστηριότητα ενός χάκερ :

- Εμφάνιση λίστας πρόσβασης
- Εμφάνιση ρολογιού
- Εμφάνιση διαδρομής ip
- Εμφάνιση διαμόρφωσης εκκίνησης
- Εμφάνιση χρηστών
- Εμφάνιση έκδοσης

Chain of Custody

Το chain of custody μπορεί να χρησιμοποιηθεί για να αποδειχθεί η ακεραιότητα των αποδεικτικών στοιχείων. Οφείλει να είναι σε θέση να απαντήσει στις ακόλουθες ερωτήσεις :

- Ποιος συγκέντρωσε τα στοιχεία;
- Που και πως αποθηκεύονται τα αποδεικτικά στοιχεία;

- Ποιος κατείχε τα αποδεικτικά στοιχεία;
- Πώς προστατεύτηκαν κατά την αποθήκευση και πώς αποθηκεύτηκαν τα αποδεικτικά στοιχεία;
- Ποιος έβγαλε τα αποδεικτικά στοιχεία από την αποθήκευση και γιατί;

Δεν υπάρχει η περίπτωση της υπερβολικής τεκμηρίωσης. Σε μια καλή προσέγγιση υπάρχουν δύο άνθρωποι οι οποίοι εργάζονται σε μια υπόθεση. Την ώρα που το ένα άτομο θα κάνει ανάλυση του υπολογιστή, το άλλο κάνει τεκμηρίωση των ενεργειών αυτών. Όταν ξεκινά μια έρευνα, ο ερευνητής οφείλει να ετοιμάσει ένα αρχείο καταγραφής για να μπορέσει να τεκμηριώσει τη συστηματική διαδικασία της έρευνας. Κάτι τέτοιο είναι απαραίτητο και στην περίπτωση αυτή. Εδώ τεκμηριώνεται ο χειρισμός των αποδεικτικών στοιχείων, η προστασία τους, η διαδικασία η οποία χρησιμοποιείται για να επαληθευτεί ότι παραμένουν αμετάβλητα, καθώς επίσης και ο τρόπος αντιγραφής τους. Στη συνέχεια ερευνείται το log, στο οποίο εξετάζεται ο τρόπος εξέτασης των media, ποια εργαλεία χρησιμοποιούνται και ποιες ενέργειες λαμβάνονται. Μπορούν να συγκεντρωθούν πολλές πληροφορίες για τον ανακριτή από αυτοματοποιημένα εργαλεία όπως είναι το Forensic Toolkit και το EnCase.

Αστάθεια των αποδεικτικών στοιχείων

Η απόκτηση των ασταθών δεδομένων θα πρέπει να συλλέγεται το συντομότερο δυνατό κατά την απόκριση σε μια επίθεση δικτύου. Στην περίπτωση που όλοι οι δρομολογητές είναι διαφορετικοί, τότε πιθανότατα αφορά προϊόντα Cisco, καθώς κατέχουν ένα αρκετά μεγάλο μερίδιο αγοράς. Οι δρομολογητές αυτοί, μπορούν να αποθηκεύσουν την τρέχουσα διαμόρφωση nonvolatile ram (NVRAM). Αυτή θεωρείται πτητική, ενώ τα δεδομένα διατηρούνται στη μνήμη τυχαίας πρόσβασης (RAM). Στην περίπτωση που απενεργοποιηθεί, διαμορφωθεί ή διαγραφεί ο δρομολογητής, χάνονται πληροφορίες. Η χρήση των δρομολογητών γίνεται κυρίως ως την αιχμή της επίθεσης. Κάτι τέτοιο σημαίνει ότι μπορεί να παίξει ενεργό ρόλο στην εισβολή ένας δρομολογητής, καθώς χρησιμοποιείται από τον εισβολέα ως τη μετάβαση από το ένα σημείο του εξοπλισμού δικτύου σε ένα άλλο. Κατά την εκκίνηση της έρευνας, ο ερευνητής πρέπει πάντα να μετακινηθεί από το πιο ευμετάβλητο στο λιγότερο ευμετάβλητο. Ένα πρώτο βήμα είναι η ανάκτηση της μνήμης RAM και NVRAM.

Μπορεί να χρησιμοποιηθεί μια απευθείας σύνδεση στη θύρα της κονσόλας με τη χρήση ενός καλωδίου RJ-45-RJ-45 και ενός θηλυκού RJ-45-to-DB-9 προσαρμογέα DTE. Σε

κάποια περίπτωση που δεν είναι διαθέσιμη η άμεση σύνδεση, τότε η επόμενη προτεινόμενη μέθοδος είναι μια απομακρυσμένη συνεδρία. Καθώς δεν μπορούν να χρησιμοποιηθούν μη ασφαλή πρωτόκολλα όπως είναι το FTP, προτιμάται ένα επαγγελματικό κρυπτογραφικό εργαλείο το Tocol Secure Shell (SSH). Ο ερευνητής φροντίζει να καταγράφει τόσο την πτητική όσο και τη μη πτητική διαμόρφωση, ώστε να μπορέσει να συγκρίνει τις αλλαγές και τους σκοπούς τεκμηρίωσης. Οι δρομολογητές της εταιρείας Cisco περιέχουν πολλαπλούς τρόπους λειτουργίας. Για να μπορέσει, συνεπώς, να αποκτήσει τη λειτουργία του προνομίου, οφείλει να είναι γνωστός από τον αναλυτή ο κωδικός πρόσβασης.

Αναφορές περιπτώσεων

Από τις πιο σημαντικές πτυχές της εγκληματολογίας υπολογιστών είναι η αναφορά των υποθέσεων. Παρόμοια με την παραδοσιακή εγκληματολογία πρέπει να γίνεται τεκμηρίωση στα πάντα. Η αναφορά ξεκινά από το πρώτο λεπτό στο οποίο βρίσκεται ο ερευνητής στην υπόθεση. Αν και κάποιες φορές μπορεί να φαίνεται ευκολότερο απλά να προχωρήσει προς τα μπρος, μια αποτυχία στην τεκμηρίωση μπορεί να οδηγήσει σε αναφορές οι οποίες είναι κακογραμμένες και δεν θα αντέξουν σε νομικό έλεγχο. Η τεκμηρίωση την οποία κρατά ο ερευνητής είτε αναιρεί είτε επικυρώνει τα αποδεικτικά στοιχεία. Συνεπώς, για να μπορέσουν να συγκεντρωθούν τα τρία βασικά στοιχεία της εγκληματολογίας δηλαδή η ανάλυση, ο έλεγχος ταυτότητας και η απόκτηση, είναι η έκθεση. Το κλειδί για να περιοριστεί μία από τις ακόλουθες ενέργειες είναι η αναφορά περίπτωσης :

- Αποκατάσταση εργαζομένων
- Απόλυση υπαλλήλου
- Πολιτική δίκη
- Ποινική δίωξη

Η τελική γραπτή έκθεση συντάσσεται μετά την ολοκλήρωση της έρευνας. Κάποια από τα στοιχεία τα οποία βρίσκονται στην αναφορά αυτή περιλαμβάνουν :

- Περίληψη υπόθεσης
- Αρχεία ελέγχου υπόθεσης
- Σελιδοδείκτες
- Επιλεγμένα γραφικά

- Διαδρομή τοποθεσίας αρχείου
- Ιδιότητες τοποθεσίας αρχείου

Δεν θεωρείται ολοκληρωμένη μία λίστα αν δε δίνει κάποιες ενδείξεις για το τι πρέπει να συμπεριλαμβάνεται. Τα περιεχόμενα της αναφοράς διαφέρουν ανάλογα με την εταιρεία. Αυτό που συνεπάγεται, είναι ότι μπορεί να γίνει χρήση των αρχείων καταγραφής και της αναφοράς από τον οποιοδήποτε αναδημιουργώντας τα βήματα τα οποία εκτελούνται καθ' όλη τη διάρκεια της έρευνας. Με τη διαδικασία της επικάλυψης οδηγούνται σε πανομοιότυπα αποτελέσματα.

5.4 Αντιμετώπιση περιστατικού

Η προσπάθεια ενός οργανισμού για την τεκμηρίωση και τον ορισμό της φύσης και το πεδίο εφαρμογής κάποιου περιστατικού ασφάλειας υπολογιστή, είναι η απόκριση σε περιστατικά. Μπορεί να χωριστεί σε τρεις μεγάλες κατηγορίες οι οποίες περιλαμβάνουν :

- Ειδοποίηση και αναγνώριση Triage
- Δράση/Αντίδραση, παρακολούθηση, ανάλυση, περιορισμός
- Πρόληψη, παρακολούθηση και αποκατάσταση επισκευής

Συμβιβασμοί

Οι ερευνητές οφείλουν να ειδοποιηθούν ότι συνέβη κάτι πριν καθοριστεί ένας συμβιβασμός. Η λειτουργία ειδοποίησης είναι καλύτερο να θεωρείται όσο το δυνατόν περισσότερο αυτοματοποιημένη. Σε διαφορετική περίπτωση, θα ήταν συντριπτικός ο όγκος των πληροφοριών καταγραφής για έναν υπάλληλο. Ακόμη και στην περίπτωση που υπάρχει υψηλό επίπεδο αυτοματοποίησης, θα πρέπει να εκτελεστεί η εγκυρότητα της ειδοποίησης. Από τη στιγμή που επίθεση θα έχει επικυρωθεί μια φορά, είναι σημαντικό να γίνει μείωση της ζημιάς της επίθεσης το γρηγορότερο δυνατό, ενώ εργάζονται για να αποκατασταθούν οι κανονικές επιχειρηματικές λειτουργίες.

Κεφάλαιο 6ο

Συμπεράσματα

Στη διπλωματική αυτή, μελετάται μια σύντομη εισαγωγή στην ψηφιακή εγκληματολογία, διάφορες κυβερνοεπιθέσεις καθώς και οι συνεχόμενες τρέχουσες τάσεις οι οποίες εντοπίζονται από πολλούς ειδικούς. Το μέλλον της ψηφιακής εγκληματολογίας είναι επικεντρωμένο από τους ερευνητές σε συγκεκριμένες τακτικές ικανότητες οι οποίες είναι υπό ανάπτυξη. Στη μελέτη αυτή παρουσιάζονται επίσης οι

κύριες προκλήσεις τις οποίες αντιμετωπίζουν οι ερευνητές. Όπως αναφέρθηκε στα προηγούμενα κεφάλαια, οι υποκείμενες τεχνικές και τεχνολογίες αναπτύσσονται με τρομερούς ρυθμούς. Διάφοροι τύποι ψηφιακών συσκευών θα συνεχίσουν να διαφέρουν ανάμεσα σε άλλες συσκευές. Οι διαφορετικές πλατφόρμες χρησιμοποιούνται ως μορφές αποθήκευσης για τις μεθόδους επικοινωνίας, τα στοιχεία, τη δομή και το σχήμα τους. Οι αναβαθμίσεις στο μάρκετινγκ των Media, εξακολουθεί να προκαλεί τη δημιουργικότητα και την προσοχή των χρηστών.

Με όμοιο τρόπο όπως εξελίσσονται οι εγκληματολογικές τεχνικές, παράλληλα γίνεται σημείωση βελτιώσεων στις υποκείμενες τεχνολογίες, ενώ προσδιορίζεται η ταχύτητα με την οποία γίνεται η ανάπτυξη της τεχνολογίας. Υπάρχει μια γρήγορη στροφή των ανθρώπων σε μεθόδους των σύγχρονων εργαλείων επικοινωνίας όπως είναι οι πλατφόρμες μέσων κοινωνικής δικτύωσης και ο εκσυγχρονισμός των φορητών συσκευών τους. Όπως προαναφέρθηκε, σε άλλες παρόμοιες επιστήμες, μια ψηφιακή εγκληματολογική προσέγγιση δεν έχει καινοτόμο χαρακτήρα, απαιτεί όμως συνεχή ενημέρωση ώστε να διατηρείται ενημερωμένη να προτρέχει της τρέχουσας τεχνολογίας. Καθώς εξελίσσονται ραγδαία οι ψηφιακές συσκευές, απαιτείται από τους εγκληματολογικούς ερευνητές η χρήση νέων εργαλείων και μεθοδολογιών ώστε να μπορέσουν να αποκτήσουν με νόμιμο τρόπο τα αποδεικτικά στοιχεία τα οποία πρέπει να προσκομιστούν σε ένα δικαστήριο.

Σαν πρώτο βήμα για να μειωθεί το ζήτημα του απορρήτου, θεωρείται απαραίτητη η αντιμετώπιση της βασικής αιτίας του προβλήματος. Η λύση τέτοιου είδους προβλημάτων βρίσκεται στο μυαλό του. Η εκπαίδευση του ανθρώπινου νου ώστε να μπορέσει να γίνει ένα ηθικό άτομο στη δουλειά του, είναι ένας από τους βασικούς παράγοντες ο οποίος θα συμβάλει στο να μειωθούν οι ανησυχίες για το απόρρητο. Καθώς οι διαδικασίες της εκπαίδευσης των ανθρώπων σχετικά με την ασφάλεια οφείλουν να είναι επαρκώς ευεργετικές, οι άνθρωποι ως όντα τείνουν να εξερευνούν κάτι νέο. Συνεπώς, όσο δυνατό και αν είναι να μεταμορφωθούν τα εργαλεία εγκληματολογίας υπολογιστών για ένα ανήθικο μυαλό, το απόρρητο των συνδεδεμένων μερών του μπορεί να τεθεί σε κίνδυνο. Για αυτό το λόγο, πρέπει να δημιουργηθεί ένα αποτελεσματικά σταθερό και ασφαλές υπολογιστικό δικτυακό πλαίσιο το οποίο μπορεί να εξασφαλίσει το απόρρητο. Ένα άλλο σημαντικό σημείο, είναι ότι υπάρχουν καινοτόμες μέθοδοι ώστε να μπορέσει να ελεγχθεί η ταυτότητα, η

εγκυρότητα και η αξιοπιστία των ψηφιακών αποδεικτικών στοιχείων, καθώς και των νομικών και επιστημονικών προτύπων.

Συνεπώς, θα πρέπει να μετρούνται όσο το δυνατόν περισσότερο τα ποσοστά στατιστικών σφαλμάτων, έτσι ώστε οι συγκεκριμένες μέθοδοι να καθορίζουν το ποσοστό εμπιστοσύνης. Με τον τρόπο αυτό, οι επιστήμονες της ψηφιακής εγκληματολογίας επικεντρώνονται στο να αναπτυχθούν επιτυχημένες μέθοδοι και μοντέλα δοκιμών ώστε να αποκτηθεί νομική αναγνώριση και επιστημονική επικύρωση και έγκριση. Συνήθως υπάρχει οργάνωση των κυβερνητικών οργανισμών με ένα γραφειοκρατικό τρόπο. Η εστίασή τους στο να ελαχιστοποιήσουν τους κινδύνους, οδηγεί σε μια αργή λήψη απόφασης. Το ψηφιακό εγκληματολογικό πεδίο σε αντίθεση εξελίσσεται ραγδαία, ζητώντας μια θετική και ευέλικτη οργάνωση. Μια ατελής ή λάθος εφαρμογή, μπορεί να υπονομεύσει την υιοθέτηση η οποία μειώνει τα λαμβανόμενα οφέλη.

Ακόμη και αν δεν υπάρχει λεπτομερής ερευνητική αξιολόγηση, οι ανακριτές των υποθέσεων μπορούν να χρησιμοποιήσουν την τακτική αυτή των πληροφοριών για ερευνητικούς σκοπούς. Απαιτείται φυσικά μια συνεργασία με ψηφιακούς εμπειρογνώμονες, ώστε να εξηγηθούν λεπτομερώς τα ψηφιακά στοιχεία και να ξεχωρίσει η προέλευση των σχέσεων και των ιχνών τους. Διαφορετικά υπάρχει περίπτωση να βγουν ανεπιθύμητα συμπεράσματα. Οι καλές διεπαφές χρήστη και η προχωρημένη εκπαίδευση, μπορούν να βοηθήσουν στο να μειωθεί ο κίνδυνος αυτός.

Ένα δύσκολο έργο για κάθε ομάδα σήμανσης αποτελεί η εγκληματολογία του δρομολογητή. Το περιστατικό πρέπει να αναλυθεί όσο το δυνατόν γρηγορότερα. Κάτι τέτοιο ισχύει για κάθε εγκληματική υπόθεση είτε πρόκειται για δικτυωμένες συσκευές είτε για υπολογιστή. Στην περίπτωση της εγκληματολογίας του δρομολογητή, από την πλευρά των αναλυτών δεν είναι εύκολο καθώς οι δρομολογητές έχουν πολλά ασταθή δεδομένα και ακόμη και αν οι αναλυτές θεωρούνται οι εμπειρότεροι στο χώρο, αν δεν υπάρχουν στοιχεία στη συσκευή δεν υπάρχει υπόθεση. Ο σχεδιασμός της έρευνας αποτελεί και το πιο σημαντικό μέρος της για να μπορέσει να αντιμετωπιστεί το φαινόμενο αυτό. Η ερευνητική ομάδα πρέπει να εργαστεί γρήγορα ώστε να κατασκευάσει ένα σχέδιο σχετικά με το πού μπορούν να βρεθούν και ποια είναι τα πιθανά στοιχεία καθώς και με ποια σειρά πρέπει να αποκτηθούν. Ως τελικό βήμα,

πρέπει να δοθεί προτεραιότητα στα πιο ασταθή στοιχεία και να προχωρήσουν από εκεί. Όταν ετοιμαστεί το σχέδιο ξεκινά η ανάλυση.

Υπάρχουν δύο τρόποι για να αναλυθούν τα στοιχεία, η ζωντανή ανάλυση στο σύστημα με τη χρήση μιας κονσόλας όταν θεωρείται δυνατή η φυσική ή απομακρυσμένη πρόσβαση στο δρομολογητή με τη χρήση πρωτοκόλλου απομακρυσμένης σύνδεσης όπως είναι τα telnet ή ssh. Ο δεύτερος τρόπος είναι να εξαχθεί η ένδειξη μνήμης από το δρομολογητή και να αναλυθεί τοπικά σε έναν υπολογιστή. Αυτό μπορεί να γίνει και σε εικονικούς δρομολογητές δημιουργώντας ένα στιγμιότυπο του εικονικού δρομολογητή. Στους δρομολογητές που χρησιμοποιούν ζωντανή ανάλυση η χρήση της εντολής εντολή "write core dump", μπορεί να γίνει για να εξαχθούν κάποιες πληροφορίες σχετικά με τη διαδικασία της ζωντανής μνήμης του δρομολογητή. Η τρέχουσα διαμόρφωση του δρομολογητή θα πρέπει να αναζητείται πάντα από τους ερευνητές για να μπορέσουν να βρουν κάποιους από τους κανόνες οι οποίοι διαμορφώθηκαν.

Επίσης, πρέπει να δοκιμάσουν μέσα στην τρέχουσα διαμόρφωση για να μπορέσουν να βρεθούν τυχόν ενσωματωμένες μικροεφαρμογές διαχείρισης συμβάντων, οι οποίες περιμένουν να εκτελεστεί μια συγκεκριμένη δραστηριότητα. Θα πρέπει επίσης να γίνει αναζήτηση των χρηστών από την ομάδα οι οποίοι συνδέονται στο σύστημα, και αν ενεργοποιηθεί να χρησιμοποιήσουν το guestell. Το guestell μπορεί να τρέξει προσαρμοσμένη εφαρμογή Linux συμπεριλαμβανομένης της Python. Θα μπορούσε επίσης να κάνει εκμετάλλευση της εγκατάστασης ενός κακόβουλου λογισμικού ή απλά με τον προγραμματισμό μιας εργασίας cron η οποία εκτελείται περιοδικά. Τέλος, οι ερευνητές οφείλουν να υποβάλουν τη δική τους έκθεση στον οργανισμό με τα ευρήματά τους. Η έκθεση πρέπει να είναι ενδελεχής όπως και η έρευνά τους. Για να γίνει αυτό, πρέπει να είναι τεκμηριωμένα όλα τα βήματα τα οποία έκαναν κατά τη διερεύνηση του συστήματος.

Σε αυτή την αναφορά πρέπει να βρίσκεται κάθε εργαλείο που χρησιμοποίησαν και κάθε αρχείο σχετικό με το περιστατικό. Όταν η αναφορά είναι καλά τεκμηριωμένη, ο οργανισμός μπορεί να βοηθηθεί ώστε να καταλάβει τι πήγε στραβά και να μπορέσει να λάβει τα κατάλληλα μέτρα. Πρέπει να γίνεται παρουσίαση και καταγραφή κάθε αποδεικτικού στοιχείου στην έκθεση αυτή, που να εξηγείται και ο τρόπος με τον οποίο βρέθηκε. Πιο συγκεκριμένα η ομάδα πρέπει να απαντήσει στις ακόλουθες ερωτήσεις :

- Πού λάβατε τα αποδεικτικά στοιχεία
- Πότε λάβατε τα στοιχεία
- Από ποιον λάβατε τα στοιχεία
- Ποιες είναι οι μέθοδοι επιληπτικών κρίσεων
- Γιατί κατασχέσατε τα στοιχεία

Η εγκληματολογία του δρομολογητή δεν θεωρείται μια εύκολη υπόθεση, καθώς δεν υπάρχει ένας αυτοματοποιημένος τρόπος για να αναζητηθούν οι ασυνέπειες σε ένα δρομολογητή. Θα πρέπει οι ερευνητές να κάνουν μια βαθιά βουτιά στη χωματερή μνήμης καθώς και στα ανακτημένα συστήματα αρχείων, ενώ θα πρέπει να αφιερώσουν και χρόνο στο να εξετάσουν αρχεία και διαδικασίες που βρίσκονται εκεί. Η εγκληματολογία των δρομολογητών δεν θεωρείται απλά ένας υπό κλάδος της εγκληματολογίας δικτύου, αλλά έχει την ίδια και αν όχι μεγαλύτερη αξία της εγκληματολογίας δικτύου ανάμεσα σε δύο ή περισσότερους υπολογιστές. Αν πραγματοποιηθεί μια επιτυχημένη επίθεση σε ένα δρομολογητή, θα μπορούσε να θέσει σε κίνδυνο ολόκληρο το δίκτυο και όχι μόνο έναν υπολογιστή. Μια αποτελεσματική και άμεση απάντηση σε ένα περιστατικό, θα μπορούσε να εξοικονομήσει πολλά χρήματα για έναν οργανισμό.

Ένας οργανισμός όσο καλά προετοιμασμένος κι αν είναι, πάντα θα υπάρχει κάτι το οποίο δεν έχει προβλεφθεί από τους διαχειριστές και μπορεί να είναι αξιοποιήσιμο από τους εισβολείς, συνεπώς η καλύτερη λύση είναι μια καλά οργανωμένη μονάδα εγκληματολογίας η οποία θα περιορίσει τη ζημιά το περισσότερο δυνατό. Αν και για κάποιες από τις τοποθεσίες των αποδεικτικών στοιχείων ο τρόπος ανακάλυψης τους μπορεί να διαφέρει ανάλογα με την περίπτωση, ελπίζουμε ότι στη διατριβή αυτή καλύφθηκαν αρκετές πτυχές σχετικά με το πώς θα έπρεπε να σκέφτονται οι ερευνητές και που να αναζητούν ψηφιακά στοιχεία. Στην περίπτωση μελλοντικής εργασίας, θα μπορούσαν να αναφερθούν διαφορετικές περιπτώσεις χρήσης, οι οποίες θα συμβάλουν στο να διεξαχθεί μια πιο εμπεριστατωμένη μεθοδολογία ως προς το πώς, που γιατί μπορούν να στραφούν οι ερευνητές στους δρομολογητές. Με αυτό τον τρόπο, μπορούν να βοηθηθούν οι μελετητές στην αντιμετώπιση ενός περιστατικού πιο αποτελεσματικά και πιο γρήγορα.

Για να μπορέσουν να βρεθούν δεδομένα στο δρομολογητή, οι πληροφορίες παρέχονται σχετικά με τη χρήση του διαδικτύου η οποία γίνεται από άλλους χρήστες, έτσι ώστε να

μην μπορεί να γίνει κατάχρηση για κακούς σκοπούς. Όταν δοθούν οι πληροφορίες οι οποίες εμφανίζονται στη ροή δεδομένων του δρομολογητή πριν και αφού αποσυνδεθεί από το δίκτυο, στη συνέχεια πραγματοποιείται η κατανόηση της διαφοράς και από τους δύο. Ένας στόχος της έρευνας αυτής, είναι η πραγματοποίηση περισσότερων ερευνών στις περιοχές αυτές. Οι ερευνητές οφείλουν να επικεντρωθούν στο να αναπτύξουν μεθόδους οι οποίες θεωρούνται συμβατές με το αυξανόμενο νομικό σύστημα. Επιπρόσθετα, οφείλουν να ανακαλύψουν νέες μεθόδους στον τομέα αυτό για κατανόηση και πειραματική επικύρωση των θεμελιωδών πτυχών και πολυπλοκότητας του τομέα εξαιτίας της τεχνολογικής προόδου και της επίδρασής της στα ψηφιακά στοιχεία.

Βιβλιογραφία

Accessdata., n.d. Αντλήθηκε από : https://accessdata.com/

Ademu, I. O., Imafidon, C. O., Preston, D. S., 2011. *A new approach of digital forensic model for digital forensic investigation*. Int. J. Adv. Comput. Sci. Appl, σσ. 175-178

Altheide Cory, Harlan Carvey, 2011. *Digital Forensics with Open Source Tools*.

Blackbagtech Technologies., n.d. Αντλήθηκε από : https://www.blackbagtech.com

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

CAINE., n.d. Αντλήθηκε από : https://www.caine-live.net/

Carrier, B., & Spafford, E. H., 2004. *An event-based digital forensic investigation framework*. In Digital forensic research workshop, (σσ. 11-13).

Carrier Brian, 2005. *File System Forensic Analysis*.

Carvey Harlan, n.d. *Windows Incident Response Block* Αντλήθηκε από : http://windowsir.blogspot.gr

Digital Forensics Framework., n.d. Αντλήθηκε από : http://digitalforensicsframework.blogspot.com/

Digital Forensics Research Workshop, 2001. *A Road Map for Digital Forensic Research*.

deft., n.d. Αντλήθηκε από : http://www.deftlinux.net/

Encase Forensic, n.d. Αντλήθηκε από : https://www.guidancesoftware.com/encase-forensic

Harlan Carvey, 2011. *Windows Registry Forensics*, Advanced Digital Forensic Analysis of the Windows Registry.

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

Henseler, J., 2000. *Computer crime and computer forensics*. In The encyclopedia of forensic science.

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

Karie, N. M., & Venter, H. S., 2015. *Taxonomy of challenges for digital forensics*. Journal of forensic sciences, σσ. 885-893.

Kent, K., Chevalier, S., Grance, T., Dang, H., 2006. *Guide to integrating forensic techniques into incident response*. NIST Special Publication, σσ. 800-86.

Lessing Marthie, n.d. *Basie von Solms Live Forensic Acquisition as Alternative to Traditional Forensic Processes.*

Magnetforensics, n.d. *Magnet IEF* Αντλήθηκε από : https://www.magnetforensics.com/magnet-ief/

Mckemmish, R., 1999. *What is Forensic Computing*? Trends and Issues in Crime and Criminal Justice.

MSAB, n.d. *XRY* Αντλήθηκε από : https://www.msab.com/products/xry/

NIST, n.d. *Populated Taxonomy* Αντλήθηκε από : https://toolcatalog.nist.gov/index.php: https://toolcatalog.nist.gov/populated_taxonomy/index.php

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

Palmer, G., 2001. *A road map for digital forensic research*. In First Digital Forensic Research Workshop. Utica, New York.

Perumal, S., 2009. *Digital forensic model based on Malaysian investigation process*. International Journal of Computer Science and Network Security, σσ. 38-44.

Pollitt, M., 2010. *A history of digital forensics*. In IFIP International Conference on Digital Forensics (σσ. 3-15). Berlin, Heidelberg: Springer.

Reith, M., Carr, C., Gunsch, G., 2002. An examination of digital forensic models. International Journal of Digital Evidence, σσ. 1-12.

Sammons John, 2012. *The Basics of Digital Forensics*, The Primer for Getting Started with Digital Forensics.

Vlachopoulos, K., Magkos, E., & Chrissikopoulos, V., 2013. *A model for hybrid evidence investigation*. Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, σ. 150.

X-Ways, n.d. *Forensics*. Αντλήθηκε από : http://www.x-ways.net/forensics/

Zareen, M. S., Waqar, A., & Aslam, B., 2013. *Digital forensics: Latest challenges and response*. In Information Assurance (NCIA), 2nd National Conference on (σσ. 21-29). IEEE.

Βιβλιογραφία 5ου κεφαλαίου

CHFI, n.d. Router Forensics and Network Forensics, Chapter 10.