Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων

ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Μεταπτυχιακή Διατριβή

Προστασία της Ιδιωτικότητας σε περιβάλλον Ψηφιακής Δικανικής Εγκληματολογίας (Privacy in Digital Forensics)

Μάρτιος, 2022

Περιεχόμενα

Ευχαριστίες

Ευχαριστώ τον καθηγητή κ. Στέφανο Γκρίτζαλη για τις πολύτιμες συμβουλές, την υποστήριξη και την καθοδήγηση καθόλη την πορεία μου στο μεταπτυχιακό «Ασφάλεια Ψηφιακών Συστημάτων».

Αφιερώνω την παρούσα μεταπτυχιακή διατριβή στην οικογένειά μου και την ευχαριστώ για την υποστήριξη και την απεριόριστη υπομονή που μου πρόσφερε.

Εισαγωγή

Η συνεχόμενη ψηφιοποίηση της καθημερινής ζωής λόγω της εκθετικής αύξησης της χρήσης των υπολογιστών και των προσωπικών συσκευών σε όλες τις εκφάνσεις της καθημερινότητας οδήγησαν στην άνθιση του ηλεκτρονικού εμπορίου και στη δημιουργία του ψηφιακού στίγματος κάθε χρήστη. Παράλληλα όμως αυξήθηκαν και οι περιπτώσεις ηλεκτρονικών εγκλημάτων όπου κακόβουλοι χρήστες καταχρώνται προσωπικά ψηφιακά δεδομένα με απώτερο σκοπό οικονομικό και πολιτικό όφελος. Ως εκ τούτου και ως αντιστάθμισμα των ανωτέρω, αναπτύσσονται τεχνικές, οι μέθοδοι και εργαλεία για την ιχνηλάτηση των κακόβουλων ενεργειών με σκοπό τον εντοπισμό των δραστών και την απόδοση ευθυνών. Παράλληλα, αναπτύσσεται και ο κλάδος της ψηφιακής εγκληματολογίας όπου ειδικοί επιστήμονες εφαρμόζουν σύννομες τεχνικές και εργαλεία για την εξαγωγή των ψηφιακών πειστηρίων.

Στο πλαίσιο της ανωτέρω αυξημένης παρουσίας των ατόμων στο διαδίκτυο γίνεται έντονος λόγος περί προστασίας των προσωπικών δεδομένων των χρηστών του διαδικτύου και γενικά όσων κατέχουν προσωπικά στοιχεία τους σε ψηφιακή μορφή. Για το λόγο αυτό έχουν αναπτυχθεί εκτενώς σε εθνικό και ευρωπαϊκό επίπεδο νομοθεσίες περί προστασίας των προσωπικών δεδομένων οι οποίες παρέχουν κατευθύνσεις για τον τρόπο επεξεργασίας και αποθήκευσης αυτών καθώς και τις προϋποθέσεις κάτω από τις οποίες αυτά μπορούν να επεξεργαστούν από τρίτα άτομα. Οι εν λόγω νομοθεσίες αποτελούν καινούργια τροχοπέδη για τους ψηφιακούς εγκληματολόγους καθώς δυσχεραίνουν την εκτέλεσης της ψηφιακής εγκληματολογικής έρευνας εισάγοντας νέες απαιτήσεις για τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών δεδομένων.

Η παρούσα μεταπτυχιακή διατριβή αποτελεί μία προσπάθεια να σκιαγραφηθεί η δραστηριότητα του ψηφιακού εγκληματολόγου κατά τη διαδικασία της συλλογής των ψηφιακών πειστηρίων εν μέσω του ανωτέρω δυναμικού και συνήθως περιοριστικού νομοθετικού και τεχνολογικού πλαισίου. Στις σελίδες που ακολουθούν θα αναλυθούν οι τεχνικές που ακολουθεί ο ψηφιακός εγκληματολόγος, το νομικό πλαίσιο το οποίο προστατεύει τα προσωπικά δεδομένα των ατόμων σε εθνικό και ευρωπαϊκό επίπεδο και κάτω από το οποίο οφείλει αυτός να δρα και πως οι υφιστάμενες τεχνικές που εφαρμόζονται ενδέχεται να παραβιάσουν την ιδιωτικότητα των ατόμων. Ακολούθως, θα αναλυθούν τεχνικές που επιτρέπουν την εκτέλεση της ψηφιακής εγκληματολογικής έρευνας λαμβάνοντας υπόψη την προστασία των προσωπικών δεδομένων και στο τελευταίο κεφάλαιο θα αναλυθεί με περαιτέρω λεπτομέρειες η εκτέλεση ψηφιακής εγκληματολογικής έρευνας στον τομέα των δικτύων έχοντας ως γνώμονα την προστασία της ιδιωτικότητας των ατόμων.

Κεφάλαιο 1

1.1. Ορισμοί

1.1.1. Τί σημαίνει ιδιωτικότητα των ψηφιακών δεδομένων;

Ιδιωτικότητα των ψηφιακών δεδομένων ονομάζεται η σχέση μεταξύ της τεχνολογίας και του νομικού δικαιώματος σε ιδιωτικότητα ως προς τη συλλογή και την μεταφορά των ψηφιακών δεδομένων [1]. Με την τεχνολογική πρόοδο και την ευρεία χρήση των ηλεκτρονικών συσκευών η προστασία της ιδιωτικότητας των δεδομένων περιλαμβάνει πλέον πέρα από τα έντυπα δεδομένα και ψηφιακές οντότητες όπως e-mails, μηνύματα μέσω εφαρμογών instant messaging, ηλεκτρονικά αρχεία κειμένου (word, pdf κτλ), voice mail, ψηφιακές εικόνες κ.α. Τα εν λόγω αρχεία γίνονται στόχος τόσο των κακόβουλων χρηστών όσο και των ερευνητών της ψηφιακής εγκληματολογίας (Forensic Investigator).

Η υλοποίηση της ιδιωτικότητας των ψηφιακών δεδομένων μπορεί να λάβει τις ακόλουθες δύο μορφές [2]:

α) Hard Privacy: Η κοινοποίηση όσο λιγότερων προσωπικών ψηφιακών δεδομένων είναι δυνατό.

β) Soft Privacy: Εάν ο κάτοχος των προσωπικών ψηφιακών δεδομένων πρέπει να δώσει σε μία έτερη ψηφιακή οντότητα μέρος των εν λόγω δεδομένων τότε πρέπει να του γνωστοποιηθούν εκ των προτέρων ο λόγος που αυτά είναι απαραίτητα να συλλεχθούν και για πόση διάρκεια αυτά θα παραμείνουν στην κατοχή της.

1.1.2. Τί σημαίνει Ψηφιακή Δικανική (Digital Forensics);

Ως Digital Forensics εννοείται: «*η χρήση των επιστημονικά δοκιμασμένων μεθοδολογιών με στόχο τη διατήρηση, τη συλλογή, την αναγνώριση, την ανάλυση, την ερμηνεία, την τεκμηρίωση και την παρουσίαση των ψηφιακών αποδεικτικών στοιχείων που προέρχονται από ψηφιακές πηγές, σκοπεύοντας τελικά να διευκολύνουν την ανασυγκρότηση του συμβάντος και τελικά αυτό να παρουσιασθεί με όλα τα σχετικά ευρήματά του, νομότυπα, στην ακροαματική διαδικασία*» [4]

Επομένως, με τον όρο Digital Forensics εννοούμε την επιστήμη η οποία προσπαθεί να ανιχνεύσει αποδεικτικά στοιχεία για εγκληματικές πράξεις εξετάζοντας ψηφιακά τεκμήρια. Στα τεκμήρια αυτά συμπεριλαμβάνονται οι υπολογιστές, το δίκτυο, το cloud, οι σκληροί δίσκοι, οι server, τα smartphones και οποιαδήποτε τερματική συσκευή συνδέεται στην υπό εξέταση υποδομή. [5]

1.1.3. Ποιος είναι ο ερευνητής της ψηφιακής εγκληματολογίας (Forensic Investigator);

Ως ερευνητή της ψηφιακής εγκληματολογίας (Forensic Investigator) εννοούμε έναν τεχνικά καταρτισμένο επαγγελματία ο οποίος αναλαμβάνει την ανάκτηση ηλεκτρονικών πειστηρίων από τον χώρο που εκτελέστηκε μία αξιόποινη πράξη [6]. Ως βασικά καθήκοντα του ψηφιακού ερευνητή μπορούν να θεωρηθούν τα ακόλουθα:

α. Η διερεύνηση ενός περιστατικού ασφαλείας ή διαρροής δεδομένων.

β. Η ανάκτηση δεδομένων από ψηφιακά μέσα αποθήκευσης.

γ. Η ανάκτηση διαγραμμένων ή κατεστραμμένων αρχείων.

δ. Η εκτίμηση του εύρους της ψηφιακής επίθεσης και ο προσδιορισμός των ψηφιακών μέσων που αποτελούν στόχο της επίθεσης.

ε. Εξαγωγή ψηφιακών πειστηρίων από τα συλλεχθέντα ψηφιακά δεδομένα ακολουθώντας τις νόμιμες διαδικασίες επεξεργασίας αυτών.

στ. Διατήρηση της ακεραιότητας και της ασφάλειας των ψηφιακών πειστηρίων.

ζ. Καταγραφή των ενεργειών κατά την εκτέλεση της δικανικής έρευνας και υποβολή αναφοράς που μπορεί να χρησιμοποιηθεί από το δικαστήριο.

Ο ρόλος του ψηφιακού ερευνητή γίνεται ολοένα και σημαντικότερος καθώς λόγω της διαρκούς αύξησης της τεχνολογικής εξάρτησης του δημόσιου και του ιδιωτικού τομέα αυξάνονται οι απαιτήσεις ανεύρεσης ψηφιακών πειστηρίων τόσο για εσωτερικά θέματα των εταιρειών (λχ. ενδοεταιρική απάτη στελέχους) όσο και για συμβάντα τα οποία μπορεί να οδηγήσουν σε μεγάλης κλίμακας προβλήματα (λχ. διαρροή κωδικών πρόσβασης από τους server μίας τράπεζας) [7]. Συνεπώς, η ψηφιακή εγκληματολογική έρευνα απαιτεί καθορισμένες διαδικασίες που συμμορφώνονται με τη βιομηχανική πρακτική, οργανωτική πρακτική και κατάλληλη νομοθεσία, είτε ως μέρος της ποινικής έρευνας ή ως μέρος μιας γενικότερης αντιμετώπισης περιστατικών ασφαλείας [8].

1.1.4. Τι είναι τα δεδομένα προσωπικού χαρακτήρα;

Τα δεδομένα προσωπικού χαρακτήρα ορίζονται στην εθνική νομοθεσία βάσει του νόμου 4624/19 (ΦΕΚ 137/Α/29-8-2019) ως «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων)*» και το ταυτοποιήσιμο φυσικό πρόσωπο *είναι «εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως σε όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους* *παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.»*

1.2. Ιστορική Αναδρομή

Η λέξη «Forensics» προέρχεται από τη λατινική λέξη «forēnsis» που σημαίνει «before the forum» και χρησιμοποιήθηκε από τα Ρωμαϊκά χρόνια για να περιγράψει τη διαδικασία όπου κάποιος που έχει διαπράξει ένα αδίκημα παρουσιαζόταν ενώπιον μίας ομάδας δημοσίων προσώπων τα οποία, αφού συνυπολόγιζαν την απολογία του και τα λεγόμενα του αντιδίκου, έκριναν την υπόθεση υπέρ του ατόμου με το καλύτερο επιχείρημα. [8] Στη σύγχρονη εποχή τα Digital Forensics αποτελούν κλάδο της εγκληματολογικής επιστήμης και αναπτύχθηκαν λόγω της ραγδαίας αύξησης της επιστήμης των υπολογιστών και της εκθετικά αυξανόμενης ευρείας χρήσης τους με άμεσο επακόλουθο την άνθηση του ηλεκτρονικού εγκλήματος. Αυτό είχε ως αποτέλεσμα την δεκαετία του 1980 στην Αμερική και στην Αγγλία να συσταθούν ομάδες για την αντιμετώπιση του ηλεκτρονικού εγκλήματος [9]. Με την εξέλιξη της τεχνολογίας αναπτύχθηκαν και τα μέσα συλλογής των ψηφιακών πειστηρίων και συστάθηκαν πρότυπα για τον τρόπο συλλογής, ανάλυσης και παρουσίασης των αποτελεσμάτων σε κατάλληλη μορφή ώστε να καθίστανται έγκυρα ως αποδεικτικά στοιχεία κατά την ακροαματική διαδικασία. Σήμερα η ψηφιακή εγκληματολογία χρησιμοποιείται τόσο στο ποινικό δίκαιο όσο και στην ιδιωτική έρευνα και αποτελεί συνήθως μέρος μιας ευρύτερης έρευνας που καλύπτει αρκετούς κλάδους.

1.3. Νομολογία-Νομικές Επεκτάσεις

Η έρευνα επί των ψηφιακών μέσων καλύπτεται από εθνική και διεθνή νομοθεσία. Υπάρχουν συχνά περιορισμοί, οι οποίοι αφορούν στην παρακολούθηση ενός δικτύου, στην ανάγνωση προσωπικών επικοινωνιών και στην καταγραφή ψηφιακών πειστηρίων τα οποία περιλαμβάνουν προσωπικά δεδομένα τόσο των υπόπτων όσο και τρίτων ατόμων ως προς την εξεταζόμενη υπόθεση. Βάσει του Κανονισμού 679/2016 [11] της Ε.Ε. για την προστασία δεδομένων προσωπικού χαρακτήρα «*Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη και δίκαιη. Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία» και «…οι συγκεκριμένοι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σαφείς, νόμιμοι και προσδιορισμένοι κατά τον χρόνο συλλογής των δεδομένων προσωπικού χαρακτήρα*». Επιπρόσθετα, στον ίδιο κανονισμό προσδιορίζονται γενικά τα προσόντα του ψηφιακού ερευνητή αναφέροντας ότι *«… οσάκις ανατίθενται σε εκτελούντα την επεξεργασία δραστηριότητες επεξεργασίας, ο* *υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί μόνο εκτελούντες επεξεργασία οι οποίοι παρέχουν επαρκείς διαβεβαιώσεις, ιδίως από πλευράς εμπειρογνωμοσύνης, αξιοπιστίας και πόρων, για την εφαρμογή τεχνικών και οργανωτικών μέτρων που θα ανταποκρίνονται στις απαιτήσεις του παρόντος κανονισμού, συμπεριλαμβανομένων εκείνων που αφορούν την ασφάλεια της επεξεργασίας.»* Ωστόσο, ο εν λόγω κανονισμός αναφέρεται γενικά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα αποκλείοντας τις περιπτώσεις που αυτή είναι απαραίτητη για την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιπτώσεις που εξετάζονται και εξειδικεύονται από την Οδηγία 680/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Συγκεκριμένα, στην παράγραφο (34) αναφέρεται: «*Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, θα πρέπει να καλύπτει κάθε πράξη ή σύνολο πράξεων που εκτελείται επί δεδομένων προσωπικού χαρακτήρα ή συνόλων δεδομένων προσωπικού χαρακτήρα για αυτούς τους σκοπούς, είτε χρησιμοποιούνται αυτοματοποιημένα μέσα είτε άλλα, όπως η συλλογή, η αρχειοθέτηση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η αλλοίωση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η συσχέτιση ή ο συνδυασμός, ο περιορισμός της επεξεργασίας, η διαγραφή ή η καταστροφή*» και στην παράγραφο (35) «*Η εκτέλεση των καθηκόντων πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων η οποία ανατίθεται θεσμικά από τον νόμο στις αρμόδιες αρχές παρέχει σε αυτές τη δυνατότητα να απαιτούν από φυσικά πρόσωπα ή να δίνουν εντολή σε αυτά να συμμορφωθούν προς τα σχετικά αιτήματα. Σε μία τέτοια περίπτωση, η συγκατάθεση του υποκειμένου των δεδομένων όπως ορίζεται στον κανονισμό (ΕΕ) 2016/679 δεν θα πρέπει να παρέχει νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές*». Επιπρόσθετα, στην παράγραφο (38) αναφέρεται ότι «*Σε κάθε περίπτωση, αυτή η επεξεργασία θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, όπως η πρόβλεψη για ειδική ενημέρωση του υποκειμένου των δεδομένων, το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, κυρίως το δικαίωμα διατύπωσης της άποψής του, το δικαίωμα να απαιτήσει αιτιολόγηση της απόφασης που ελήφθη κατόπιν της εν λόγω αξιολόγησης και το δικαίωμα αμφισβήτησης της απόφασης*» και στην παράγραφο (43) «*Ένα φυσικό πρόσωπο θα πρέπει να έχει δικαίωμα πρόσβασης σε δεδομένα τα οποία συνελέγησαν και το αφορούν και να μπορεί να ασκεί το δικαίωμα αυτό ευχερώς και σε εύλογα τακτά διαστήματα, προκειμένου να έχει επίγνωση της επεξεργασίας και να ελέγχει τη νομιμότητά της*». Τέλος, στην παράγραφο (49) αναφέρεται ότι «*Εάν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία στο πλαίσιο ποινικής έρευνας και ποινικής διαδικασίας ενώπιον δικαστηρίου, τα κράτη μέλη θα πρέπει να μπορούν να προβλέπουν ότι η άσκηση των δικαιωμάτων ενημέρωσης, πρόσβασης και διόρθωσης, διαγραφής και περιορισμού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα γίνεται σύμφωνα με τους εθνικούς κανόνες περί δικαστικών διαδικασιών*».

Οι προαναφερθέντες κανονισμοί έχουν ενσωματωθεί στο ελληνικό δίκαιο με τον νόμο 4624/19 [10] όπου στο άρθρο 24 αναφέρεται ότι «*Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, επιτρέπεται όταν η επεξεργασία αυτή είναι αναγκαία για την εκπλήρωση των καθηκόντων που τους έχουν ανατεθεί και εφόσον είναι … β) αναγκαία για την αποτροπή κινδύνων για την εθνική ασφάλεια, εθνική άμυνα ή δημόσια ασφάλεια ή για τη διασφάλιση φορολογικών και τελωνειακών εσόδων γ) αναγκαία για τη δίωξη ποινικών αδικημάτων δ) αναγκαία για την αποτροπή σοβαρής βλάβης στα δικαιώματα άλλου προσώπου*» και στο άρθρο 25 «*Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από ιδιωτικούς φορείς για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, επιτρέπεται, εφόσον είναι απαραίτητη: … β) για τη δίωξη ποινικών αδικημάτων ή γ) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, εκτός και εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τύχουν επεξεργασίας τα δεδομένα αυτά*».

Από την ανωτέρω ευρωπαϊκή και εθνική νομολογία γίνεται κατανοητό ότι ο ψηφιακός ερευνητής έχει πολλά τροχοπέδη στην εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία των προσωπικών δεδομένων καθώς πρέπει να λάβει υπόψη του την ανάγκη διαρκούς προστασίας των συλλεχθέντων προσωπικών δεδομένων καθόλη τη διάρκεια της επεξεργασίας αυτών με παράλληλη την απαίτηση διαρκούς ενημέρωσης για την επεξεργασία που αυτά υφίστανται [13]. Για τη συλλογή στοιχείων που μπορεί να περιέχουν προσωπικά δεδομένα ο ψηφιακός ερευνητής πρέπει να λάβει ένταλμα έρευνας το οποίο απαιτεί επαρκής αιτιολόγηση για την έκδοσή του (και την κατ’ επέκταση απαίτηση ύπαρξης ενοχοποιητικών στοιχείων που δικαιολογούν περαιτέρω έρευνα)[14] και στο οποίο θα καθορίζονται με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν καθώς σε περίπτωση που αντληθούν ψηφιακά πειστήρια από αντικείμενα για τα οποία δεν έχει εκδοθεί ένταλμα έρευνας τα εν λόγω αποδεικτικά στοιχεία θα απορριφθούν κατά την ακροαματική διαδικασία [8]. Κατά τη συλλογή όμως ψηφιακών πειστηρίων υπάρχει περίπτωση ο ψηφιακός ερευνητής να συλλέξει στοιχεία τρίτων ως προς την υπόθεση ατόμων, πολλά από αυτά να αποτελούν προσωπικά τους δεδομένα. [1] Στις επόμενες παραγράφους θα αναλυθούν πιθανές περιπτώσεις παραβίασης προσωπικών δεδομένων και θα παρατεθούν προτάσεις για εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία προσωπικών δεδομένων.

Κεφάλαιο 2

Στο παρόν κεφάλαιο θα αναλυθούν οι επιμέρους κατηγορίες της ψηφιακής δικανικής έρευνας. Ακολούθως, θα αναλυθούν οι πρακτικές που εφαρμόζονται κατά τη διενέργεια της ψηφιακής δικανικής και το κεφάλαιο θα ολοκληρωθεί με την παρουσίαση προβλημάτων ιδιωτικότητας κατά την εφαρμογή των εν λόγω πρακτικών και θα παρατεθούν προτεινόμενες λύσεις για την εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία των προσωπικών δεδομένων.

2.1. Κατηγορίες

Η ψηφιακή δικανική έρευνα ανάλογα με το αντικείμενο προς εξέταση χωρίζεται στις ακόλουθες κατηγορίες:

- α. Computer Forensics
  - 1) Disk Forensics
  - 2) Memory Forensics
- β. Network Forensics
  - 1) Wireless Forensics
- γ. Database Forensics
- δ. Malware Forensics
- ε. Email Forensics
- στ. Mobile Forensics
- ζ. Cloud Forensics
- η. Social Media Forensics
- θ. IOT Forensics

Ακολούθως θα αναλυθεί συνοπτικά η κάθε κατηγορία ενώ στο τελευταίο κεφάλαιο της πτυχιακής εργασίας θα γίνει εκτενής λόγος για τα Network Forensics.

2.1.1. Computer Forensics

Τα Computer Forensics αναφέρονται στη διαδικασία εφαρμογής επιστημονικών και αναλυτικών τεχνικών έρευνας στα λειτουργικά συστήματα των υπολογιστών και των δομών των αρχείων με αποτέλεσμα τη δημιουργία νομικά έγκυρων αποδεικτικών στοιχείων. Με την εφαρμογή τεχνικών ανάλυσης των δομικών τμημάτων των υπολογιστών (λχ. σκληροί-ψηφιακοί δίσκοι) και την αναγνώριση, διατήρηση, ανάκτηση, ανάλυση και παρουσίαση των περιεχομένων τους με σύννομες μεθόδους αντλούνται αποδεικτικά στοιχεία κατάλληλα για την ακροαματική διαδικασία [8]. Τα Computer Forensics αναλύονται στις ακόλουθες υπό-κατηγορίες:

2.1.1.1. Disk Forensics

Τα Disk Forensics είναι κλάδος των Computer Forensics που ασχολείται με την ανεύρεση ψηφιακών πειστηρίων από μέσα αποθήκευσης όπως σκληροί δίσκοι, CD/DVD, συσκευές USB κτλ. [15]. Τα δεδομένα που μπορούν να ανακτηθούν από τις πρακτικές του εν λόγω κλάδου είναι: α) email, διεγραμμένα email, β) πληροφορίες χρήσης διαδικτύου, γ) διεγραμμένα αρχεία, δ) διαγραμμένες εικόνες και ταινίες, ε) πληροφορίες πρόσβασης και χρήσης, στ) προσωρινά αρχεία, ζ) αρχεία καταγραφών (log files) [16]

2.1.1.2. Memory Forensics

Τα Memory Forensics είναι κλάδος των Computer Forensics που ασχολείται με την εκτέλεση δικανικής έρευνας αναλύοντας την memory dump[1]. Χρησιμοποιείται κατά κύριο λόγο στην έρευνα εξειδικευμένων επιθέσεων σε υπολογιστές οι οποίες δεν αφήνουν ίχνη στο σκληρό δίσκο του υπολογιστή [18]. Επιπρόσθετα, κατά την ανωτέρω έρευνα συλλέγονται στοιχεία από την μνήμη του συστήματος (system registers, cache, RAM) σε raw μορφή.[19]

2.1.2. Network Forensics

Τα Network Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας που έχει ως στόχο «την ιχνηλάτηση, καταγραφή και ανάλυση δικτυακών συμβάντων με σκοπό τον εντοπισμό πηγών κακόβουλων επιθέσεων και άλλων προβλημάτων» [20]. Κατά τη διάρκεια των Network Forensics γίνεται πλήρης καταγραφή της δραστηριότητας του δικτύου (e-mail, Instant Messaging (I.M.)

[1] Memory Dump είναι μία διαδικασία κατά την οποία τα περιεχόμενα της μνήμης αποθηκεύονται και παρουσιάζονται σε περίπτωση που μία εφαρμογή ή το σύστημα σταματήσει να λειτουργεί αναίτια (system crash). Η εν λόγω διαδικασία βοηθά στην ανεύρεση των αιτιών που οδήγησαν στις ανωτέρω δυσλειτουργίες [17]

επικοινωνία, δραστηριότητα σε web browsers, μεταφορές αρχείων κτλ) καθώς το ενθυλακωμένο περιεχόμενο των frames αποθηκεύεται μαζί με όλη τη καταγραφείσα δικτυακή ροή [21].

2.1.2.1. Wireless Forensics

Τα Wireless Forensics αποτελούν κλάδο των Network Forensics και σκοπός τους είναι η συλλογή και η ανάλυση πακέτων που διακινούνται στα ασύρματα δίκτυα με χρήση σύννομων μεθόδων με σκοπό την ανεύρεση ψηφιακών πειστηρίων που μπορούν να χρησιμοποιηθούν στην ακροαματική διαδικασία [22].

2.1.3. Database Forensics

Τα Database Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την εξαγωγή ψηφιακών πειστηρίων μέσω της μελέτης των βάσεων δεδομένων και των περιεχόμενων σε αυτές metadata [23].

2.1.4. Malware Forensics

Τα Malware Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την εξαγωγή ψηφιακών πειστηρίων μέσω της μελέτης του τρόπου εισόδου, διάδοσης και λειτουργίας των malware στο υπό εξέταση σύστημα. [24]

2.1.5. E-mail Forensics

Τα E-mail Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την ανάκτηση και την ανάλυση e-mail συμπεριλαμβάνοντας διαγραμμένα e-mail, ημερολόγια και επαφές. Η εν λόγω δικανική ανάλυση συνήθως εκτελείται σε περιπτώσεις ερευνών μεγάλης κλίμακας όπου είναι απαραίτητη η μελέτη των διαύλων επικοινωνίας των εμπλεκόμενων προσώπων. [25]

2.1.6. Mobile Forensics

Τα Mobile Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την αναζήτηση ψηφιακών πειστηρίων μέσω της μελέτης φορητών συσκευών. Ως φορητές συσκευές εννοούνται τα κινητά τηλέφωνα, τα smartphones, τα tablets, το GPS κ.α. [26] οι οποίες αποθηκεύουν πληθώρα στοιχείων για τον χρήστη τα οποία συμβάλλουν στη σκιαγράφηση της προσωπικότητας, της δραστηριότητας και των κινήτρων του. [27]

2.1.7. Cloud Forensics

Τα Cloud Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την αναζήτηση ψηφιακών πειστηρίων μέσω της χρήσης επιστημονικών μεθόδων αναζήτησης, εντοπισμού και συλλογής ψηφιακών δεδομένων καθώς και ανακατασκευής συμβάντων σε cloud υποδομές. [28]

2.1.8. Social Media Forensics

Τα Social Media Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την ενίσχυσή της μέσω της μελέτης των δημοσιεύσεων και των επαφών των πιθανών δραστών για την ανεύρεση πιθανών υπόπτων και μαρτύρων και τη χρησιμοποίηση φωτογραφιών, καταλόγων επαφών, δημογραφικών στοιχείων, προσωπικών μηνυμάτων και δεδομένων τοποθεσίας για την ενίσχυση των ψηφιακών πειστηρίων. [28]

2.1.9. IOT Forensics

Τα IOT Forensics αποτελούν τμήμα της ψηφιακής δικανικής έρευνας με αντικείμενο την ανεύρεση ψηφιακών πειστηρίων μέσω της αναζήτησης και της καταγραφής δεδομένων από «έξυπνες» συσκευές που επικοινωνούν μεταξύ τους, καθιστώντας το εν λόγω εγχείρημα εξαιρετικά δύσκολο λόγω του τεραστίου όγκου δεδομένων και της πολυπλοκότητας των εμπλεκόμενων συστημάτων. [28]

2.2. Διαδικασίες Ψηφιακής Δικανικής Έρευνας

Οι ψηφιακές έρευνες όπως και κατ' επέκταση όλος ο κλάδος της εγκληματολογίας γίνονται βάσει μίας συγκεκριμένης σειράς διαδικασιών και μεθοδολογιών που έχουν τεθεί από επιστήμονες αλλά και ειδικούς του εκάστοτε τομέα και ακολουθούν τις κάτωθι αρχές: [13]

Ακεραιότητα: Τα στοιχεία τα οποία είναι μέρος μίας έρευνας δε πρέπει να υποστούν αλλοίωση ή αλλαγή διότι με οποιαδήποτε μετατροπή χάνεται η αξιοπιστία τους.

Αρμοδιότητα/ Εξειδίκευση: Όποιος έχει πρόσβαση στα εν δυνάμει ψηφιακά αποδεικτικά στοιχεία πρέπει να έχει εξειδίκευση στη ψηφιακή δικανική.

Διαθεσιμότητα και Ευθύνη: Όλα τα στοιχεία πρέπει να είναι μόνιμα διαθέσιμα στον ψηφιακό ερευνητή αλλά και επαρκώς προστατευμένα από οποιονδήποτε άλλο. Συνεπώς τα άτομα που διαθέτουν ψηφιακά αποδεικτικά στοιχεία είναι υπεύθυνα για όλες τις ενέργειες που διαπράττονται με αυτά.

Επαναληψιμότητα: Ένα ανεξάρτητο τρίτο πρόσωπο πρέπει να είναι σε θέση να επαναλάβει ολόκληρη τη διαδικασία της ψηφιακής δικανικής που εφαρμόστηκε για την εξαγωγή συμπερασμάτων και να επιτύχει το ίδιο αποτέλεσμα.

Ο τρόπος συλλογής και αποθήκευσης των προαναφερθέντων δεδομένων ακολουθεί ορισμένα διεθνή πρότυπα. Πιο συγκεκριμένα, η εν λόγω διαδικασία χωρίζεται στις ακόλουθες κατηγορίες βάσει του ISO/IEC 27037:2012 : [29]

α) Στον εντοπισμό των δεδομένων

β) Στη συλλογή των δεδομένων

γ) Στην απόκτηση των δεδομένων

δ) Στη διατήρηση των δεδομένων

Ακολούθως, τα ανωτέρω δεδομένα θα αναλυθούν σε κάποιο εγκληματολογικό εργαστήριο. Η διαχείριση και η σειρά επεξεργασίας τους κατά την ανωτέρω διαδικασία ακολουθούν τις οδηγίες του προτύπου ISO/IEC 27042:2015 [30] ως ακολούθως:

α) διερεύνηση των συλλεχθέντων στοιχείων

β) ανάλυση των στοιχείων

γ) ερμηνεία των εξαγόμενων αποτελεσμάτων

δ) δημιουργία αναφοράς

Λαμβάνοντας υπόψη τα ανωτέρω και ανάλογα με το μοντέλο διερεύνησης και τη μεθοδολογία που θα χρησιμοποιηθεί διακρίνονται οι εξής έξι φάσεις έρευνας που θα ακολουθήσει ο ψηφιακός ερευνητής και οι οποίες είναι κοινές σε κάθε μοντέλο διερεύνησης [31]:

α) Σχεδιασμός της ψηφιακής δικανικής έρευνας

β) Εντοπισμός των δεδομένων προς συλλογή

γ) Συλλογή των δεδομένων — at scene

δ) Αποθήκευση-διατήρηση των δεδομένων

ε) Επεξεργασία των δεδομένων

στ) Ανάλυση των δεδομένων — in lab

ζ) Δημιουργία της τελικής αναφοράς

Τα βήματα που ακολουθεί ο ψηφιακός ερευνητής κατά την εκτέλεση της ψηφιακής δικανικής έρευνας από την έναρξη αυτής έως και την υποβολή της αναφοράς των αποτελεσμάτων μπορούν να συνοψισθούν στον ακόλουθο πίνακα [7]:

S1	***Identification***: Identifying that an incident has taken place – e.g. crime report, link from another investigation: a. *assess* – establish the crime scene(s) b. *triage & report* – rapid evaluation of situation and report on judgement
S2	***Acquisition***: Physical seizure and storage of devices and data – locally and remote – a. *local* - acquisition of locally held data b. *remote* - acquisition of data held on the Internet/Cloud/private networks
S3	***Preservation***: Copying and verification (check summing) of media i.e. making a forensic image: a. *static imaging* – lab-based – storage device (disk/chip removed). b. *live imaging* – i.e. crime scene: image store attached to target machine or over-the-network imaging. c. *memory imaging*
S4	***Search***: Recovery of data from physical media, including undeletion, decryption etc.: a. *physical search* – (1) search of binary images, (2) file carving, (3) searching in the absence of a file system. b. *logical search* – search of file system: i. *brute-force* – recovery of all material (e.g. all jpg). ii. *directed* – search led by knowledge of case. 1. OS – Evidence from the operating system: a. *configuration* – How was the system set up: devices, users, network, applications etc. b. *accidental* – Artifacts left by fundamental operation of device (e.g. spool files, pagefile.sys). c. *logged* – system logs. 2. Applications a. *configuration* – How was each application set up? e.g. default save directory. b. *accidental* – Artifacts left by fundamental operation - e.g. tmp files c. *logged* – e.g. error logs and transaction logs. 3. Network (local) – e.g. browser forensics, email, messaging: a. *configuration* – How was each network application set up? b. *accidental* – Artifacts left by fundamental operation - e.g. cache files c. *logged* – e.g. browser history. 4. Network (remote) – server and network devices (routers) a. *configuration* – How was each network device set up? b. *accidental* – Artifacts left by fundamental operation - e.g. routing tables, web-server logs. c. *logged* – e.g. dhcp/dns logs. 5. Network (surveillance) – packet sniffing, ISP cooperation: a. *Traffic analysis* – If traffic is encrypted, then source/destination, timestamp and volume information may still be available.
S5	***Analysis***: relevance judgments, organization of low-level facts into evidence: four semi-orthogonal concerns: temporal, spatial, relational, functional a. *Functional* – What happened? Who did what? b. *Temporal* – When or in what order did things happen? c. *Spatial* – Where did things happen? d. *Relational* – What items of interest are related to others and how?
S6	***Reconstruction***: hypotheses induction and testing. Equivocal analysis. a. What do you think happened? b. How can it be supported from the facts? c. What contra-indications are there? d. Alternative explanations?
S7	***Reporting***: Court report, court appearance.
S8	***Reflection & Review***: Consideration of performance and lessons to be learned. a. Produce a document detailing which forensics investigators were involved, and their specific activities, if possible. b. Discard irrelevant data that was acquired and preserved. c. Consider whether any of the investigators require support or counseling.

Πίνακας 1: Βήματα Digital Forensics

Σύμφωνα με το ίδιο άρθρο [31] κατά την φάση της έρευνας και αναζήτησης των στοιχείων σε περιβάλλον windows (και κατ' επέκταση σε linux στα αντίστοιχα αρχεία-φακέλους) ο ψηφιακός ερευνητής εξετάζει τα ακόλουθα για ύπαρξη τυχών ενοχοποιητικών στοιχείων:

α) Home Directory: Ο φάκελος αυτός συσχετίζεται με ένα συγκεκριμένο προφίλ χρήστη και σε αυτόν περιλαμβάνονται οι φάκελοι "desktop", "my documents", "favorites" στους οποίους κατά κανόνα αποθηκεύονται τα έγγραφα και τα αρχεία που δημιουργεί ή τροποποιεί ο χρήστης.

β) File Properties (security): Τα δικαιώματα προσπέλασης ενός αρχείου μπορεί να καταδείξουν τον υπολογιστή ή τον χρήστη που το δημιούργησε ή το τροποποίησε. Συνήθως, ο ιδιοκτήτης ενός αρχείου είναι το account το οποίο είχε συνδεθεί στα windows κατά τη δημιουργία του αρχείου.

γ) Registry: H registry αποτελεί σημαντική πηγή πληροφοριών καθώς παρέχει τα αρχεία καταγραφών (log files) της συνολικής δραστηριότητας του χρήστη στον υπολογιστή όπως επίσης και τα logs επεξεργασίας αρχείων σε χρονολογική σειρά (mac times[28]). Απαιτεί γνώση από τη πλευρά του ψηφιακού ερευνητή για τον άμεσο εντοπισμό των αρχείων που απαιτούνται καθώς η ψηφιακή δικανική είναι συνήθως μία διαδικασία που περιορίζεται τόσο χρονικά όσο και σε πόρους.

δ) Browser Artifacts: Στην τοπική μνήμη του υπολογιστή ενδέχεται να αποθηκεύονται cached δεδομένα αναφορικά με τις σελίδες που έχει επισκεφτεί ο χρήστης (urls) και τα favorites του φυλλομετρητή που χρησιμοποιεί. Υπάρχει άμεση συσχέτιση χρησιμότητας των εν λόγω αρχείων και του διατιθέμενου χρόνου για την εξαγωγή τους καθώς είναι εύκολο να διαγραφούν ή να τροποποιηθούν είτε από τον φυλλομετρητή είτε από κάποιο άλλο πρόγραμμα.

ε) E-mail Artifacts: Τα εν λόγω δεδομένα είναι πολύτιμα για τα Network Forensics, συνδέονται άμεσα με ένα συγκεκριμένο χρήστη αλλά η δυσκολία έγκειται στο χρόνο που χρειάζεται η εξαγωγή τους και στο αν τα δεδομένα είναι αποθηκευμένα τοπικά στον υπολογιστή ή στον email server.

στ) Instant Messaging Artifacts: Πολλές εφαρμογές instant messaging τηρούν αρχείο καταγραφών των συνομιλιών με τα ονόματα των χρηστών τοπικά στον υπολογιστή και η κατοχή τους είναι πολύτιμη για τη ψηφιακή δικανική. Ωστόσο, ενδέχεται το back up των εν λόγω εφαρμογών να γίνεται μέσω web server καθιστώντας αδύνατη τη συλλογή στοιχείων.

Όλα τα ανωτέρω είναι time significant και απαιτείται να υπάρχει κοινός χρόνος μεταξύ των υπό διερεύνηση συσκευών ώστε ο ψηφιακός ερευνητής να μπορεί να συνδέσει χρονικά τα διάφορα στοιχεία τόσο μεταξύ τους όσο και με ένα συγκεκριμένο προφίλ χρήστη. Επιπρόσθετα, ο ψηφιακός ερευνητής θα αναζητήσει δεδομένα που έχουν γίνει κρυφά με τη χρήση κάποιας τεχνικής anti-forensics (πχ steganography) [32] και θα χρησιμοποιήσει εξειδικευμένα προγράμματα (forensics tools) για να αποσπάσει μόνο τη χρήσιμη για αυτόν πληροφορία [33] και γενικότερα θα ακολουθήσει μία υβριδική προσέγγιση για την έρευνα ενός συστήματος η οποία θα είναι συνδυασμός live analysis (system up and running) και post-mortem analysis (system down or up) [34]. Γίνεται τέλος κατανοητό ότι κατά την εκτέλεση της ψηφιακής δικανικής ανάλυσης είναι πιθανό να χρησιμοποιηθούν πολλές και διαφορετικές τεχνικές απόκτησης ψηφιακών αποδεικτικών στοιχείων που απαντώνται σε διάφορους κλάδους της ψηφιακής δικανικής καθώς ο υπολογιστής και οι φορητές συσκευές είναι συνδεδεμένες τόσο μεταξύ τους όσο και με το διαδίκτυο και για μία δικανική έρευνα απαιτούνται όσο περισσότερα ψηφιακά πειστήρια δύνανται να αντληθούν.

2.3. Υφιστάμενες τεχνικές προστασίας ιδιωτικότητας

Από την παράγραφο 2.2 έγινε αντιληπτό ότι ο ψηφιακός ερευνητής ακολουθεί συγκεκριμένη μεθοδολογία, διακριτά βήματα σαφώς οριοθετημένα και θεσμοθετημένα για την εκτέλεση της ψηφιακής δικανικής. Ωστόσο, πέρα από τα νομικά τροχοπέδη περί ιδιωτικότητας που αναλύθηκαν στην παράγραφο 1.3. ο ψηφιακός ερευνητής αντιμετωπίζει ορισμένα τεχνικά προβλήματα κατά την εκτέλεση της ανωτέρω έρευνας. Τα ψηφιακά συστήματα (υπολογιστές, φορητές συσκευές) σχεδιάζονται πλέον με αυξημένες δυνατότητες προστασίας της ασφάλειας της συσκευής και της ιδιωτικότητας του χρήστη [35] με την χρήση αυτών των δυνατοτήτων να επεκτείνεται και σε εύχρηστα λογισμικά τα οποία γίνονται συνεχώς αποτελεσματικότερα [36]. Τα λογισμικά αυτά αποτελούν κομμάτι των τεχνολογιών PET (Privacy Enhancing Technologies) τα οποία χωρίς να επηρεάζουν αισθητά την λειτουργικότητα των συσκευών και των υπηρεσιών περιορίζουν τη χρήση και τη διακίνηση προσωπικών δεδομένων [37].

Σκοπός των τεχνολογιών PET είναι η προστασία της ιδιωτικότητας των χρηστών με τον περιορισμό της χρήσης και της κοινοποίησης σε τρίτα άτομα των προσωπικών τους δεδομένων καθώς και τη θέσπιση προϋποθέσεων ώστε τα εν λόγω δεδομένα να μπορούν να επεξεργαστούν και να χρησιμοποιηθούν από τρίτους. [38] Μερικές τεχνολογίες PET είναι οι ακόλουθες [39]:

α)Communication anonymizers

β)Obfuscation

γ)Online shared bogus accounts

δ)Enhanced privacy ID

ε)Homomorphic encryption

στ)Zero-knowledge proof

ζ)Secure multi-party computation

η) Non-interactive zero-knowledge proof

θ) Format-preserving encryption

ι) Blinding

ια) Differential privacy

ιβ) Pseudonymization

ιγ)Transparency Enhancing Tools

Οι τεχνολογίες PET μολονότι χρησιμοποιούνται για την προστασία της ιδιωτικότητας των χρηστών αποτελούν πολλές φορές τροχοπέδη στον ψηφιακό ερευνητή κατά τη συλλογή των ψηφιακών πειστηρίων. Η δράση τους πολλές φορές εμποδίζει τα χρησιμοποιούμενα εργαλεία δικανικής ανάλυσης με αποτέλεσμα μαζί με έτερες τεχνικές που σκοπίμως δρουν με τέτοιο σκοπό να γίνεται λόγος για τον όρο Anti-Forensics (AF). Ως Anti-Forensics χαρακτηρίζονται «οι πρακτικές που έχουν ως σκοπό την αλλοίωση και τον περιορισμό των διαθέσιμων ψηφιακών πειστηρίων καθώς και την παρεμπόδιση της εκτέλεσης της ψηφιακής δικανικής έρευνας»[40] όπως επίσης και την αύξηση του χρόνου έρευνας του ψηφιακού ερευνητή έτσι ώστε είτε τα αποδεικτικά στοιχεία να καταστούν χρονικώς άκυρα είτε ο επιτιθέμενος να έχει τον απαιτούμενο χρόνο να καλύψει τα εν λόγω αποδεικτικά στοιχεία [42]. Ως εφαρμογή τεχνικών Anti-Forensics θεωρείται η χρήση των κάτωθι :

α. Data Hiding (πχ. Steganography)

β. Artefact Wiping

γ.Trail Obfuscation

δ. Encryption [41]

ε. Memory Injection [42]

στ. Syscall Proxying [42]

ζ. Virtual Machines [42]

η. Attack against forensic tools and methods [43]

Ωστόσο, τόσο η χρήση των PETs όσο και των τεχνικών Anti-Forensics δημιουργεί προβλήματα ιδιωτικότητας τρίτων χρηστών κατά την εκτέλεση της ψηφιακής δικανικής λόγω μη σωστής εφαρμογής τους, μη σωστής συντήρησής τους ή και λόγω κατασκευαστικών σφαλμάτων των χρησιμοποιούμενων εργαλείων. Στην επόμενη παράγραφο θα αναλυθούν περιπτώσεις όπου παρατηρούνται προβλήματα παραβίασης της ιδιωτικότητας των χρηστών κατά την εκτέλεση της ψηφιακής δικανικής.

2.4. Privacy Issues in Digital Forensics

Από τα προαναφερθέντα γίνεται κατανοητό ότι κατά τη διαδικασία της συλλογής των αποδεικτικών στοιχείων υφίσταται η πιθανότητα να παραβιαστούν προσωπικά δεδομένα κάποιου χρήστη. Ο ψηφιακός ερευνητής κατά την εκτέλεση της διαδικασίας συλλογής ψηφιακών πειστηρίων που περιεγράφηκε στην παράγραφο 2.2 θα αναζητήσει αρχεία τα οποία ενδέχεται να βρεθούν στις ακόλουθες μορφές: [42]

α) Κρυπτογραφημένα με αλγόριθμο κρυπτογράφησης ή με τεχνική Anti-Forensics και μπορεί να είναι φωτογραφίες, βίντεο και αρχεία κειμένου διάφορων ατόμων χωρίς τη δυνατότητα a priori να ταυτοποιηθούν οι ιδιοκτήτες τους.

β) Μετα-δεδομένα δραστηριότητας των χρηστών στο υπό εξέταση πληροφοριακό σύστημα (για παράδειγμα χρήση των εφαρμογών, είσοδος-έξοδος από εφαρμογές, cookies για το διαδίκτυο).

γ) Αρχεία καταγραφής δραστηριότητας και αρχεία καταγραφής συμβάντων όπου καταγράφεται η δικτυακή ροή όλων των χρηστών του εν λόγω συστήματος.

Τα μετα-δεδομένα της δραστηριότητας των χρηστών στο διαδίκτυο είναι διαθέσιμα στον ψηφιακό ερευνητή με τη χρήση των κατάλληλων εργαλείων δικανικής έρευνας (Forensic Tools) ακόμα και αν οι on line συναλλαγές τους γίνουν με τη χρήση της in cognito λειτουργίας των browsers [44] καθιστώντας προσωπικά στοιχεία τρίτων ατόμων διαθέσιμα κατά τη διαδικασία της ψηφιακής δικανικής. Στο ίδιο άρθρο αναφέρεται ότι ακόμα και αρχεία κειμένου τα οποία ανήκουν στα άτομα για τα οποία έχει εκδοθεί ένταλμα έρευνας μπορεί να περιέχουν διαδραστικά δεδομένα τα οποία συσχετίζονται με τρίτα ως προς την υπόθεση άτομα. Επιπρόσθετα, από την ανωτέρω διαδικασία συλλογής ψηφιακών πειστηρίων ο ψηφιακός ερευνητής αποκτά το σύνολο των ψηφιακών μέσων αποθήκευσης που ανήκουν στον ύποπτο της υπό εξέταση υπόθεσης και τα οποία μπορεί να περιλαμβάνουν προσωπικά αρχεία (ιατρικά δεδομένα, οικογενειακές φωτογραφίες-βίντεο) τα οποία δεν συσχετίζονται με την υπόθεση και η απόκτηση και η επεξεργασία αυτών αποτελεί καταπάτηση της ιδιωτικότητάς του [45].

Λόγω των ανωτέρω τεχνικών όπου συνήθης είναι η πρακτική να λαμβάνονται πλήρη αντίγραφα του σκληρού δίσκου του υπό εξέταση συστήματος ώστε να διασφαλισθεί η ακεραιότητα των δεδομένων υφίσταται η πιθανότητα κατά την εξέταση των e-mail server ο ψηφιακός ερευνητής να αποκτήσει πρόσβαση στα mail χιλιάδων χρηστών που δεν έχουν σχέση με την υπόθεση, ακόμα και αν η αναζήτηση για συγκεκριμένα mail έχει γίνει με τη χρήση προσδιορισμένων λέξεων-κλειδιών. [1] Μία έτερη πρακτική είναι να λαμβάνεται κρυπτογραφημένο το πλήρες αντίγραφο του δίσκου με αποτέλεσμα ο ψηφιακός ερευνητής να μην μπορεί a priori να εντοπίσει τα σχετικά με την υπόθεση δεδομένα. Υπάρχουν και οι περιπτώσεις όπου μπορεί να λάβει το κλειδί αποκρυπτογράφησης με αποτέλεσμα τα προσωπικά δεδομένα τρίτων ως προς την υπόθεση ατόμων να παραβιάζονται [1].

Πέρα από τη διαδικασία που θα ακολουθηθεί για τη συλλογή των ψηφιακών πειστηρίων, το πρόβλημα της ιδιωτικότητας κατά τη συλλογή δεδομένων έγκειται και στην ακεραιότητα του ίδιου του ερευνητή. Βάσει των προγραμματισμένων διαδικασιών που ακολουθούνται κατά την έρευνα (Standard Operating Procedures, SOPs) ο ψηφιακός ερευνητής έρχεται συνήθως σε επαφή με πληροφορίες που δεν είναι άμεσα συσχετίσιμες με την υπό εξέταση υπόθεση [46]. Επιπρόσθετα, στα [47,48] αναφέρεται από τον Επίτροπο της Ευρωπαϊκής Ένωσης για τις εσωτερικές υποθέσεις ότι οι κάτοικοι της Ε.Ε. πρέπει να προστατευτούν από περιπτώσεις κακόβουλων ερευνητών. Είναι επιπλέον πιθανό κατά την έρευνα ο ψηφιακός ερευνητής να μην αποκαλύψει ορισμένα στοιχεία προσωπικού χαρακτήρα ώστε να τα χρησιμοποιήσει μετέπειτα για ιδίους σκοπούς [49]. Αυτό ωστόσο δεν αποτελεί μόνο παραβίαση της ιδιωτικότητας των προσωπικών δεδομένων αλλά θέτει ενδεχομένως σε κίνδυνο και τον οργανισμό που δέχεται την ψηφιακή δικανική έρευνα καθώς η γνωστοποίηση παραβίασης των εν λόγω στοιχείων θα έχει αρνητικό αντίκτυπο στη φήμη του και θα του προσδώσει αρνητική δημοσιότητα.

Από την παράγραφο 2.3 έγινε κατανοητό ότι τόσο τα PETs όσο και τα Anti-Forensics τυχαίνουν ευρείας αποδοχής και η χρήση τους ολοένα και αυξάνεται. Η χρήση τους ωστόσο ενέχει κινδύνους για την ιδιωτικότητα των χρηστών κατά τη συλλογή ψηφιακών πειστηρίων από τον ψηφιακό ερευνητή. Στο [40] αναφέρονται τα ακόλουθα:

α) Μερικοί από τους χρήστες που εγκαθιστούν εργαλεία Anti-Forensics δεν τα χρησιμοποιούν σωστά με αποτέλεσμα σημαντικά προσωπικά δεδομένα να παραμένουν διαθέσιμα.

β) Μερικά εργαλεία Anti-Forensics δεν λειτουργούν με τον τρόπο που διαφημίζονται αφήνοντας στοιχεία που μπορεί να οδηγήσουν στην ανάκτηση των δεδομένων.

Αναλυτικότερα, τα ανωτέρω εργαλεία παρουσιάζουν τις ακόλουθες δυσλειτουργίες οι οποίες μπορούν να εκθέσουν τα προσωπικά δεδομένα χρηστών στον ψηφιακό ερευνητή [50]:

α) Incomplete wiping of unallocated space.

β) Failures in erasing targeted user and system files.

γ) Registry usage records missed.

δ) Data recoverable from special filesystem structures.

ε) Archived Registry hives recoverable.

Συνεπώς, η χρήση ορισμένων προγραμμάτων Anti-Forensics οδηγεί στην ελλιπή διαγραφή των δεδομένων με αποτέλεσμα κρίσιμα προσωπικά δεδομένα να καθίστανται διαθέσιμα στον ψηφιακό ερευνητή [51]. Ο επόμενος πίνακας παρουσιάζει συνοπτικά τους τομείς που γνωστά εργαλεία Anti-Forensics αποτυγχάνουν να εκτελέσουν εκκαθάριση των δεδομένων με αποτέλεσμα να παραβιάζεται η ιδιωτικότητα των ατόμων από τον ψηφιακό ερευνητή [53]:

	Wiping failures - 'free' space	Wiping failures - targeted files	Registry records missed	Activity files missed	Data recoverable from filesystem structures
Acronis Privacy Expert 8	Multi-paragraph text, fragment of browser History index, cached Web pages all recoverable.	File metadata not overwritten; Recycle Bin index file not wiped, allowing recovery of original metadata for bin contents; failed to delete designated mail from Outlook 2003.	Several keys under the ComDlg32 branch were intact, revealing recently used folders and documents; "Save As" key for Microsoft Office overlooked; IE download directory location.	Restore Point data, including user registry back-ups not eliminated; omitted a Windows prefetch folder component that contained path info and names of wiped files; recent Office document shortcuts missed; IE browsing cache index file only partially wiped.	Cookies, small images resident in MFT recoverable; file name data disclosed in NTFS journal.
Absolute Shield 3.42	Multi-paragraph text, cached Webmail page views recoverable.	User cannot designate arbitrary files for wiping; metadata not overwritten.	Yahoo profile chat partner disclosure; "Save As" key for Microsoft Office overlooked; ShellNoRoam/ BagMRU key revealed file names.	Restore Point data, including user registry back-ups not eliminated; Windows prefetch folder intact, disclosing path and names, other data, for wiped files.	Cookies, small images resident in MFT recoverable; file name data disclosed in NTFS journal; directory index files for some folders contained entries disclosing wiped file names; pagefile contained multi-paragraph text from deleted documents.
Cyber Scrub Privacy Suite 4	Multi-paragraph text, fragments of Web pages recoverable; file slack incompletely wiped, revealing fragments of documents, web data.	Yahoo IM client log renamed but not deleted.	RecentDocs key in user hive listed recently used documents, broken down by file type.	IE History, IE cache and IE cookie index files all were missed; Windows Media Player resource file with content URL missed; Windows prefetch folder intact, disclosing path and names, other data, for wiped files.	Wiped file name data disclosed in NTFS journal and in a few unallocated MFT entries.
Evidence Blaster 2005	Did not feature wiping of unallocated space; extensive data recovery possible.	Deleted but failed to wipe user-specified documents and files under My Docs folder; also failed to wipe contents of Recycle Bin, IE cache files and cookies; metadata not obfuscated.	ComDlg32 branch was intact, revealing recently used folders and documents; recent search terms also not wiped; WordPad recent file key intact; "Save As" key for Microsoft Office overlooked.	IE History index file incompletely purged, leaving some record elements; IE browsing cache index file was also only partially cleaned; Yahoo IM client log missed; Windows Media Player resource file with content URL missed.	Pagefile contained multi-paragraph text from deleted documents and web content; directory index files for some folders contained entries disclosing wiped file names.
Evidence Eliminator 5.058 b14	A small number of references to wiped file names and paths were recoverable.	__eetemp directory in filesystem root contained undeleted copies of prefetch folder files, as well as IE History, cache and cookie index files.	"Save As" keys for Microsoft Office applications missed; ShellNoRoam/ BagMRU key revealed file names.	Windows Media Player resource file with content URL missed.	Directory index files for some folders contained entries disclosing wiped file names.

	Wiping failures - 'free' space	Wiping failures - targeted files	Registry records missed	Activity files missed	Data recoverable from filesystem structures
History Kill 2005	Did not feature wiping of unallocated space; extensive data recovery possible.	User cannot designate arbitrary files for wiping; deleted but failed to wipe many of the files targeted for elimination, including contents of Recycle Bin and IE cache; browser History files deleted but not wiped.	ComDlg32 branch was largely untouched, revealing recently used folders and documents; Acrobat recent file list remained; WordPad recent file key intact; "Save As" key for Microsoft Office overlooked.	Restore Point data, including user registry back-ups not eliminated; Windows prefetch folder intact, disclosing path and names, other data, for wiped files; shortcut files to recent Office documents overlooked.	Cookies, small images resident in MFT recoverable; wiped file name data disclosed in NTFS journal; pagefile contained multi-paragraph text from deleted documents, web pages.
Privacy Eraser Pro 5.0	Multi-paragraph text and fragments of Web pages recoverable; file slack incompletely wiped, revealing fragments of documents, web data.	Restore Point files deleted but not wiped, allowing recovery; same true of Windows prefetch folder contents and Recycle Bin index file.	"Save As" key for Microsoft Office overlooked; ShellNoRoam/ BagMRU key revealed file names.	IE browsing cache index file was also only partially cleaned; Windows Media Player resource file with content URL was missed; Yahoo IM client log missed.	Wiped file name data disclosed in NTFS journal and in a few unallocated MFT entries.
Privacy Guardian 4.0	Multi-paragraph text and fragments of Web pages recoverable.	Wiping failed for most of the user-specified files under the My Docs folder tree – some were also left undeleted; IE cache index only partially purged.	"Save As" key for Microsoft Office overlooked.	Windows prefetch folder intact, disclosing path and names, other data, for wiped files; missed MS Office shortcuts to recently used files and Yahoo IM client log; IE cookie index file overlooked.	Wiped file name data disclosed in NTFS journal and in a few unallocated MFT entries; pagefile contained multi-paragraph text from deleted documents, fragments of web pages and IM chat sessions; cookies and images small enough to be resident in the MFT were recoverable.
Secure Clean 4	A small number of references to wiped file names and paths were recoverable; slack space for one file contained fragments of cached web page.	Failed to purge deleted mail stores in both Outlook Express and Outlook 2003.	"Save As" key for Microsoft Office overlooked; ShellNoRoam/ BagMRU key revealed file names.	Windows prefetch folder intact, disclosing path and names, other data, for wiped files;	Wiped file name data disclosed in NTFS journal and in a few unallocated MFT entries.

	Wiping failures - 'free' space	Wiping failures - targeted files	Registry records missed	Activity files missed	Data recoverable from filesystem structures
TracksCleaner 3.0	Function to wipe unallocated space froze without progress repeatedly on test system; slack space contained numerous fragments of targeted documents and web content.	Failed to wipe most user-targeted files, and Recycle Bin contents, conventionally deleting instead; also failed to wipe program-selected files, including IE cache contents, files in the system Temp folder and browser History files.	ComDlg32 tree largely untouched, revealing recently used documents; Acrobat recent file list remained; Explorer Recent Docs key intact; "Save As" key for Microsoft Office overlooked.	Restore Point data, including user registry back-ups not eliminated; Windows prefetch folder intact, disclosing path and names, other data, for wiped files; IE cache index file left untouched.	Wiped file name data disclosed in NTFS journal and in a few unallocated MFT entries; pagefile contained numerous web page fragments and multi-paragraph text from deleted documents, and IM chat sessions;
Window Washer 6	Multi-paragraph text, fragments of Web pages recoverable; file slack incompletely wiped, revealing fragments of documents, web data.	Deleted message fragment recovered from Outlook Express mail store; browser History file contained a few references to activity prior to wiping tool's operation.	"Save As" key for Microsoft Office overlooked; ShellNoRoam/ BagMRU key revealed file names.	Restore Point data, including user registry back-ups not eliminated; Windows prefetch folder intact, disclosing path and names, other data, for wiped files; IE cache index file left untouched; missed MS Office shortcuts to recently used files and Yahoo IM client log.	Pagefile contained numerous web page fragments and multi-paragraph tracts from deleted documents, and IM chat sessions; wiped file name data disclosed in NTFS journal and in a few unallocated MFT entries; directory index files for some folders contained entries disclosing wiped file names.

Πίνακας 2: Privacy preserving Failure points of known AF tools

Μία έτερη κατάσταση που μπορεί να προκαλέσει προβλήματα ιδιωτικότητας είναι κατά τη διαδικασία της εργαστηριακής ανάλυσης των δεδομένων αυτά να αναλύονται από ερευνητές διαφορετικού κράτους και κατ' επέκταση διαφορετικού νομικού πλαισίου αναφορικά με την προστασία της ιδιωτικότητας [14]. Για παράδειγμα, τα κράτη- μέλη της Ε.Ε. διέπονται από το GDPR ενώ οι Ηνωμένες Πολιτείες της Αμερικής δεν έχουν κάποια εθνική νομοθεσία επί του θέματος και ακολουθούν σε κάθε πολιτεία διαφορετικά πρότυπα [53].

Υπάρχει ωστόσο η περίπτωση και τα εργαλεία εκτέλεσης της ψηφιακής δικανικής έρευνας να οδηγήσουν τον ψηφιακό ερευνητή σε παραβίαση προσωπικών δεδομένων. Σύμφωνα με το [54] ορισμένα γνωστά εργαλεία ευρέθησαν με ευπάθειες οι οποίες αξιοποιούμενες από κακόβουλους χρήστες μπορούν να οδηγήσουν σε κοινοποίηση των συλλεχθέντων στοιχείων σε τρίτους και κατ' επέκταση αλλοίωση των δεδομένων και προσβολή τους ως αποδεικτικό μέσο. Έτερα εργαλεία χρησιμοποιούν τεχνικές Data Mining για τη συλλογή διάφορων πληροφοριών από το προς εξέταση σύστημα τις οποίες και έπειτα συσχετίζουν με σκοπό τη δημιουργία προφίλ χρηστών. Αυτό έχει ως αποτέλεσμα να υφίσταται η πιθανότητα σκιαγράφησης της δραστηριότητας χρηστών που δεν σχετίζονται με την προς εξέταση υπόθεση [55].

Επιπρόσθετα, όσο αυξάνονται οι αποθηκευτικές δυνατότητες των συσκευών τόσο αυξάνεται και η πιθανότητα να έχουν αποθηκευτεί (ή και διαγραφεί) προσωπικά δεδομένα διαφόρων χρηστών. Κατά την ανάλυση των αρχείων καταγραφής της registry αναφορικά με τη χρήση του σκληρού δίσκου μπορεί να αποσπαστούν στοιχεία χρήσης για δραστηριότητες που δεν σχετίζονται με την υπό διερεύνηση υπόθεση [56]. Επίσης, ακόμα και από τα διεγραμμένα αρχεία μπορούν να ανακτηθούν πληροφορίες γι' αυτά (meta data) οι οποίες μπορούν να οδηγήσουν στην ιχνηλάτηση της συμπεριφοράς των χρηστών (ανάκτηση εικόνων, συνομιλιών, logs εφαρμογών κτλ) [57]. Εκτός αυτού, μπορεί να αποσπαστούν πληροφορίες που είναι αποκλειστικές για την κατασκευάστρια εταιρεία είτε υπό την μορφή κατασκευαστικών χαρακτηριστικών των συσκευών και του αντίστοιχου λογισμικού είτε μέσω της ανάκτησης εταιρικών συνομιλιών και email. [57] Τέλος, στο ίδιο άρθρο αναφέρεται ότι μέχρι τα meta data να ανακτηθούν και να αναλυθούν δεν είναι δυνατός ο προσδιορισμός του ιδιοκτήτη τους οπότε αναπόφευκτα προσωπικές πληροφορίες θα περιέλθουν στην κατοχή του ερευνητή κατά το στάδιο της εργαστηριακής ανάλυσης.

Σύμφωνα με το άρθρο [57] έντονο είναι το πρόβλημα με τα meta data στα συστήματα βάσεων δεδομένων όπου τηρούνται πολλαπλά αντίγραφα των βάσεων δεδομένων και των αρχείων δραστηριότητας (data items in table storage, indexes, logs, materialized views, temporary relations) τα οποία περιλαμβάνουν προσωπικές πληροφορίες οι οποίες μπορούν να ανακτηθούν από τον ερευνητή κατά την at scene ψηφιακή δικανική έρευνα. [58] Επίσης, τα database forensics αντιμετωπίζουν ορισμένα προβλήματα προστασίας της ιδιωτικότητας καθώς ορισμένα δικαιώματα των χρηστών καταπατούνται ως ακολούθως:[13]

α) Προστασία των δεδομένων των ατόμων που δεν εμπλέκονται με την υπό εξέταση υπόθεση σε μία post-mortem έρευνα με την υιοθέτηση συγκεκριμένων κανόνων αποθήκευσης των δεδομένων.

β) Το δικαίωμα πρόσβασης στα δεδομένα καταπατείται καθώς ο ερευνητής a priori αποκτά τα δεδομένα κατά τη φάση της at scene ψηφιακής δικανικής έρευνας.

γ) Το δικαίωμα της ασφαλούς διαγραφής των δεδομένων καταπατείται καθώς με τη συλλογή των meta data αυτά πολλές φορές καθίστανται ανακτήσιμα.

Ένα έτερο πρόβλημα παραβίασης της ιδιωτικότητας κατά τα cloud forensics είναι η συλλογή προσωπικών στοιχείων πολλών χρηστών μίας cloud server-εφαρμογής λόγω του multi-tenant χαρακτήρα της (με τον όρο multi-tenancy εννοούμε τη λήψη δεδομένων ταυτόχρονα από πολλές πηγές. Αυτό έχει ως αποτέλεσμα να συλλεχθούν στοιχεία πολλών και διαφορετικών προελεύσεων οδηγώντας στο λεγόμενο third party privacy breach (TPPB) [59]). Παράλληλα δημιουργείται ζήτημα προστασίας της ιδιωτικότητας και κατά την έρευνα σε cloud based servers με διαμοιραζόμενους πόρους. Σε αυτούς τους servers η κοινή χρήση ενός αρχείου ή πόρου από πολλούς χρήστες αλλοιώνει την ταυτότητα κατοχής του αρχείου οπότε μπορεί τα κακόβουλα αρχεία να ανακατευτούν με αρχεία από μη κακόβουλους χρήστες με αποτέλεσμα να υπάρχει ο κίνδυνος εκτέλεσης ψηφιακής δικανικής έρευνας σε προσωπικά στοιχεία τρίτων ατόμων [60].

Τέλος, κατά τη διενέργεια των Mobile Forensics ο ψηφιακός ερευνητής ενδέχεται να συλλέξει κωδικούς αυθεντικοποίησης χρηστών που είναι αποθηκευμένοι στην προσωρινή μνήμη των κινητών (volatile memory-data in motion) [99] και λαμβάνοντας υπόψη ότι οι χρήστες επαναχρησιμοποιούν τα ίδια διαπιστευτήρια σε πολλές εφαρμογές [98] είναι πολύ πιθανή η παραβίαση προσωπικών δεδομένων με την απόκτηση πρόσβασης στα εν λόγω στοιχεία. Επιπρόσθετα, η πρόσβαση σε δεδομένα που αποθηκεύουν οι εφαρμογές της google σε μία κινητή συσκευή μπορεί να διευκολύνει τον ψηφιακό ερευνητή στην σκιαγράφηση του συμπεριφορικού προφίλ του χρήστη αυτής καθώς και να επιβεβαιώσει την εγκυρότητα των ευρημάτων σε άλλα σημεία της συσκευής [100] με αποτέλεσμα να υφίσταται κίνδυνος ο ερευνητής να έρθει σε επαφή με προσωπικά δεδομένα του χρήστη της εν λόγω συσκευής.

Συνοψίζοντας τα ανωτέρω, οι υφιστάμενες τεχνικές εκτέλεσης ψηφιακής δικανικής έρευνας ενέχουν τον κίνδυνο καταπάτησης της ιδιωτικότητας τρίτων ως προς την υπόθεση ατόμων τόσο λόγω σφάλματος των εφαρμοζόμενων τεχνικών και των εργαλείων ψηφιακής δικανικής, όσο και λόγω αστοχιών των εργαλείων Anti-Forensics και του υφιστάμενου νομικού πλαισίου. Ορισμένες από τις προαναφερθείσες ευπάθειες συνοψίζονται στον ακόλουθο πίνακα:

Digital Forensic Procedures	**Privacy Issues**
Indiscriminate acquisition/collection of digital data	**Third Party Privacy** Breach (TPPB) must be avoided
Full disk images are created and analysed	Deleted files can lead to **false accusations**
Data can be collected from personal devices	Need for **informed consents** complete and understandable by the users
During the investigation, the data to be acquired may be hosted on servers in different countries	Different **jurisdictions** can understand privacy differently
Warrants can be necessary during private investigation.	Matching of **privacy policies** and **warrants** (formally defined) for automated analysis.
Correlation is needed in order to build a timeline	**Multi-device** context (more and more data)
Digital forensics tools and methodologies must be accepted and tested by a broad group of experts in the field	Privacy requirements must be integrated by design in **existing tools and methodologies**
Digital forensic principles must be guaranteed	The **manipulation of data** (e.g., encryption) to protect privacy must be done considering digital forensic principles 8.2.2.1

Πίνακας 3: Privacy issues in Digital Forensics

Στο επόμενο κεφάλαιο θα αναλυθούν οι τρόποι και οι τεχνικές με τους οποίους μπορεί να εκτελεστεί ψηφιακή δικανική έρευνα με έμφαση στην προστασία των προσωπικών δεδομένων.

Κεφάλαιο 3

3.1. Εισαγωγή

Η ασφάλεια της πληροφορίας παραδοσιακά διέπεται από τις αρχές της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Αντίθετα, η ιδιωτικότητα της πληροφορίας διέπεται από ηθικούς κανόνες και νόμους και συνήθως η προστασία αυτής δεν επιτυγχάνεται μόνο με τις ανωτέρω αρχές προστασίας της ασφάλειας της πληροφορίας. [61] Συνεπώς και όπως έγινε κατανοητό στις προηγούμενες παραγράφους η ιδιωτικότητα της πληροφορίας καταπατάται συχνά κατά την εκτέλεση της ψηφιακής δικανικής έρευνας σε όλες τις μορφές της κάνοντας επιτακτική την ανάγκη θέσπισης κανόνων και τεχνικών ώστε ο ψηφιακός ερευνητής να εκτελεί απρόσκοπτα και κατά privacy aware τρόπο την εν λόγω έρευνα. Στις παραγράφους που ακολουθούν θα αναλυθούν τεχνικές όπου καθιστούν δυνατή την εκτέλεση ψηφιακής δικανικής έρευνας ενώ ταυτόχρονα προστατεύονται τα προσωπικά δεδομένα τρίτων ως προς την υπόθεση χρηστών.

Γενικά, οι τεχνικές προστασίας της ιδιωτικότητας κατά την εκτέλεση της ψηφιακής δικανικής έρευνας χωρίζονται σε δύο κατηγορίες: α) εφαρμογή μεθοδολογιών-πολιτικών ασφαλείας και β) εφαρμογή τεχνολογικών μέσων [62].

3.1.1. Εφαρμογή μεθοδολογιών-πολιτικών ασφαλείας

Γενικά, οι ισχύουσες πολιτικές για τη συλλογή και επεξεργασία των δεδομένων είναι οι ακόλουθες [62]:

α) Δημιουργία δύο ψηφιακών αντιγράφων των αποκτηθέντων δεδομένων από τα οποία το ένα θα τηρηθεί από τον ιδιοκτήτη τους και το άλλο από τον ψηφιακό ερευνητή.

β) Διαγραφή μη σχετικών με την υπόθεση αρχείων με χρήση των υφιστάμενων εργαλείων διαγραφής.

γ) Περιορισμό της έρευνας στα εναπομείναντα δεδομένα σε αυτά για τα οποία έχει εκδοθεί ένταλμα έρευνας.

δ) Χειρισμός των δεδομένων ως εμπιστευτικά.

Στο [62] προτείνεται η κατηγοριοποίηση των τεχνικών στις ακόλουθες τρεις κατηγορίες με κάθε μία να αναλύεται σε επιμέρους πολιτικές για την εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία των προσωπικών δεδομένων με γνώμονα τις υφιστάμενες μεθοδολογίες απόκτησης-ανάλυσης και παρουσίασης των δεδομένων που αναλύθηκαν σε προηγούμενες παραγράφους:

α) Imaging privacy policies.

β) Analysis privacy policies.

γ) Presentation privacy policies.

3.1.1.1. Imaging privacy policies

Στην κατηγορία αυτή περιλαμβάνονται οι ακόλουθες πολιτικές:

α) Επίδειξη του εντάλματος έρευνας στον ιδιοκτήτη των δεδομένων με σκοπό αυτός να είναι ενήμερος για ποια δεδομένα θα συλλεχθούν και θα επεξεργαστούν.

β) Παροχή της δυνατότητας στον ιδιοκτήτη των δεδομένων να κατηγοριοποιήσει τα δεδομένα του ως προσωπικά και μη προσωπικά.

γ) Λαμβάνοντας υπόψη την προηγούμενη κατηγοριοποίηση, ο ψηφιακός ερευνητής συλλέγει δεδομένα σχετικά με την εξεταζόμενη υπόθεση (οι τεχνικές συλλογής και τα είδη των δεδομένων που συλλέγονται έχουν αναλυθεί σε προηγούμενη παράγραφο).

δ) Εάν ζητηθεί από τον ιδιοκτήτη των δεδομένων, τότε στο πλαίσιο διατήρησης της εμπιστευτικότητας αυτών πρέπει να κρυπτογραφηθούν πριν αποθηκευτούν για δικανική ανάλυση.

ε) Χρησιμοποίηση hash functions και ψηφιακών υπογραφών για τη διατήρηση της ακεραιότητας και της αυθεντικότητας των συλλεχθέντων δεδομένων.

στ) Καταγραφή της διαδικασίας συλλογής των δεδομένων, τοποθέτηση ψηφιακής υπογραφής του ψηφιακού ερευνητή σε κάθε αναφορά και παράδοση ενός αντιγράφου κάθε αναφοράς καθώς και ενός αντιγράφου της ψηφιακής υπογραφής του στον κάτοχο των δεδομένων.

ζ) Παράδοση στον κάτοχο των δεδομένων αντιγράφου της ψηφιακής υπογραφής των συλλεχθέντων δεδομένων.

3.1.1.2. Analysis privacy policies

Στην κατηγορία αυτή περιλαμβάνονται οι ακόλουθες πολιτικές που αφορούν την επεξεργασία των συλλεχθέντων δεδομένων κατά την φάση της ανάλυσης αυτών από τον ψηφιακό ερευνητή:

α) Η επεξεργασία των κρυπτογραφημένων προσωπικών δεδομένων πρέπει να γίνει από εξουσιοδοτημένο προσωπικό και επιτρέπεται η αποκρυπτογράφησή τους μόνο μέσω κατάλληλου λογισμικού και μόνο για το διάστημα που εκτελείται η επεξεργασία αυτών.

β) Καταγραφή της διαδικασίας επεξεργασίας των δεδομένων ώστε να είναι δυνατή σε μεταγενέστερο χρόνο η εξέταση εάν συντελέστηκε παραβίαση των προσωπικών δεδομένων του κατόχου αυτών.

γ) Απαγορεύεται η χρήση των συλλεχθέντων δεδομένων για σκοπούς πέρα από αυτούς που καθορίζονται στο ένταλμα έρευνας.

3.1.1.3. Presentation privacy policies

Στην κατηγορία αυτή περιλαμβάνονται οι ακόλουθες πολιτικές που καθορίζουν τον τρόπο αποθήκευσης και επεξεργασίας των δεδομένων μετά την ολοκλήρωση της ανάλυσης αυτών και ποια άτομα θα έχουν πρόσβαση σε αυτά:

α) Το δικαστήριο μπορεί να ελέγξει τις δραστηριότητες του ψηφιακού ερευνητή ώστε να εξακριβώσει ότι τα συλλεχθέντα και επεξεργασθέντα δεδομένα είναι σύμφωνα με το ένταλμα έρευνας για την υπό εξέταση υπόθεση.

β) Τα δεδομένα που αφορούν την εξεταζόμενη υπόθεση (τόσο αυτά που κατέχονται από τον ιδιοκτήτη των δεδομένων όσο και από τον ψηφιακό ερευνητή) είναι άμεσα ελεγχόμενα από το δικαστήριο ώστε να είναι δυνατή η έρευνα εάν παρουσιαστεί παραβίαση αυτών των δεδομένων.

γ) Τα συλλεχθέντα δεδομένα θα διαγραφούν μόνιμα όταν η υπόθεση εκδικαστεί ή ακυρωθεί από το δικαστήριο.

3.1.2. Εφαρμογή τεχνολογικών μέσων

Η προστασία των προσωπικών δεδομένων με τη χρήση τεχνολογικών μέσων κατά την εκτέλεση της ψηφιακής δικανικής έρευνας μπορεί να χωριστεί στις ακόλουθες κατηγορίες: [14]

α) Εφαρμογή τεχνολογιών και μέσων ώστε οι εταιρείες να διασφαλίζουν την ετοιμότητά τους για εκτέλεση ψηφιακής δικανικής έρευνας με ταυτόχρονη την προστασία τόσο των εταιρικών δεδομένων όσο και των προσωπικών δεδομένων των πελατών και των υπαλλήλων.

β) Privacy-preserving τεχνικές data mining που επιτρέπουν την έρευνα στα δεδομένα που έχουν συλλεχθεί περιορίζοντας την παραβίαση ευαίσθητων ή προσωπικών πληροφοριών.

γ) Τεχνικές επιλεκτικής παρουσίασης των κατεχόμενων πληροφοριών μέσω μεθόδων ανωνυμοποίησης και κρυπτογράφησης.

Στην παράγραφο που θα ακολουθήσει θα γίνει εκτενής λόγος για τις προτεινόμενες τεχνολογίες και τεχνικές που μπορούν να εφαρμοστούν ώστε να εκτελεστεί ψηφιακή δικανική έρευνα με ταυτόχρονη την προστασία των προσωπικών δεδομένων.

3.2. Frameworks for privacy aware digital forensics

Αρχικά, στο [63] περιγράφεται μία τεχνική για την εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία προσωπικών δεδομένων αναφορικά με τα e-mail μιας εταιρείας. Κατά την εν λόγω τεχνική ο ψηφιακός ερευνητής αναζητεί ψηφιακά πειστήρια σε κρυπτογραφημένο τμήμα των e-mail που έχει ζητήσει με βάση ορισμένες λέξεις-κλειδιά και αν ο αριθμός των λέξεων φτάσει ένα προκαθορισμένο κατώφλι αποκρυπτογραφούνται τα e-mail που περιέχουν τις εν λόγω λέξεις. Η εταιρεία στην οποία ανήκουν τα e-mail μπορεί να καθορίσει το όριο των λέξεων-κλειδιών από το οποίο και πέρα θα αποκρυπτογραφούνται τα e-mail καθώς και να αποκλείσει λέξεις-κλειδιά από την αναζήτηση όπως πχ. το όνομα της εταιρείας, προσφωνήσεις κτλ. Η τεχνική χρησιμοποιεί γνωστές κρυπτογραφικές μεθόδους συνδυάζοντας τεχνικές συμμετρικής κρυπτογράφησης, τεχνικές hashing και τεχνικές διαμοιρασμού μυστικού κλειδιού. Αναλυτικότερα, η τεχνική απαρτίζεται από τα εξής στάδια:

α. Η εταιρεία συλλέγει τους λογαριασμούς mail που εκτιμάται ότι εμπλέκονται με την υπό εξέταση υπόθεση.

β. Η εταιρεία ή ο data protection officer της εταιρείας κρυπτογραφεί τα ανωτέρω e-mail με χρήση της εν λόγω μεθόδου χρησιμοποιώντας τον αριθμό κωδικών λέξεων που έχουν καθοριστεί από την εταιρεία όπως επίσης και τις λέξεις που αποκλείονται από την αναζήτηση.

γ. Τα κρυπτογραφημένα δεδομένα παραδίδονται στον ψηφιακό ερευνητή.

δ. Ο ψηφιακός ερευνητής εκτελεί έρευνα στο κρυπτογραφημένο αρχείο πληκτρολογώντας λέξεις-κλειδιά και αποκρυπτογραφούνται μόνο αυτά τα email που περιέχουν τουλάχιστον το κατώτερο όριο λέξεων-κλειδιών που όρισε η εταιρεία.

Ένας έτερος τρόπος για να εκτελεστεί ψηφιακή δικανική έρευνα με έμφαση στην προστασία προσωπικών δεδομένων στις κινητές συσκευές είναι να χρησιμοποιηθούν δεδομένα γεωγραφικού προσδιορισμού των χρηστών όπου με τη χρήση προγράμματος αποθηκεύεται το ιστορικό της γεωγραφικής θέσης των κινητών συσκευών. [64] Ο ψηφιακός ερευνητής αποκτά ένταλμα έρευνας για μία συγκεκριμένη περιοχή και έπειτα μέσω του προγράμματος για την εν λόγω περιοχή αναλύει τις κινήσεις των κινητών συσκευών περιορίζοντας την έρευνά του σε αυτές που θεωρεί ύποπτες. Έπειτα, για τις συσκευές που υπάρχουν υποψίες ζητείται από την google η αποκάλυψη της ταυτότητας των κατόχων τους. Καθόλη τη διάρκεια της διαδικασίας και πριν η google αποκαλύψει τα στοιχεία των υπόπτων τα προσωπικά δεδομένα τους προστατεύονται καθώς οι κινητές συσκευές χαρακτηρίζονται μόνο με αριθμούς.

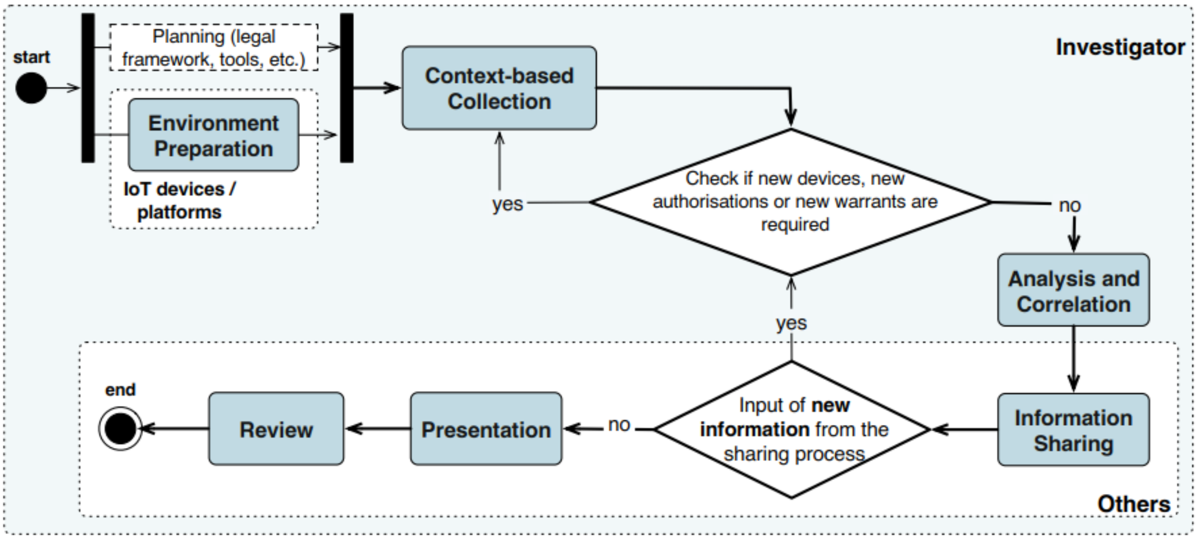
Ένας έτερος τρόπος για να εκτελεστεί ψηφιακή δικανική έρευνα με έμφαση στην προστασία προσωπικών δεδομένων στα κοινωνικά δίκτυα είναι η χρήση του αλγορίθμου «Compute Metrics» με τον οποίο γίνεται ανάλυση των ποσοτήτων «Betweenness centrality[2]» και «Closeness Centrality[3]» χωρίς να αποκαλύπτονται πληροφορίες για τους ενδιάμεσους κόμβους και το συνολικό κοινωνικό δίκτυο (με εξαίρεση το μέγεθος αυτού). [65] Με την ανάλυση των εν λόγω ποσοτήτων ο ψηφιακός ερευνητής μπορεί να εντοπίσει τους κόμβους των οποίων η δραστηριότητα θεωρείται ύποπτη ως προς την εξεταζόμενη υπόθεση χωρίς να αποκαλύπτονται προσωπικά ή ανωνυμοποιημένα στοιχεία για τους εν λόγω κόμβους, προστατεύοντας με αυτόν τον τρόπο την ιδιωτικότητά τους.

---

[2] **Betweenness centrality** is a way of detecting the amount of influence a node has over the flow of information in a graph. It is often **used** to find nodes that serve as a bridge from one part of a graph to another.

[3] **Closeness centrality** is a useful measure that estimates how fast the flow of information **would** be through a given node to other nodes. **Closeness centrality** measures how short the shortest paths are from node i to all nodes.

Ένας έτερος τρόπος για εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία προσωπικών δεδομένων σε περιβάλλον IOT συσκευών είναι η χρήση του μοντέλου PROFIT (Privacy Aware IOT Forensics). Κατά το εν λόγω μοντέλο χρήστες συσκευών IOT έχουν την δυνατότητα αρχικά της αυτόβουλης συνεργασίας με τον ψηφιακό ερευνητή παρέχοντας τα απαραίτητα για την έρευνα στοιχεία. [66] Καθόλη τη διάρκεια της διαδικασίας οι χρήστες των συσκευών διατηρούν τον έλεγχο των προσωπικών δεδομένων που υπάρχουν στις συσκευές τους με την εφαρμογή ενός συνόλου αρχών προστασίας της ιδιωτικότητας. Τα στάδια της εν λόγω διαδικασίας παρουσιάζονται στο ακόλουθο διάγραμμα και αναλύονται ως εξής: [67]



Διάγραμμα 1: Μοντέλο PROFIT

α) Προετοιμασία: Το εν λόγω στάδιο δεν περιγράφεται στο ανωτέρω διάγραμμα και περιλαμβάνει την προετοιμασία των συσκευών από τους χρήστες με την εγκατάσταση του προγράμματος PROFIT και την αποδοχή ή όχι των όρων χρήσεως και επεξεργασίας. Στο στάδιο αυτό μπορούν να μην εγκαταστήσουν το πρόγραμμα αλλά η εγκατάσταση αυτού διευκολύνει την όλη διαδικασία καθώς και την προστασία των προσωπικών τους δεδομένων.

β) Preparation: Κατά τον εν λόγω στάδιο ο ψηφιακός ερευνητής αναλύει το νομικό πλαίσιο κάτω από το οποίο θα εκτελέσει την έρευνα, προετοιμάζει τα εργαλεία επεξεργασίας των συλλεχθέντων πληροφοριών και ελέγχει εάν απαιτείται η έκδοση ενταλμάτων έρευνας (σε περίπτωση μη συνεργάσιμων χρηστών).

γ) Context-based collection: Περιλαμβάνει την διαδικασία συλλογής των δεδομένων από τις συσκευές και την αναζήτηση συσχετίσεων μεταξύ τους αναφορικά με την υπό εξέταση υπόθεση (δημιουργία chains of custody).

δ) Data analysis and correlation: Κατά το εν λόγω στάδιο τα συλλεχθέντα δεδομένα αναλύονται και συσχετίζονται μεταξύ τους.

ε) Information sharing: Στο στάδιο αυτό ανταλλάσσονται πληροφορίες με έτερους οργανισμούς αναφορικά με την υπό εξέταση υπόθεση.

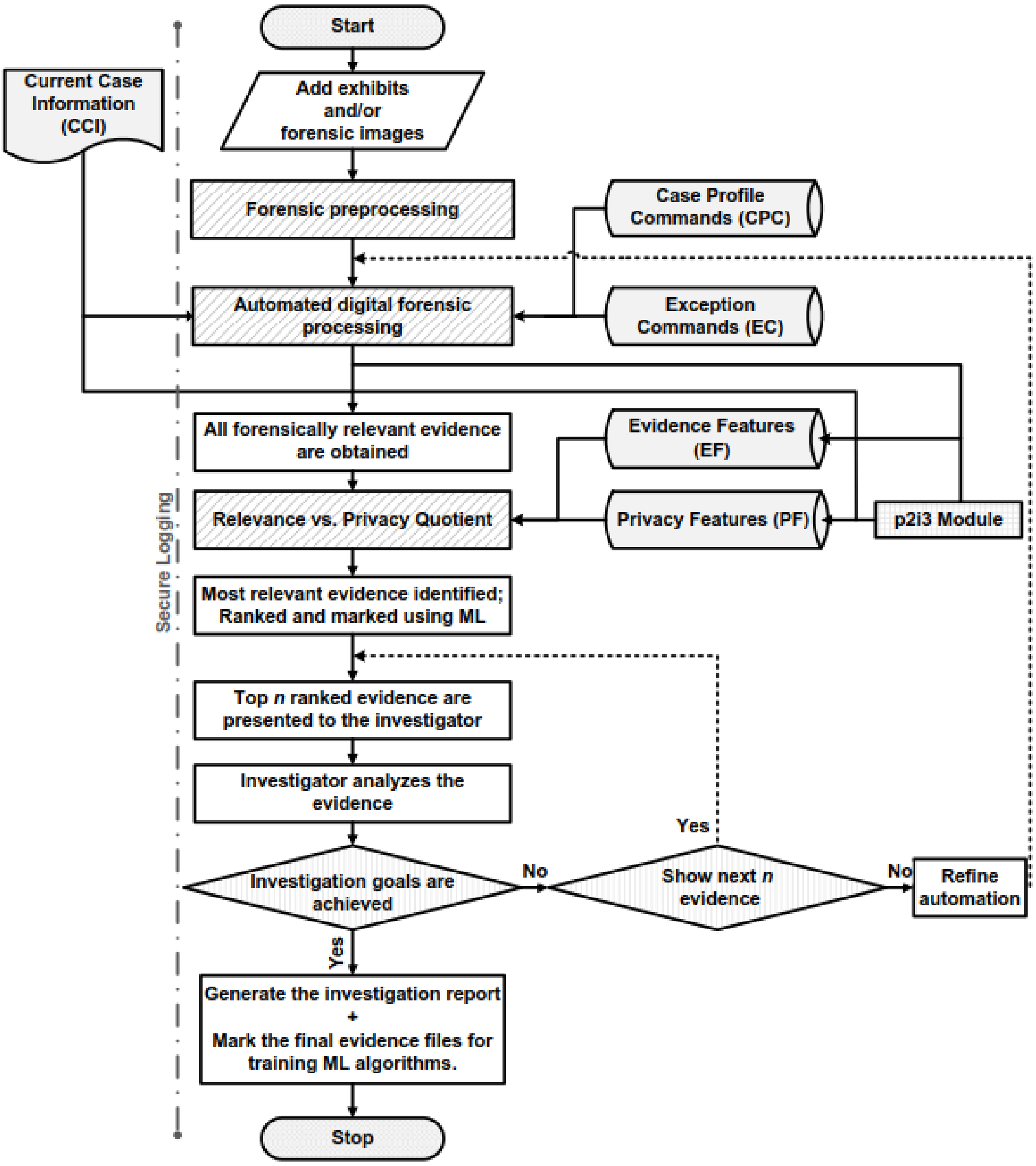
στ) Presentation: Κατά τον εν λόγω στάδιο τα αποτελέσματα της έρευνας παρουσιάζονται στις αρχές και ελέγχεται η εγκυρότητά τους σε σχέση με την εξεταζόμενη υπόθεση.

ζ) Review: Κατά τον εν λόγω στάδιο γίνεται έλεγχος της συνολικής ακολουθείσας διαδικασίας και καταστρέφονται όλα τα συλλεχθέντα δεδομένα ενημερώνοντας παράλληλα τους κατόχους τους για τη μόνιμη διαγραφή τους.

Το πρόγραμμα PROFIT συμβάλλει στην προστασία της ιδιωτικότητας των χρηστών καθώς κατά το στάδιο της προετοιμασίας όπου το πρόγραμμα εγκαθίσταται στις συσκευές οι χρήστες μπορούν να συμφωνήσουν ή όχι με τους όρους χρήσης και συλλογής δεδομένων και το πρόγραμμα ακολούθως θα συλλέξει δεδομένα ανάλογα με τις επιλογές τους. Επιπρόσθετα, οι χρήστες έχουν τη δυνατότητα να ελέγχουν τα δεδομένα που συλλέγονται από το PROFIT καθώς και να επιλέξουν εάν θα συνεργαστούν για τη συλλογή τους ή θα απαιτηθεί έκδοση εντάλματος έρευνας. Κατά το στάδιο της συλλογής των δεδομένων από τον ψηφιακό ερευνητή συλλέγονται από τις συσκευές τα απαραίτητα για την υπόθεση δεδομένα με το πρόγραμμα να ελέγχει τα requests του ψηφιακού ερευνητή ως προς την τήρηση αυτής της αρχής. Κατά το στάδιο analysis and correlation τα δεδομένα προστατεύονται από αυθαίρετη επεξεργασία ή πρόσβαση σε αυτά. Κατά το στάδιο Information sharing όπου ενδέχεται να απαιτηθεί να αποκτήσουν πρόσβαση στα δεδομένα έτεροι οργανισμοί το PROFIT θα ζητήσει την άδεια από τους χρήστες για αυτή την επιπρόσθετη πρόσβαση και επεξεργασία. Τέλος, πρέπει να αναφερθεί ότι οι χρήστες έχουν την επιλογή της διατήρησης της υπό εξέτασης συσκευής στην κατοχή τους καθόλη τη διάρκεια της έρευνας με την προϋπόθεση ότι έχουν αυτοβούλως συμμετάσχει στην εν λόγω έρευνα.

Στις προηγούμενες παραγράφους έγινε λόγος για τα PETs και τους τρόπους που αυτά προστατεύουν την ιδιωτικότητα των χρηστών. Ωστόσο, τα PETs θα πρέπει να παρέχουν και τη δυνατότητα να αποκαλύπτουν τα στοιχεία των χρηστών όταν αυτοί αποκαλυφθούν ότι διαπράττουν κάποια αξιόποινη πράξη. [68] Αυτό καθίσταται εφικτό με τη χρήση του πρωτοκόλλου PPINA (Protect Private Information, Not Abuser) το οποίο λειτουργεί ως πρόσθετο στα υφιστάμενα PETs και επιτρέπει να παραμείνουν οι χρήστες ανώνυμοι κατά τη χρήση του δικτύου έως ότου υπάρχουν αποδείξεις ότι κάποιος χρήστης εκτελεί κάποιου είδους επίθεση στον server ώστε να μπορεί ο ψηφιακός ερευνητής να ζητήσει την αποκάλυψη της ταυτότητας του επιτιθέμενου. [44] Για την υλοποίηση του εν λόγω πρωτοκόλλου χρησιμοποιούνται τεχνικές ψηφιακής υπογραφής και κρυπτογράφησης δημοσίου κλειδιού ενώ είναι απαραίτητη και η ύπαρξη μίας ανεξάρτητης οντότητας (του Directory Service το οποίο αναλαμβάνει το ρόλο και του Forensic Investigation Entity, FIE) όπου εάν ο server αντιληφθεί μία συγκεκριμένη ροή ως κακόβουλη θα αποστείλει τα στοιχεία της στο FIE και αυτό, κατόπιν επιβεβαίωσης της εν λόγω ροής ως κακόβουλης θα επιστρέψει στον server τα στοιχεία του χρήστη στον οποίο ανήκει η εν λόγω ροή. Ένα έτερο πρωτόκολλο για εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία προσωπικών δεδομένων είναι το investigative Data Acquisition Platform (IDAP) [69] το οποίο χρησιμοποιώντας μία semi-trusted τρίτη οντότητα (proxy) προστατεύει την ιδιωτικότητα τρίτων ως προς την υπόθεση ατόμων καθώς μόνο τα σχετικά με την υπόθεση δεδομένα συλλέγονται, ο data holder και ο proxy μπορούν να συνεργαστούν εάν παραστεί ανάγκη να εξακριβωθεί η έρευνα του ψηφιακού ερευνητή στο δικαστήριο και η πιθανότητα αυτός να συλλέξει δεδομένα τρίτου ως προς την υπόθεση ατόμου είναι μικρή. Ο Proxy δρα ως εξής: α) όλη η επικοινωνία μεταξύ του data holder και του ψηφιακού ερευνητή διέρχεται από τον proxy β) ο ψηφιακός ερευνητής παρέχει στον proxy αναγνωριστικές πληροφορίες για το είδος των επιθυμητών προς συλλογή δεδομένων και γ) ο proxy με βάση τις αναγνωριστικές πληροφορίες που έλαβε από τον ψηφιακό ερευνητή απορρίπτει τα δεδομένα που έλαβε από τον data holder και που δεν σχετίζονται με τις εν λόγω πληροφορίες. Αυτά έχουν ως αποτέλεσμα να ενισχύεται η χρήση των PETs στη ψηφιακή αναζήτηση πειστηρίων με γνώμονα την ιδιωτικότητα των χρηστών.

Ένας έτερος τρόπος για να εκτελεστεί ψηφιακή δικανική έρευνα με έμφαση στην προστασία προσωπικών δεδομένων σε ένα σύνολο συλλεχθέντων δεδομένων είναι με τη χρήση του πρωτοκόλλου DF 2.0 το οποίο χρησιμοποιεί τεχνικές machine learning και έχοντας ως οδηγό τις πληροφορίες για τη συγκεκριμένη υπόθεση που εισάγονται από τον ψηφιακό ερευνητή (αρχείο Current Case Information, CCI).[70] Ο τρόπος επεξεργασίας των δεδομένων από το πρωτόκολλο DF 2.0 φαίνεται στο ακόλουθο διάγραμμα:



Διάγραμμα 2: Πρωτόκολλο DF 2.0

Βάσει του ανωτέρω διαγράμματος λειτουργίας του πρωτοκόλλου DF 2.0 τα δεδομένα, αφού υποστούν επεξεργασία στο στάδιο «Automated Digital Forensic Processing» χωρίζονται σε δύο κατηγορίες, στα δεδομένα που είναι σχετικά με την υπόθεση (Forensically Relevant Files, FRF) και στα δεδομένα που δεν σχετίζονται με αυτή (Forensically Irrelevant Files, FIF). Τα FIF καθίστανται αμέσως μη προσβάσιμα στον ψηφιακό ερευνητή ενώ τα FRF προχωρούν στο επόμενο στάδιο επεξεργασίας. Αυτό κατά τους δημιουργούς του εν λόγω πρωτοκόλλου είναι το πρώτο στάδιο προστασίας της ιδιωτικότητας κατά την ψηφιακή δικανική ανάλυση των δεδομένων. Ακολούθως, στο στάδιο «Relevance vs Privacy Quotient» τα δεδομένα με τη χρήση machine learning ταξινομούνται σε φθίνουσα σειρά ανάλογα με το βαθμό σχετικότητάς τους με την εξεταζόμενη υπόθεση ενώ παράλληλα κατηγοριοποιούνται και με βάση εάν περιέχουν προσωπικά δεδομένα και το είδος αυτών (κατηγορίες PF:Private File, NPF:Non-Private File, PCF: Personally-Identifiable-Information (PII) Containing File). Ακολούθως στον ψηφιακό ερευνητή παρουσιάζεται η πρώτη ομάδα με τα πιο σχετικά με την υπόθεση δεδομένα (μαζί με τον χαρακτηρισμό τους ως προς την ιδιωτικότητα) προς διερεύνηση. Η επόμενη ομάδα δεν παρουσιάζεται μέχρι να αναλυθούν τα δεδομένα της πρώτης ομάδας και ο ψηφιακός ερευνητής κρίνει ότι απαιτείται διερεύνηση περαιτέρω στοιχείων. Αυτό το στάδιο κατά τους δημιουργούς του πρωτοκόλλου είναι το δεύτερο στάδιο προστασίας της ιδιωτικότητας κατά την ψηφιακή δικανική ανάλυση των δεδομένων καθώς περιορίζονται τα δεδομένα που ελέγχονται από τον ψηφιακό ερευνητή στα πιο σχετικά με την εξεταζόμενη υπόθεση και το εύρος μίας πιθανής παραβίασης αυτών μπορεί να προβλεφθεί λόγω του χαρακτηρισμού κάθε δεδομένου ως περιέχον προσωπικά ή όχι στοιχεία. Τέλος, η δραστηριότητα του ψηφιακού ερευνητή καταγράφεται σε log αρχεία στα οποία δεν έχει πρόσβαση με σκοπό την μετέπειτα διερεύνηση εάν υπάρχει καταπάτηση της ιδιωτικότητας των χρηστών και εξακρίβωση του εύρους αυτής.

Ένας έτερος τρόπος για να εκτελεστεί ψηφιακή δικανική έρευνα με έμφαση στην προστασία προσωπικών δεδομένων είναι η προστασία των δεδομένων από τον ψηφιακό ερευνητή στο πλαίσιο μίας ακούσιας έκθεσή του σε προσωπικά δεδομένα με την κατηγοριοποίηση αρχικά των προς συλλογή δεδομένων ανάλογα με τον βαθμό που αυτά περιέχουν προσωπικά στοιχεία [44]. Ακολούθως, οι ομάδες πλέον αυτών των δεδομένων θα κρυπτογραφηθούν και θα παρουσιαστούν στον ψηφιακό ερευνητή με αύξουσα σειρά περιεχομένου σε προσωπικά δεδομένα. Για να αποκτήσει ο ψηφιακός ερευνητής πρόσβαση στην επόμενη ομάδα δεδομένων πρέπει να αποδείξει ότι κατέχει επαρκείς πληροφορίες που συσχετίζονται με το περιεχόμενο της αμέσως προηγούμενης ομάδας (εξασφαλίζεται με τη χρήση τεχνικών hashing και XOR) με αποτέλεσμα να προστατεύονται οι πληροφορίες των ανώτερων επιπέδων που περιέχουν προσωπικά δεδομένα (στην περίπτωση που ο ψηφιακός ερευνητής δεν γνωρίζει επαρκείς πληροφορίες για την παρούσα ομάδα δεδομένων που ερευνά δεν είναι δυνατή η “αποκρυπτογράφηση” του κλειδιού του κρυπτογραφημένου επόμενου επιπέδου). Τέλος, η εν λόγω μεθοδολογία διασφαλίζει την προστασία της διαδικασίας από επιθέσεις brute force για την ανεύρεση του κλειδιού κρυπτογράφησης κάθε ομάδας δεδομένων με τη χρήση ψηφιακής υπογραφής και μίας Signing Authority, περιορίζοντας με αυτόν τον τρόπο τον αριθμό αιτήσεων πρόσβασης σε ανώτερο επίπεδο που μπορεί να ζητήσει ο ψηφιακός ερευνητής. [71]

Ένας έτερος τρόπος για να εκτελεστεί ψηφιακή δικανική έρευνα με έμφαση στην προστασία προσωπικών δεδομένων είναι η έρευνα ενός κρυπτογραφημένου αρχείου δεδομένων με τη χρήση λέξεων-κλειδιών. Κατά την εν λόγω τεχνική ο data owner εκτελεί κατηγοριοποίηση των εν λόγω δεδομένων με βάση κάποιες λέξεις-κλειδιά και έπειτα κρυπτογραφεί τα εν λόγω δεδομένα. Έπειτα, ο ψηφιακός ερευνητής ετοιμάζει μία λίστα με λέξεις-κλειδιά που σχετίζονται με την υπό εξέταση υπόθεση και ο data owner του παραδίδει το κλειδί αποκρυπτογράφησης των δεδομένων το οποίο σχετίζεται με τις δικές του λέξεις-κλειδιά. Ο ψηφιακός ερευνητής μπορεί να αποκρυπτογραφήσει και να αναλύσει τα αρχεία των οποίων οι λέξεις-κλειδιά ταυτίζονται με αυτές που ο ίδιος έχει ορίσει. Με αυτόν τον τρόπο, κρυπτογραφημένα τμήματα των δεδομένων που δεν σχετίζονται με τις λέξεις-κλειδιά που έχει ορίσει ο ψηφιακός ερευνητής δεν μπορούν να αποκρυπτογραφηθούν και να αναλυθούν από αυτόν με αποτέλεσμα να προστατεύεται η ιδιωτικότητα του κατόχου τους. [1] Στο [72] προτείνεται μία παραλλαγή της μεθόδου keyword search για δεδομένα που βρίσκονται σε κάποιον server με τη χρήση τεχνικών homomorphic και commutative encryption. Κατά την εν λόγω μέθοδο ο server administrator κρυπτογραφεί το σύνολο των δεδομένων και ο ψηφιακός ερευνητής του αποστέλλει κρυπτογραφημένο ένα σύνολο από keywords (με σκοπό ο server administrator να μην μάθει το αντικείμενο της έρευνας) καθώς και έναν τρόπο (μέσω trapdoor) όπου μπορεί να συσχετίσει το περιεχόμενο του αρχείου των keywords με τα κρυπτογραφημένα του δεδομένα. Ακολούθως, ο server administrator επιστρέφει στον ψηφιακό ερευνητή κρυπτογραφημένα τα δεδομένα που αντιστοιχούν στις λέξεις-κλειδιά που έδωσε χωρίς να έχει πρόσβαση στα υπόλοιπα δεδομένα. Με αυτόν τον τρόπο περιορίζεται η πρόσβαση του ψηφιακού ερευνητή στα απαραίτητα μόνο για την υπόθεση δεδομένα προστατεύοντας την ιδιωτικότητα των κατόχων των δεδομένων που δεν έχουν σχέση με την υπόθεση αυτή.

Τέλος, ένα έτερο πρωτόκολλο που μπορεί να χρησιμοποιηθεί για την εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία προσωπικών δεδομένων είναι το PPEDFI (Privacy Preserving Efficient Digital Forensic Investigation Framework) [73] το οποίο δέχεται ως τιμές εισόδου στοιχεία από τον ψηφιακό ερευνητή όπως στοιχεία των υπόπτων και πληροφορίες για την υπόθεση όπως επίσης και πληροφορίες για την έκβαση παρελθοντικών υποθέσεων ώστε να μειωθούν οι χρόνοι επεξεργασίας των δεδομένων και να παρουσιασθούν για τελική ανάλυση δεδομένα σχετικά μόνο με την εν λόγω υπόθεση. Ακολούθως, εκτελεί επεξεργασία στα συλλεχθέντα δεδομένα και επιστρέφει στον ψηφιακό ερευνητή ένα ποσοστό από τα εν λόγω δεδομένα το οποίο ανταποκρίνεται στις προαναφερθείσες τιμές εισόδου. Στη συνέχεια, τα δεδομένα εξόδου του πρωτοκόλλου κατατάσσονται σε φθίνουσα σειρά σχετικότητας με την υπό εξέταση υπόθεση με σκοπό να αναλυθούν από τον ψηφιακό ερευνητή μόνο τα δεδομένα που σχετίζονται με αυτή, με αποτέλεσμα να προστατεύεται τόσο η ιδιωτικότητα των κατόχων δεδομένων τρίτων ως προς την εξεταζόμενη υπόθεση όσο και η ιδιωτικότητα των υπόπτων της υπό εξέταση υπόθεσης.

Κεφάλαιο 4

4.1. Εισαγωγή

Η δικανική των δικτύων (Network Forensics) αποτελεί τμήμα της ψηφιακής δικανικής έρευνας και έχει ως στόχο «την ιχνηλάτηση, καταγραφή και ανάλυση δικτυακών συμβάντων με σκοπό τον εντοπισμό πηγών κακόβουλων επιθέσεων και άλλων προβλημάτων» [20]. Τα Network Forensics αποτελούν συνήθως post mortem έρευνα μιας επίθεσης και ενεργοποιούνται αφού έχει λάβει χώρα η εν λόγω επίθεση (notitia criminis-after crime notification). Είναι μία χρονικά περιορισμένη έρευνα με σκοπό και περιεχόμενο άμεσα σχετιζόμενο με τη δικτυακή επίθεση που έλαβε χώρα. [74]

Κατά τη διάρκεια των Network Forensics γίνεται πλήρης καταγραφή της δραστηριότητας του δικτύου (e-mail, Instant Messaging (I.M.) επικοινωνία, δραστηριότητα σε web browsers, μεταφορές αρχείων κτλ) καθώς το ενθυλακωμένο περιεχόμενο των frames αποθηκεύεται μαζί με όλη τη καταγραφείσα δικτυακή ροή [21]

Η ιχνηλάτηση, καταγραφή και ανάλυση των ανωτέρω συμβάντων συνήθως απαιτεί άριστη γνώση των δικτυακών τεχνολογιών (για παράδειγμα γνώση του τρόπου λειτουργίας- επικοινωνίας των πρωτοκόλλων στα επίπεδα 2 και 3 του OSI) [75] κάνοντας απαραίτητη την ύπαρξη εργαλείων και προγραμμάτων που διευκολύνουν τις ανωτέρω εργασίες [76] [77]. Τα εν λόγω εργαλεία υποστηρίζουν το έργο του ψηφιακού ερευνητή με το να συνοψίζουν και να ομαδοποιούν τα συλλεγμένα δεδομένα καθώς και να επισημαίνουν επεξεργασμένα ή ακατέργαστα στοιχεία που μπορεί να βοηθήσουν στα Network Forensics [78] (για παράδειγμα παρουσίαση συνημμένων αρχείων, μεταδιδόμενων μηνυμάτων, διαπιστευτηρίων κ.α. σε κατανοητή από τον άνθρωπο μορφή).

Τόσο τα συλλεγμένα στοιχεία όσο και τα αποτελέσματα των Network Forensics πρέπει να διέπονται από τις ακόλουθες πέντε αρχές [79]:

Παραδεκτά: Πρέπει να μπορούν να χρησιμοποιηθούν στο δικαστήριο ή οπουδήποτε απαιτηθεί.

Γνήσια: Πρέπει να βρίσκονται σε άμεση συσχέτιση με το συμβάν.

Πλήρεις: Πρέπει να αποτελούν ενοχοποιητικά στοιχεία για τη συγκεκριμένη υπόθεση.

Αξιόπιστα: Δεν υπάρχουν αμφιβολίες για την αυθεντικότητα και τη γνησιότητά τους.

Πειστικά: Πρέπει να μπορούν να χρησιμοποιηθούν ως αξιόπιστα δεδομένα στο δικαστήριο.

Τα Network Forensics με γνώμονα ορισμένα κοινά χαρακτηριστικά τους διακρίνονται γενικά στις ακόλουθες κατηγορίες:

α) Σκοπός

Ως προς τον σκοπό της έρευνας τα Network Forensics κατατάσσονται σε “General Network Forensics” τα οποία αποσκοπούν γενικά στην προστασία του δικτύου και στην βελτίωση της ασφάλειάς του και στα “Strict Network Forensics” τα οποία αποσκοπούν στη συλλογή στοιχείων στο πλαίσιο ικανοποίησης νομικών υποχρεώσεων και οδηγιών [80].

β) Συλλογή της ροής των δεδομένων

Ως προς τον τρόπο συλλογής της ροής των δεδομένων τα Network Forensics κατατάσσονται σε “Catch-it-as-you-can” όπου γίνεται ανάλυση μεγάλου όγκου πακέτων τα οποία διέρχονται από συγκεκριμένο σημείο συλλογής στο δίκτυο και “Stop-look-and-listen” όπου κάθε πακέτο αναλύεται ξεχωριστά και οι πληροφορίες αποθηκεύονται για μελλοντική χρήση [81].

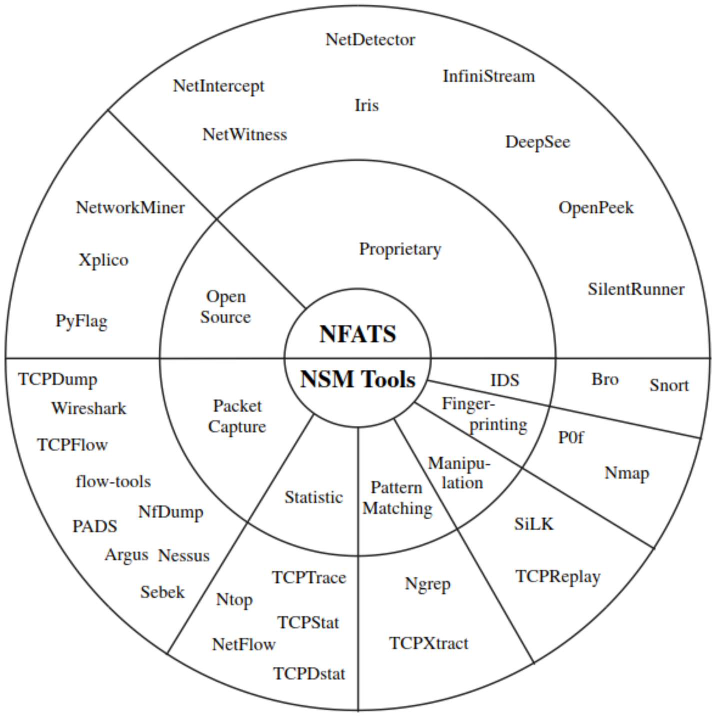
Γ) Υποδομή

Ως προς την υποδομή τους τα Network Forensics διακρίνονται σε “hardware-based with pre-installed software” και σε “exclusively software tools”.

4.2. Network Forensic Analysis Tools (NFATS)

Τα εργαλεία NFATs που αναφέρθηκαν συνοπτικά στην εισαγωγή επιτρέπουν στον διαχειριστή του συστήματος να παρακολουθεί την ροή των δεδομένων στο δίκτυο, να συλλέγει πληροφορίες για μη αναμενόμενες ροές δεδομένων (anomalous traffic), να συνδράμει τον ψηφιακό ερευνητή στη συλλογή στοιχείων κατά τα Network Forensics και στην αντιμετώπιση ενός δικτυακού συμβάντος (incident response) [82].

Τα NFATs καταγράφουν όλη τη δικτυακή ροή και επιτρέπουν στον ψηφιακό ερευνητή την εξαγωγή στοιχείων βασισμένων στην ομαδοποίηση των κοινών χαρακτηριστικών των συλλεγμένων δεδομένων. Τα NFATs συνεργάζονται με τα Firewalls και τα Intrusion Detection Systems (IDS) για τη συλλογή δεδομένων τα οποία διατηρούν για μεγάλα χρονικά διαστήματα επιτρέποντας τη διεξαγωγή αποτελεσματικότερων incident responses και γρήγορων αναλύσεων. Η καταγραφείσα κακόβουλη ροή δεδομένων μπορεί να χρησιμοποιηθεί στην εκτέλεση προσομοιώσεων με σκοπό την ανεύρεση των συνθηκών κάτω από τις οποίες εκτελέστηκε η επίθεση και ενοχοποιητικών στοιχείων που θα υποδεικνύουν ένα συγκεκριμένο δράστη [83]. Στον αντίποδα, υπάρχουν λογισμικά ανοικτού κώδικα τα οποία παρέχουν υπηρεσίες ασφάλειας του δικτύου (Network Security and Monitoring Tools) τα οποία διευκολύνουν τη διαδικασία των Network Forensics αλλά τα παρεχόμενα από αυτά στοιχεία δεν έχουν αυτοτελώς νομική υπόσταση στο δικαστήριο. Στην εικόνα που ακολουθεί δίνεται μία σχηματική απεικόνιση ανά κατηγορία των γνωστότερων NFATs και NSMs:



Εικ.1: Κατηγοριοποίηση NFATs και NSMs

Τα βασικά χαρακτηριστικά που πρέπει να έχουν τα NFATs είναι τα ακόλουθα [84]:

α) Ικανότητα επεξεργασίας μεγάλου όγκου δεδομένων.

β) Ικανότητα εξαγωγής οποιασδήποτε απαραίτητης πληροφορίας από τα συλλεγμένα δεδομένα της δικτυακής κίνησης.

γ) Ικανότητα επιβεβαίωσης-επαλήθευσης των εξαχθέντων αποτελεσμάτων.

δ) Ικανότητα επεξεργασίας και εξαγωγής αποτελεσμάτων από μη ολοκληρωμένες ροές δεδομένων.

ε) Ικανότητα De-capsulation τμηματοποιημένων πακέτων δεδομένων (μέσω IP fragmentation ή data stream multiplexing).

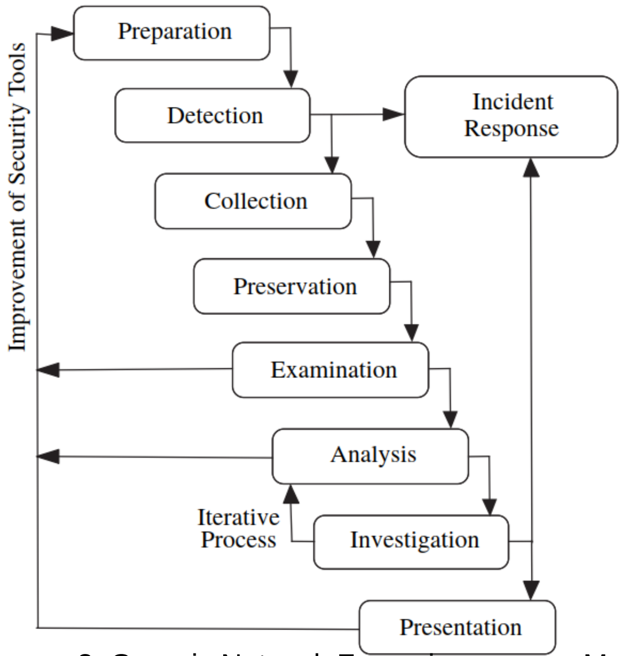
στ) Ικανότητα ανάλυσης της καταγραφείσας δικτυακής ροής της οποίας τα πακέτα έχουν γίνει encapsulated με χρήση κάποια τεχνικής tunneling (λχ. VPN).

ζ) Ικανότητα εντοπισμού των encapsulated layer 7 εφαρμογών και των αντίστοιχων χρησιμοποιούμενων πορτών.

η) Παροχή user friendly interface για την ευκολία συλλογής στοιχείων κατά τα Network Forensics.

4.3. Network Forensics process Model

Λαμβάνοντας υπόψη τα υφιστάμενα μοντέλα για Network Forensics προτείνεται η διεξαγωγή των Network Forensics βάσει της ακόλουθης γενικής διαδικασίας:



Διάγραμμα 3: Generic Network Forensics process Model

Κατά την **προετοιμασία** για την υλοποίηση του ανωτέρω μοντέλου τα NFATs τοποθετούνται σε στρατηγικά σημεία στο δίκτυο για τη συλλογή των δεδομένων (ανάλογα με τον τρόπο λειτουργίας τους).

Κατά το στάδιο του **εντοπισμού** της επίθεσης γίνεται παρακολούθηση του δικτύου για εντοπισμό μη συνηθισμένων ροών δεδομένων και συμβάντων.

Κατά τη **διερεύνηση** των εντοπισμένων συμβάντων γίνεται διαχωρισμός των false positive με τα false negative συμβάντα και γίνεται προσπάθεια να μην αλλοιωθούν τα συλλεγμένα δεδομένα από την εν λόγω διαδικασία.

Κατά το στάδιο του **Incident Response** ο οργανισμός ή η εταιρεία ανάλογα με το βαθμό και το είδος της επίθεσης αναλαμβάνει διαδικασίες για να την αντιμετωπίσει βάσει των πολιτικών που έχει θεσπίσει. Το σχέδιο δράσης που θα αναπτύξει θα καθορίσει επιπρόσθετα εάν θα συνεχιστεί η συλλογή στοιχείων για την εν λόγω επίθεση.

Κατά το στάδιο της **συλλογής των στοιχείων** ακολουθούνται συγκεκριμένες διαδικασίες κατά τις οποίες μέσω του συνδυασμού hardware-software συλλέγονται όσο το δυνατόν περισσότερα δεδομένα με όσο το δυνατόν μικρότερο αντίκτυπο στη φυσιολογική λειτουργία του δικτύου.

Κατά το στάδιο της **διατήρησης των δεδομένων** αυτά διατηρούνται σε αποθηκευτικό μέσο με read-only δικαιώματα και έχουν ληφθεί οι hash τιμές τους. Η επεξεργασία στο πλαίσιο διενέργειας των Network Forensics γίνεται σε αντίγραφο αυτών με σκοπό τα αποτελέσματα της έρευνας να μπορούν να επαληθευτούν εάν ακολουθηθεί η ίδια μεθοδολογία στα αρχικά δεδομένα.

Κατά το στάδιο του **ελέγχου** ομαδοποιούνται τα συλλεγμένα δεδομένα, επιλύονται αντιφατικές ή ανακριβείς πληροφορίες όπως αντικρουόμενες χρονοσφραγίδες και ακολούθως εξάγονται ενοχοποιητικά στοιχεία για το υπό διερεύνηση συμβάν.

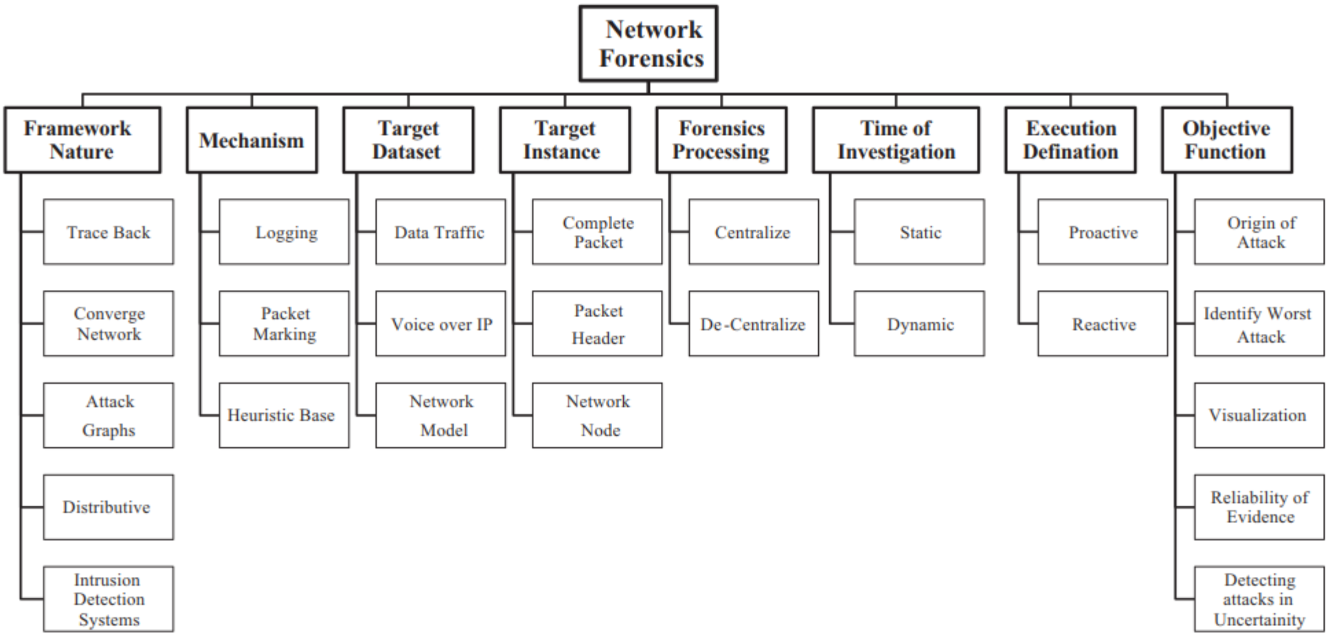
Κατά το στάδιο της **ανάλυσης** τα ενοχοποιητικά στοιχεία ομαδοποιούνται και εξετάζονται με σκοπό να εξακριβωθούν τα αίτια της επίθεσης.

Κατά το στάδιο της **δικανικής έρευνας** χρησιμοποιούνται τα εξαχθέντα δεδομένα από το στάδιο της ανάλυσης για τον εντοπισμό της διαδρομής επίθεσης, την πηγή αυτής και όλους τους ενδιάμεσους κόμβους καθώς και για την τελική απόδοση ευθυνών.

Τέλος, κατά το στάδιο της **παρουσίασης** παρατίθενται με απλούς τεχνικούς όρους σε νομικούς φορείς τα αποτελέσματα της έρευνας και στοιχειοθετείται με πλήρη έγγραφη τεκμηρίωση η απόδοση ευθυνών σε συγκεκριμένα πρόσωπα.

4.4. Network Forensic Technics

Στην παρούσα ενότητα θα γίνει λόγος για την γενική κατηγοριοποίηση των τεχνικών με τις οποίες υλοποιούνται τα Network Forensics (Network Forensic Technics-NFT). Οι τεχνικές αυτές κατηγοριοποιούνται με γνώμονα συγκεκριμένες παραμέτρους βάσει των οποίων παρουσιάζουν συγκεκριμένα κοινά γνωρίσματα:



Εικ.2: Κατηγοριοποίηση των τεχνικών για Network Forensics

Η παράμετρος **Framework Nature** πραγματεύεται τον κύριο μηχανισμό με τον οποίο λειτουργούν τα NFT (Trace Back, IDS, Distributive κτλ).

Η παράμετρος **Mechanism** δείχνει την μέθοδο με την οποία τα NFT εκτελούν ψηφιακή δικανική ανάλυση σε αρχεία log, πακέτα και δικτυακά συμβάντα.

Η παράμετρος **Target Dataset** πραγματεύεται το είδος της ροής δεδομένων στην οποία θα εκτελεστούν Network Forensics.

Η παράμετρος **Target Instance** περιγράφει το είδος των δεδομένων που συλλέγονται ώστε να χρησιμοποιηθούν μετέπειτα για Network Forensics Investigation.

Η παράμετρος **Forensic Processing** περιγράφει εάν η δικανική έρευνα θα γίνει centralized ή decentralized.

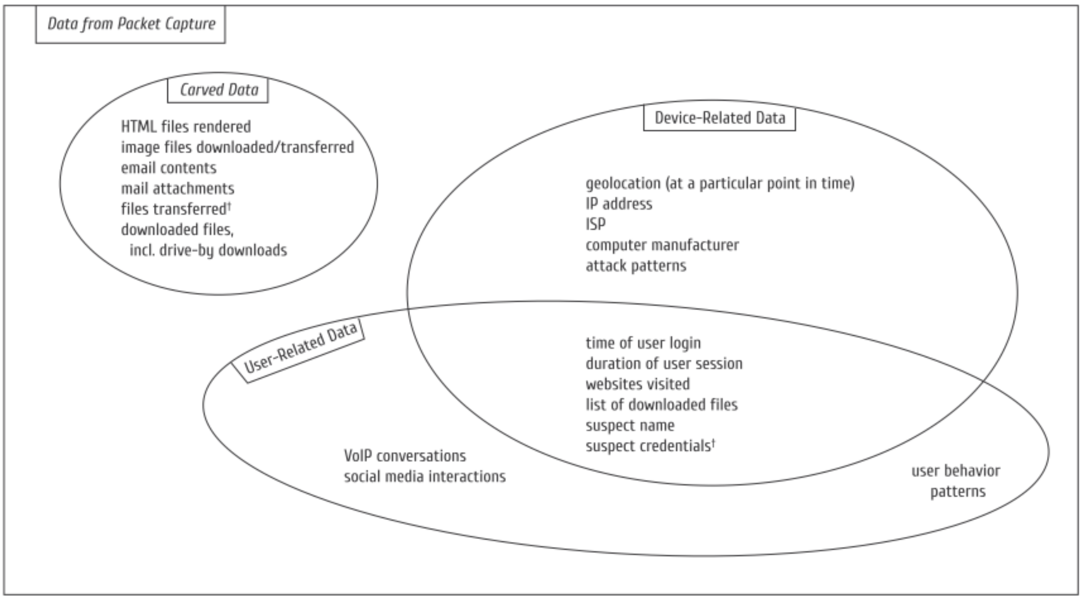
Η παράμετρος **Time of investigation** περιγράφει εάν η ανάλυση θα γίνει σε back up συλλεγμένα δεδομένα (static) ή σε δεδομένα που θα λαμβάνονται και θα αναλύονται ενώ το υπό εξέταση σύστημα συνεχίζει να δουλεύει.

Η παράμετρος **Execution Definition** περιγράφει τον τρόπο δράσης του NFT (proactive ή reactive).

Η παράμετρος **Objective Function** περιγράφει το σκοπό που θέλει να επιτύχει το NFT (για παράδειγμα να ανακατασκευάσει την επίθεση, να εντοπίσει την πηγή αυτής κ.α.)

4.5. Privacy issues in Network Forensics

Στις προηγούμενες παραγράφους έγινε λόγος για τις υφιστάμενες τεχνικές, τα διαθέσιμα προγράμματα και τη διαδικασία με την οποία εκτελούνται τα Network Forensics. Κατέστη επιπλέον σαφές ότι για την εκτέλεση της ψηφιακής δικανικής ανάλυσης στα δίκτυα είναι απαραίτητη η συλλογή όλων των πακέτων της δικτυακής ροής του υπό εξέταση συστήματος καθώς η διεύθυνση IP, από μόνη της, δεν αποτελεί στοιχείο λόγω του δυναμικού χαρακτήρα της και συνήθως λόγω της αδυναμίας να συσχετιστεί άμεσα με κάποιο φυσικό πρόσωπο [91] ή ακόμα και μία γεωγραφική θέση [92]. Από τα εν λόγω πακέτα μπορούν να συλλεχθούν αξιόπιστα υποστηρικτικά στοιχεία με την ανακατασκευή των αποθηκευμένων σε αυτά metadata, αρχείων και μηνυμάτων [85] και μέσω της ανάλυσης των κοινών στοιχείων των ροών δεδομένων που απαντώνται σε γνωστές δικτυακές επιθέσεις (SYN flood attack, XMAS scan, SYN/FIN attack) [86]. Επιπρόσθετα, αξιοποιούνται log αρχεία από IDS, firewalls, packet sniffers και NFATs [87] καθώς και authentication logs και routing tables από τους routers που παρεμβάλλονται στην καταγραφείσα δικτυακή ροή [88]. Συνοπτικά, τα συλλεγμένα στοιχεία κατά τη διαδικασία των Network Forensics φαίνονται στην ακόλουθη εικόνα:



Εικ.3: Συλλεγμένα δεδομένα κατά τη διαδικασία Network Forensics

Ωστόσο, από τις προηγούμενες παραγράφους γίνεται κατανοητό ότι η απόκτηση όλης της δικτυακής ροής των δεδομένων εγκυμονεί τον κίνδυνο να παραβιαστεί η ιδιωτικότητα όλων των χρηστών του εν λόγω δικτύου [89]. Κατά τη ψηφιακή δικανική ανάλυση των δικτύων είναι πιθανή η περίπτωση ο network administrator να πρέπει να παραδώσει την δικτυακή ροή που έχει συλλέξει στον ψηφιακό ερευνητή ως υλικό προς διερεύνηση. Το εν λόγω υλικό στις περισσότερες περιπτώσεις περιέχει και δεδομένα ατόμων που δεν έχουν σχέση με την εξεταζόμενη υπόθεση. Τα προαναφερθέντα στις προηγούμενες παραγράφους NFAT προγράμματα έχουν την δυνατότητα να αποθηκεύουν και να αναπαράγουν τα εν λόγω στοιχεία και επομένως να παραβιάζουν διπλά την ιδιωτικότητα των ατόμων. Επιπρόσθετα, η εναρμόνιση της λειτουργίας των εταιρειών με την εκάστοτε νομοθεσία ενίοτε απαιτεί την καταγραφή της δικτυακής ροής για ένα ορισμένο χρονικό διάστημα (σε οργανισμούς όπως ISPs, πανεπιστήμια, ιδιωτικές εταιρείες). Η αξιοποίηση των εν λόγω αρχείων κατά τη ψηφιακή δικανική ανάλυση των δικτύων είναι δυνατό να εκθέσει τα προσωπικά δεδομένα των χρηστών των εν λόγω δικτύων.

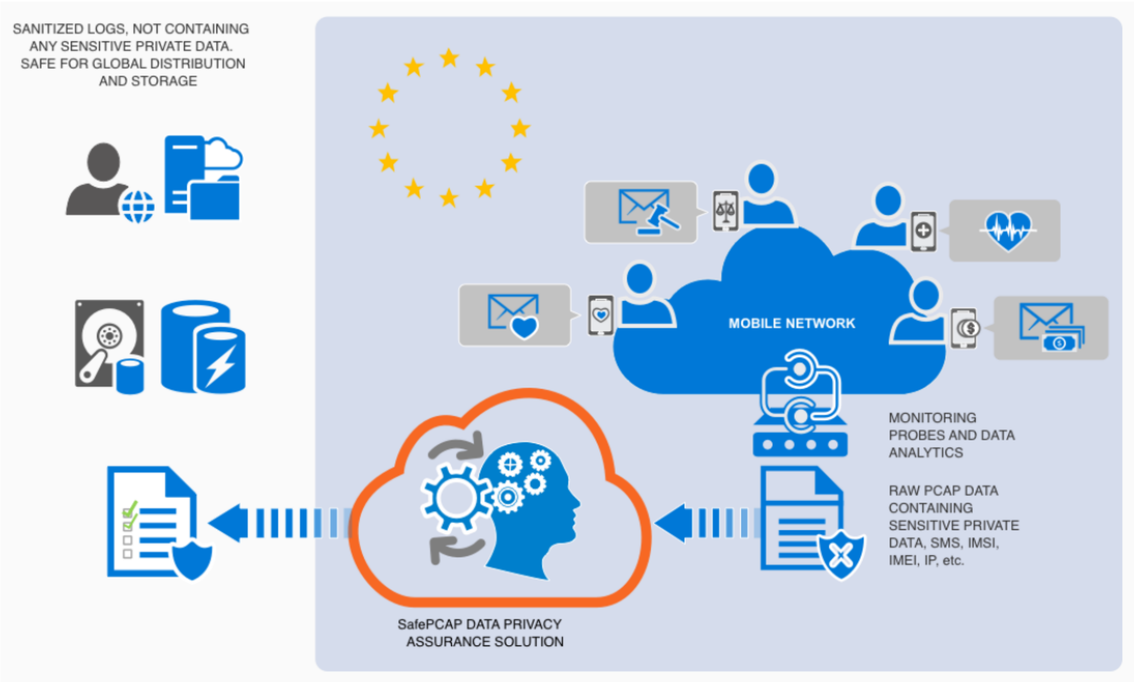
Εκτός αυτού, τα δεδομένα που συλλέγονται κατά τη καταγραφή της δικτυακής ροής μπορούν να αποκαλύψουν τις ιστοσελίδες που επισκέφτηκαν οι χρήστες, σε ποιες χρονικές στιγμές, ποιες υπηρεσίες χρησιμοποίησαν καθώς και τον όγκο των δεδομένων που αντάλλαξαν. Οι τεχνικές “Deep Packet Inspection” (DPI) μπορούν να αποκαλύψουν και να καταγράψουν δραστηριότητες στο διαδίκτυο σε τέτοιο βαθμό που κινδυνεύει η ιδιωτικότητα όλων το ατόμων τα στοιχεία των οποίων έχουν καταγραφεί [90]. Επιπρόσθετα, από τα εξαχθέντα email τρίτων ως προς την εξεταζόμενη υπόθεση ατόμων υπάρχει η δυνατότητα εύρεσης προσωπικών τους στοιχείων όπως το πραγματικό ονοματεπώνυμο και όλα τα συνημμένα αρχεία και η εξέταση της mac address του υπολογιστή στον οποίο ανήκουν τα πακέτα μπορεί να καταδείξει τον κατασκευαστή του μηχανήματος (άρα και τον χρήστη στον οποίο ανήκει το εν λόγω μηχάνημα) (μέσω του OUI, Organizational Unique Identifier). Τέλος, εάν οι αποθηκευμένοι κωδικοί έχουν υποκλαπεί και βρίσκονται κωδικοποιημένοι στην μορφή BASE64 μπορούν να μετατραπούν σε UTF-8 και να αποκαλυφθούν.

4.6. Privacy aware Network Forensics

Γίνεται κατανοητό από τις προηγούμενες παραγράφους ότι η ιδιωτικότητα των ατόμων είναι δυνατόν να καταπατηθεί σε κάθε στάδιο της ψηφιακής δικανικής ανάλυσης των δικτύων. Είναι λοιπόν επιτακτική η ανάγκη να υιοθετηθούν μηχανισμοί και τεχνικές ώστε να εκτελεστεί απρόσκοπτα η ψηφιακή δικανική ανάλυση των δικτύων και παράλληλα να προφυλαχθεί η ιδιωτικότητα των ατόμων.

Αρχικά, πρέπει να δοθεί έμφαση στον τρόπο αποθήκευσης των δεδομένων της δικτυακής ροής του προς εξέταση συστήματος καθώς η παράνομη πρόσβαση σε αυτά τα δεδομένα μπορεί να θέσει υπό αμφισβήτηση τη διατήρηση της ιδιωτικότητας των ατόμων (ως παράνομη πρόσβαση εννοείται, πέρα από την περίπτωση hacking, και η περίπτωση κάποιος (λχ. ο ψηφιακός ερευνητής) να αποκτήσει πρόσβαση στα αρχεία χωρίς να πληροί τις νόμιμες διαδικασίες (έκδοση εντάλματος) και χωρίς να έχει λάβει υπόψη την πολιτική της εταιρείας περί διαχείρισης των αποθηκευμένων δεδομένων της). Εκτός αυτού, μία ψηφιακή δικανική ανάλυση των δικτύων χωρίς συγκεκριμένη τεχνική και κριτήρια έρευνας μπορεί να θέσει στη διάθεση του ψηφιακού ερευνητή δεδομένα ατόμων που δεν έχουν σχέση με την υπόθεση.

Επιπρόσθετα, πέρα από τη συλλογή δεδομένων η ψηφιακή δικανική ανάλυση των δικτύων περιλαμβάνει και τη μεταφορά των συλλεγμένων δεδομένων για την περαιτέρω ανάλυσή τους. Επειδή τα εν λόγω δεδομένα περιλαμβάνουν ιδιωτικά στοιχεία των χρηστών, στοιχεία του εσωτερικού δικτύου μιας εταιρείας κ.α. η εν λόγω μεταφορά είναι συχνά απαγορευτική, καθώς παραβιάζει πολιτικές ιδιωτικότητας των εταιρειών και τον κανονισμό προστασίας ιδιωτικότητας της Ε.Ε. (GDPR). Μία λύση στο εν λόγω πρόβλημα είναι η χρήση μεθόδων όπως το SafePcap [93] με το οποίο γίνεται scrambling στα πακέτα πριν την αποθήκευσή τους με σκοπό την αφαίρεση στοιχείων προσωπικού χαρακτήρα. Το SafePcap χρησιμοποιεί τεχνικές όπως anonymization και pseudonymization με σκοπό να αποκρύψει από τα αποθηκευμένα πακέτα στοιχεία προσωπικού χαρακτήρα. Η εν λόγω διεργασία μπορεί να εκτελεστεί και κατά τη διάρκεια της λήψης των εν λόγω πακέτων και σε ήδη αποθηκευμένα πακέτα που συλλέχθηκαν με κάποιο NFAT. Με την εν λόγω τεχνική διατηρείται το binary integrity των πακέτων με τον επανυπολογισμό του μήκους, του checksum και όλων των service fields των επηρεασμένων πακέτων ενώ παράλληλα ικανοποιούνται οι απαιτήσεις ιδιωτικότητας του GDPR.



Εικ.4: Λειτουργία SafePCAP

Μία έτερη λύση για εκτέλεση ψηφιακής δικανικής ανάλυσης των δικτύων χωρίς να διακυβεύεται η ιδιωτικότητα των χρηστών είναι η χρήση των Group Signatures. Με τη χρήση της εν λόγω τεχνικής εάν το μέλος μίας ομάδας υπογράψει ψηφιακά ένα πακέτο τότε τα υπόλοιπα μέλη της ομάδας μπορούν να εξακριβώσουν εάν αυτό το πακέτο ανήκει σε μέλος της ομάδας αλλά δεν μπορούν να εντοπίσουν την ταυτότητα του εν λόγω μέλους. Για να γίνει η αποκάλυψη της ταυτότητας του ιδιοκτήτη του πακέτου αυτού είναι απαραίτητη η ύπαρξη μιας εξουσιοδοτημένης τρίτης οντότητας, του Group Manager.

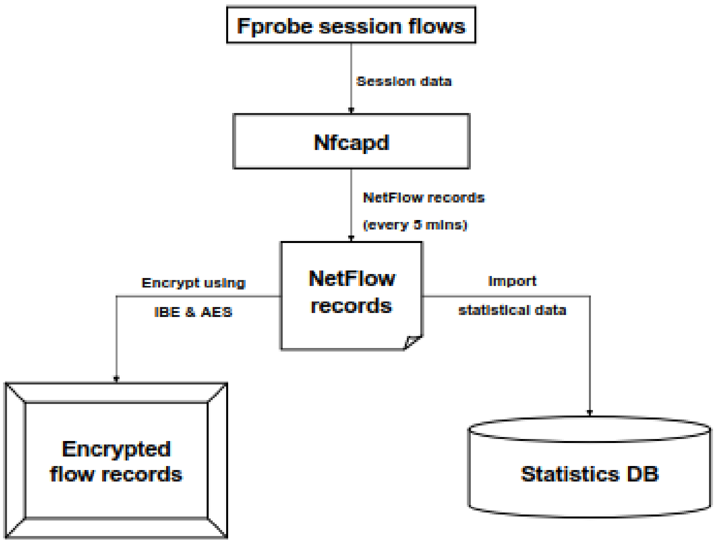
Αναλυτικότερα, έστω ένας group manager και ένα πλήθος n μελών με δικαιώματα απλού χρήστη, τα οποία χαρακτηρίζονται με τους αριθμούς 1,2,3,4……n. O group manager έχει ένα μυστικό κλειδί msk, κάθε χρήστης (i) ε (1,….,n) έχει το δικό του μυστικό κλειδί sk[i] με το οποίο υπογράφει τα πακέτα του και υπάρχει ένα μοναδικό δημόσιο κλειδί επιβεβαίωσης των υπογραφών pk. O group manager παράγει με κάποια μέθοδο key-gen τα κλειδιά pk, msk και sk(i) και τα διανέμει στους εκάστοτε αποδέκτες. Ακολούθως, εάν ένα οποιοδήποτε μέλος (i) του group χρησιμοποιήσει το μυστικό του κλειδί sk(i) για να υπογράψει ένα πακέτο m θα λάβει μία ψηφιακή υπογραφή σ. Οποιοδήποτε έτερο μέλος του group χρησιμοποιώντας το δημόσιο κλειδί pk μπορεί να εξακριβώσει ότι το ζεύγος (m,σ) ανήκει σε κάποιο μέλος του group. O group manager μπορεί να χρησιμοποιήσει το κλειδί msk για να αποκαλύψει την ταυτότητα του ιδιοκτήτη του ζεύγους (m,σ) μέσω διαδικασίας Open operation[4]. Η εν λόγω τεχνική είναι CCA[5]-fully anonymous εάν ένας αριθμός μελών του group δεν μπορεί να ανακαλύψει την ταυτότητα του μέλους (i) ακόμα και εάν μπορούν να ανοίξουν τις ψηφιακές υπογραφές όλων των πακέτων των μελών εκτός από το ζεύγος (m,σ) του χρήστη (i) και είναι fully traceable όταν κανένας αριθμός μελών του group δεν μπορεί να δημιουργήσει ένα έγκυρο ζεύγος (m,σ) χωρίς ο group manager να μην μπορεί να το ταυτοποιήσει με ένα συγκεκριμένο μέλος. Συναφώς, η χρήση της εν λόγω τεχνικής κατά τη διαδικασία συλλογής των δεδομένων προστατεύει την ιδιωτικότητα των χρηστών ενώ ο ψηφιακός ερευνητής επεξεργάζεται τα εν λόγω δεδομένα για την ανεύρεση του ενόχου, του οποίου η ταυτότητα θα αποκαλυφθεί μετέπειτα με την προαναφερθείσα τεχνική εάν συντρέχουν τεκμηριωμένοι νόμιμοι λόγοι για την άρση της προστασίας της ιδιωτικότητάς του.

Μία άλλη πρόταση για ψηφιακή δικανική ανάλυση των δικτύων με έμφαση στη προστασία της ιδιωτικότητας αναφέρεται στο [89] όπου στα αποκτηθέντα δεδομένα εφαρμόζεται κρυπτογράφηση IBE[6] με τη χρήση της διεύθυνσης IP του χρήστη και μιας χρονοσφραγίδας (public key) και το private key να τμηματοποιείται και να μοιράζεται σε διαφορετικά άτομα. Επιπρόσθετα, αποθηκεύονται στατιστικά στοιχεία της κίνησης του δικτύου (ομαδοποίηση των ξεχωριστών δικτυακών ροών των χρηστών βάσει κοινών χαρακτηριστικών) για την εξυπηρέτηση διαφόρων λειτουργιών των εταιρειών-οργανισμών (λχ. τιμολόγηση, quality of service) χωρίς να είναι δυνατό το query για στατιστικά στοιχεία ενός συγκεκριμένου ατόμου.

[4] Open Operation είναι μία διαδικασία κατά την οποία ως είσοδος λαμβάνεται μία τιμή comm(a) και μία επιπρόσθετη πληροφορία aux και ως έξοδος λαμβάνεται η τιμή a. Η εν λόγω διαδικασία έχει πλήρη αντιστοιχία όταν υπάρχει μόνο ένα a το οποίο αντιστοιχεί στο comm(a) [97]

[5] Chosen Ciphertext Attack

[6] Identity Based Encryption



Διάγραμμα 4: IBE encryption scheme

Με την ανωτέρω πρόταση προστατεύονται τα εν αποθέσει δεδομένα των χρηστών από μη εξουσιοδοτημένη πρόσβαση σε αυτά (γνώση του private key) καθώς αυτό δεν είναι μοναδικό και εξαρτάται από την εκάστοτε χρονοσήμανση της ροής και επιπλέον δεν είναι δυνατή η ανεύρεση προσωπικών πληροφοριών από τη βάση στατιστικών δεδομένων. Εάν απαιτηθεί από τον ψηφιακό ερευνητή να αποκτήσει πρόσβαση σε δικτυακή ροή συγκεκριμένου χρονικού διαστήματος και συγκεκριμένης IP τότε πρέπει όλα τα άτομα που έχουν τα τμήματα του private key για το εν λόγω διάστημα και την εν λόγω IP να τα συνθέσουν εκ νέου στο private IBE key.

Στο [91] οι F. Li et al προτείνουν μία πειραματική μέθοδο κατά την οποία είναι δυνατή η ταυτοποίηση ενός χρήστη βάσει της δραστηριότητάς του σε επίπεδο εφαρμογής αναλύοντας μετα-δεδομένα που έχουν συλλεχθεί κατά την καταγραφή της δικτυακής ροής του υπό εξέταση δικτύου. Τα μετα-δεδομένα που χρησιμοποιούνται για την εν λόγω ταυτοποίηση είναι:

α) date and time stamp

β) source and destination ip address

γ) port numbers

δ) protocol ID (TCP/UDP)

ε) length of a datagram

στ) TCP flags (πχ. SYN, FIN, ACK και PUSH)

Για παράδειγμα, μέσω single packet analysis είναι δυνατός ο εντοπισμός μεγάλων μηνυμάτων που ανταλλάσσονται μέσω skype, η προσθήκη/αφαίρεση παραληπτών μέσω της χρήσης του Hotmail και ο διαμοιρασμός αρχείων μέσω του Dropbox. Επιπρόσθετα, μέσω multiple packet analysis είναι δυνατός ο εντοπισμός της έναρξης συνομιλίας μέσω του Facebook (στέλνονται δύο πακέτα TCP συγκεκριμένου μεγέθους) καθώς και ο εντοπισμός της τροποποίησης ενός εγγράφου μέσω του Google Docs (αποστολή-λήψη διακριτών TCP πακέτων). Τέλος, μέσω streamed packet analysis είναι δυνατός ο εντοπισμός δραστηριοτήτων upload-download καθώς και βιντεοκλήσης μέσω skype.

Επομένως, ο ψηφιακός ερευνητής μπορεί μέσω της ανωτέρω μεθόδου να συλλέξει πολύτιμες για την έρευνα πληροφορίες από ανεξάρτητες πηγές δεδομένων χωρίς να χρειάζεται να εξετάσει το payload των συλλεχθέντων πακέτων, προστατεύοντας με αυτόν τον τρόπο την ιδιωτικότητα των χρηστών και μειώνοντας την απαιτούμενη υπολογιστική ισχύ για την εκτέλεση της ψηφιακής δικανικής ανάλυσης των δικτύων. Μέσω της δημιουργίας ενός συμπεριφορικού προφίλ για τους χρήστες μπορεί να εντοπίσει όχι μόνο ποιος έκανε κάτι αλλά και το τι έκανε και με ποιόν τρόπο.

Συνεπώς, η ανωτέρω πειραματική μέθοδος έχει τα ακόλουθα πλεονεκτήματα :

α) Βελτιστοποίηση των μεθόδων ταξινόμησης της δικτυακής ροής μέσω packet-based και flow-based τεχνικών με την μείωση της απαίτησης για ποσότητα και περιεκτικότητα στα συλλεχθέντα πακέτα.

β) Η ανάλυση επικεντρώνεται στη δραστηριότητα του χρήστη σε επίπεδο εφαρμογής και όχι σε δευτερεύουσες εργασίες που μπορεί να εντοπιστούν κατά την ανάλυση της δικτυακής ροής (για παράδειγμα δεν θα αναλυθούν πακέτα τα οποία αντιστοιχούν σε μία διαφήμιση στο Facebook).

γ) Η ιδιωτικότητα του χρήστη προστατεύεται καθώς αναλύονται μόνο μετα-δεδομένα που δεν μπορούν να συσχετιστούν άμεσα ή έμμεσα με αυτόν.

δ) Βελτιώνονται οι δυνατότητες ανάλυσης του ψηφιακού ερευνητή καθώς η εν λόγω μέθοδος δεν επηρεάζεται από το εάν τα πακέτα είναι κρυπτογραφημένα ή όχι και δεν απαιτούνται τεχνικές Deep Packet Inspection (DPI).

Μία έτερη λύση για την εκτέλεση ενός πρώιμου σταδίου ψηφιακής δικανικής ανάλυσης των δικτύων με έμφαση στη προστασία της ιδιωτικότητας από τους διαχειριστές του δικτύου είναι η χρήση του πρωτοκόλλου RPINA (Respect Private Information, Not Abuser) [94] σε ένα δίκτυο όπου ανταλλάσσονται δεδομένα μεταξύ χρηστών και server χωρίς να αποκαλύπτεται η ταυτότητα των χρηστών εκ των προτέρων και ενώ χρησιμοποιούνται τεχνολογίες PET (Privacy Enhancing Technologies). Με το εν λόγω πρωτόκολλο οι ανώνυμοι χρήστες επικοινωνούν αρχικά με ένα Directory Service (DS) στο οποίο καταχωρούνται τα στοιχεία τους (για κάθε session δημιουργούν οι χρήστες ένα ζεύγος private/public key και το DS κρατά ένα signed αντίγραφο αυτού του ζεύγους (non-repudiation) σε περίπτωση απαίτησης για εκτέλεση forensics) και έπειτα συνάπτεται επικοινωνία χρησιμοποιώντας τα εν λόγω στοιχεία με τον server. Σε περίπτωση που ο server υποπτευθεί κακόβουλη δραστηριότητα από κάποιον χρήστη θα στείλει το περιεχόμενο της δικτυακής ροής στο DS (στην περίπτωση αυτή θα λάβει το ρόλο του Forensic Investigation Entity). Το DS, αφού εξετάσει και διαπιστώσει ότι η εν λόγω δικτυακή ροή είναι κακόβουλη θα χρησιμοποιήσει το αποθηκευμένο αντίγραφο του signed ζεύγους private/public key που ανταποκρίνεται στην εν λόγω δικτυακή ροή και θα απαντήσει στον server με τα στοιχεία του συγκεκριμένου χρήστη στον οποίο ανήκει η εν λόγω δικτυακή ροή. Με αυτόν τον τρόπο και πριν εκτελεσθεί ψηφιακή δικανική ανάλυση των δικτύων από κάποιον ειδικό ψηφιακό ερευνητή οι διαχειριστές του δικτύου μπορούν να συλλέξουν πολύτιμα δεδομένα για την μετέπειτα έρευνα. Η τεχνική αυτή είναι ανεξάρτητη του χρησιμοποιούμενου PET, δεν θέτει σε κίνδυνο την ιδιωτικότητα των υπολοίπων χρηστών του δικτύου (αποκαλύπτονται τα στοιχεία μόνο του χρήστη του οποίου η δραστηριότητα χαρακτηρίζεται κακόβουλη) και συμβάλει στην επιτυχή αναγνώριση του κακόβουλου χρήστη (η καταχώρηση του υπογεγραμμένου ζεύγους private/public key στο DS στην αρχή της επικοινωνίας διασφαλίζει το non-repudiation αυτής).

Τέλος, μία έτερη λύση για εκτέλεση ψηφιακής δικανικής ανάλυσης των δικτύων με έμφαση στη προστασία της ιδιωτικότητας κατά τη συλλογή ψηφιακών πειστηρίων σε περίπτωση που έγινε δικτυακή επίθεση χρησιμοποιώντας πολλούς υπολογιστές ως ενδιάμεσους κόμβους είναι η χρήση του πρωτοκόλλου STOP (Session TOken Protocol).[95] Το εν λόγω πρωτόκολλο σε κάθε βήμα αποθηκεύει σε επίπεδο εφαρμογής πληροφορίες σχετικές με την διεργασία και τον χρήστη που άνοιξε μία socket για την εν λόγω διεργασία και στέλνει αντίστοιχο αίτημα αναγνώρισης σε έτερο υπολογιστή εάν διαπιστώσει ότι υπάρχει κάποιος έτερος κόμβος πριν τον εξεταζόμενο που εμπλέκεται με την υπό εξέταση επικοινωνία. Σε κάθε βήμα επιστρέφεται στο πρόγραμμα ένα hashed token και ο ψηφιακός ερευνητής δεν μπορεί να μάθει άμεσα τα στοιχεία του χρήστη και της διεργασίας κάθε βήματος αλλά πρέπει να αποστείλει το hashed token στον διαχειριστή του δικτύου ο οποίος θα κρίνει εάν είναι σκόπιμη η αποκάλυψη των εν λόγω πληροφοριών. Με αυτόν τον τρόπο προστατεύονται τα προσωπικά στοιχεία των ενδιάμεσων κόμβων σε περίπτωση που εκτελείται ψηφιακή δικανική έρευνα σε επίθεση που χρησιμοποιεί ενδιάμεσους κόμβους[7].

[7] Τεχνική Stepping stone [96]

Επίλογος

Στις σελίδες που προηγήθηκαν έγινε λόγος αρχικά για το υφιστάμενο εθνικό και ευρωπαϊκό νομικό πλαίσιο βάσει του οποίου προστατεύονται τα προσωπικά δεδομένα των ατόμων και αναλύθηκαν οι διαδικασίες που ακολουθεί ο ψηφιακός εγκληματολόγος για να συλλέξει ψηφιακά πειστήρια. Ακολούθως, αναφέρθηκαν οι πιθανές παραβιάσεις της ιδιωτικότητας των χρηστών από την εκτέλεση της ψηφιακής εγκληματολογικής έρευνας τόσο σε προσωπικές ηλεκτρονικές συσκευές (κινητά, υπολογιστές) όσο και σε server και διαδικτυακές οντότητες και στη συνέχεια παρουσιάστηκαν μεθοδολογίες με τις οποίες μπορεί να εκτελεστεί ψηφιακή εγκληματολογική ανάλυση σε ψηφιακά δεδομένα με γνώμονα την προστασία των προσωπικών δεδομένων. Τέλος, στο τελευταίο κεφάλαιο της μεταπτυχιακής διατριβής έγινε λόγος για τη ψηφιακή εγκληματολογική έρευνα στα δίκτυα υπολογιστών, αναφέρθηκαν οι εφαρμοζόμενες τεχνικές εκτέλεσης αυτής, τα προβλήματα παραβίασης της ιδιωτικότητας των χρηστών που μπορεί να προκαλέσουν και προτάθηκαν μέθοδοι ώστε η εκτέλεση της εν λόγω έρευνας να γίνει με γνώμονα την προστασία των προσωπικών δεδομένων.

Κλείνοντας την παρούσα μεταπτυχιακή διατριβή κρίνεται σκόπιμο να αναφερθεί ότι το νέο νομοθετικό πλαίσιο περί προστασίας των προσωπικών δεδομένων για τις ευρωπαϊκές χώρες (GDPR) έχει θέσει νέους κανόνες για την εκτέλεση της ψηφιακής εγκληματολογικής έρευνας στα ψηφιακά δεδομένα κάνοντας επιτακτική την ανάγκη επαναπροσδιορισμού τόσο των υφιστάμενων πρακτικών-διαδικασιών εκτέλεσης της ψηφιακής εγκληματολογικής έρευνας και ανάλυσης όσο και των χρησιμοποιούμενων τεχνολογικών μέσων λαμβάνοντας πάντα υπόψη τις αυξανόμενες τεχνολογικές δυσκολίες στη συλλογή ψηφιακών πειστηρίων που παρουσιάζονται λόγω των νέων προγραμμάτων PET και των νέων τεχνικών Anti-Forensics. Τέλος, λόγω των διαρκώς νέων ανακυπτόντων τεχνικών μη εξουσιοδοτημένης πρόσβασης στις ηλεκτρονικές συσκευές με σκοπό την υπεξαίρεση προσωπικών πληροφοριών, χρημάτων κτλ καθίσταται αδήριτη η ανάγκη άμεσης ανεύρεσης νέων μεθοδολογιών εκτέλεσης digital forensics με βάση τα υφιστάμενα εργαλεία ψηφιακής ανάλυσης και εμπλουτισμού της υφιστάμενης βιβλιογραφίας με σύγχρονες τεχνικές παράκαμψης των PETs και AF καθώς η υφιστάμενη βιβλιογραφία κινδυνεύει να χαρακτηριστεί ως παρωχημένη σε σχέση με το νέο, πολύπλοκο και συνεχώς εξελισσόμενο περιβάλλον στο οποίο καλείται να δράσει ο ψηφιακός εγκληματολόγος έχοντας παράλληλα ως γνώμονα σε κάθε στάδιο της δραστηριότητάς του την προστασία των προσωπικών δεδομένων.

Βιβλιογραφία

[1] Frank Y.W. Law et al, «Protecting Digital Data Privacy in Computer Forensic Examination», Systematic Approaches to Digital Forensic Engineering (SADFE), 2011.

[2] J. Michael, «Privacy and human rights: an international and comparative study, with special reference to developments in information technology», Dartmouth Pub. Co., 1994.

[3] Gautham Pallapa, Nirmala Roy, Sajal K. Das, «Ubiquotous Computing Environment», Centre of Research in Wireless Mobility and Networking, University of Texas.

[4] Κων/νος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, «Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και επικοινωνιών .Τεχνικά και νομικά θέματα», εκδόσεις Παπασωτηρίου, 2010.

[5] 5 Cases solved using extensive Digital Forensic Evidence, Online, available http: https://blog.eccouncil.org/5-cases-solved-using-extensive-digital-forensic-evidence/, accessed:06-08-20.

[6] How to become a digital forensic investigator in 2020, Online, available http: https://blog.eccouncil.org/how-to-become-a-digital-forensic-investigator-in-2020/#:~:text=A%20digital%20forensic%20investigator%20is,i.e.%2C%20after%20a%20security%20incident, accessed: 15-08-20.

[7] Ferguson, R.I. and Renaud, Karen and Wilford, Sara and Irons, Alastair, «PRECEPT : a framework for ethical digital forensics investigations», Journal of Intellectual Capital, 21 (2), pp. 257-290, 2020.

[8] Αθανασία Κούρμπαση, «Νομικό πλαίσιο εργαστηρίου ψηφιακής εγκληματολογίας σε στρατιωτικό περιβάλλον», Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς.

[9] Ψηφιακή εγκληματολογία, Wikipedia, Online, available http: https://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CE%B5%CE%B3%CE%BA%CE%BB%CE%B7%C2%B5%CE%B1%CF%84%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1, accessed:12-02-21.

[10] Νόμος 4624/19 (ΦΕΚ 137/Α/29-8-2019): Προστασία δεδομένων προσωπικού χαρακτήρα.

[11] Κανονισμός 679/2016 της Ε.Ε. για την προστασία δεδομένων προσωπικού χαρακτήρα.

[12] Οδηγία 680/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

[13] Ana Nieto, Ruben Rios and Javier Lopez, «Privacy-Aware Digital Forensics», chapter 8, Network, Information and Computer Security (NICS) Lab, Computer Science Department, University of Malaga, Spain, 2019.

[14] Ali Dehghantanha, Katrin Franke, «Privacy-Respecting Digital Investigation», Twelfth Annual Conference on Privacy, Security and Trust (PST), 2014.

[15] Disk Forensics, Resource Centre for Cyber Forensics-India, Online, available http: http://www.cyberforensics.in/(A(YFMf49VLzAEkAAAAMWE3NDQ2ZTEtNjg5MC00Mjc5LWE0NjQtNTc2NDQxNjRlNTdhxwC8Rqlzd2-ICCb20r6htoqh1sI1))/Research/DiskForensics.aspx?AspxAutoDetectCookieSupport=1#:~:text=Disk%20forensics%20is%20the%20science,Authenticate%20the%20evidence, accessed:16-02-21.

[16] Disk Drive Forensics, Global Digital Forensics, Online, available http: https://evestigate.com/disk-drive-forensics/, accessed:16-02-21.

[17] Memory Dump, techopedia, Online, Available http: https://www.techopedia.com/definition/20663/memory-dump#:~:text=A%20memory%20dump%20is%20a,to%20application%20or%20system%20failure., accessed:16-02-21.

[18] Memory Forensics, Wikipedia, Online, available http: https://en.wikipedia.org/wiki/Memory_forensics#:~:text=Memory%20forensics%20is%20forensic%20analysis,be%20analyzed%20for%20forensic%20information., accessed: 16-02-21.

[19] What is Digital Forensics? History, Process, Types, Challenges, Guru 99, Online, available http: https://www.guru99.com/digital-forensics.html#:~:text=Different%20types%20of%20Digital%20Forensics,Forensics%2C%20Memory%20Forensics%2C%20etc., accessed:16-02-21.

[20] Ranum M. , Network flight recorder, Online, available HTTP: http://www.ranum.com/, accessed: 08-08-20.

[21] Eric Conrad, Seth Misenar and Joshua Feldman, «CISSP Study Guide», Third Edition,2015.

[22] Hristina Marošević, «Wireless Forensics», Faculty of Electrical Engineering and Computing, University of Zagreb, 2017.

[23] Database Forensics, Wikipedia, Online, available http: https://en.wikipedia.org/wiki/Database_forensics#:~:text=Database%20forensics%20is%20a%20branch,to%20database%20contents%20and%20metadata., accessed:16-02-21.

[24] What is Malware Forensics? , Hawk Eye Forensic, Online, available http: https://hawkeyeforensic.com/2020/05/04/what-is-malware-forensics/, accessed:16-02-21.

[25] Frederik Armknecht, Andreas Dewald, «Privacy-preserving email forensics», Digital Investigation, pp.127-136, 2015.

[26] The Mobile Forensics Process: Steps & Types, Infosec, online, available http: https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/, accessed:16-02-21.

[27] Shahzad Saleem, Oliver Popov, «Formal Approach for the Selection of a Right Tool for Mobile Device Forensics», ResearchGate, 2014.

[28] Mohammed I. Alghamdi, «Digital forensics in cyber security - recent trends, threats, and opportunities», Periodicals of Engineering and Natural Sciences, Vol. 8, No. 3, pp.1321-1330, July 2020.

[29] ISO/IEC 27037:2012.

[30] 27042:2015.

[31] Rogers MK, Goldman J, Mislan R, et al. , «Computer forensics field triage process model», Journal of Digital Forensics, Security and Law.;1(2):2, 2006.

[32] P. Gladyshev, «Formalizing Event Reconstruction in Digital Investigations», Ph.D. Thesis, Department of Computer Science, University College Dublin, Dublin, Ireland, 2004.

[33] Wynand Staden, «Protecting Third Party Privacy in Digital Forensic Investigations», 9th International Conference on Digital Forensics (DF), Orlando, FL, United States. pp.19-31, Jan 2013.

[34] Ayman Shaabana, Nashwa Abdelbaki, «Comparison Study of Digital Forensics Analysis Techniques; Findings versus Resources», The 5th International Workshop on Privacy and Security in HealthCare (PS Care 2018), Procedia Computer Science 141 ,pp.545–551, 2018.

[35] Langheinrich, M., «Privacy by design—principles of privacy-aware ubiquitous systems», In International conference on Ubiquitous Computing, Springer, Berlin, Heidelberg, pp. 273-291, 2001.

[36] Caviglione, L., Wendzel, S. and Mazurczyk, W., «The future of digital forensics: Challenges and the road ahead», IEEE Security & Privacy, Vol. 15 No. 6, pp. 12-17, 2017.

[37] Privacy-enhancing technologies, Wikipedia, Online, available http: https://en.wikipedia.org/wiki/Privacy-enhancing_technologies#:~:text=A%20privacy%2Denhancing%20technologies%20(PET,data%20security%2C%20and%20empowering%20individuals.&text=PETs%20use%20techniques%20to%20minimize,functionality%20of%20an%20information%20system., accessed: 17-02-21.

[38] Wynand Staden, «Protecting Third Party Privacy in Digital Forensic Investigations» , 9th International Conference on Digital Forensics (DF), Orlando, FL, United States. pp.19-31, Jan 2013.

[39] Simone Fischer-Hubner, Leonardo A. Martucci, «Privacy in Social Collective Intelligence Systems», pp:105-124, 2014.

[40] Kessler, G.C. , «Anti-forensics and the digital investigator», Proceedings of the 5th Australian Digital Forensics Conference, Mt. Lawley, Western Australia: Edith Cowan University, December 2007.

[41] Adedayo M. Balogun, Shao Ying Zhu, «Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology», International Journal of Advanced Computer Science and Applications, Vol. 4, No.5, pp:36-40, 2013.

[42] Παπουτσής Δημήτριος, «Ανασκόπηση και περιγραφή των μεθοδολογιών, προτύπων και εργαλείων που χρησιμοποιούνται για την ανάλυση ψηφιακών πειστηρίων διαδικτυακών υπηρεσιών (Web Services Forensics)- Επίδειξη κυριοτέρων ανοιχτών εργαλείων με συγκεκριμένες περιπτώσεις χρήσης», Μεταπτυχιακή Διατριβή, Πανεπιστήμιο Πειραιώς, 2015.

[43] Kevin Conlan, Ibrahim Baggili, Frank Breitinger, «Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy», Proceedings of the 16th Annual USA Digital Forensics Research Conference, Digital Investigation 18 ,pp.66-75, 2016.

[44] Asou Aminnezhad, Ali Dehghantanha, Mohd Taufik Abdullah, «A Survey on Privacy Issues in Digital Forensics», International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4), pp.311-323, 2012.

[45] Verma R., Govindaraj J., and Gupta G., «Data privacy perceptions about digital forensic investigations in india», Ifip international conference on digital forensics pp. 25–45, 2016.

[46] I-Long Lin, Yun-Sheng Yen, Annie Chang: «A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime», International Journal of Computer Engineering Science (IJCES), Volume 2 Issue 3, 2012.

[47] EU's anti-corruption drive hits Bulgaria, Romania, Report available at: http://www.euractiv.com/justice/eus-anti-corruption-drive-hits-b-news-505391, 06 Jun 2013, accessed 11-04-20.

[48] EU fights corruption, Report available at: http://www.neurope.eu/article/eu-fights-corruption, 05- Mar-2013.

[49] Suresh V.A, Venkatesh B. B and Anajaneyulu A.C, «Data Preservations by Using Digital Forensic Techniques», International Journal of Computer Systems (ISSN: 2394-1065), Volume 03– Issue 03, March, 2016.

[50] Matthew Geiger, Lorrie Faith Cranor, «Counter-Forensic Privacy Tools- A Forensic Evaluation», Institute for Software Research, Carnegie Mellon University, 2005.

[51] M. Geiger and L. F. Cranor, «Scrubbing Stubborn Data: An Evaluation of Counter-Forensic Privacy Tools», IEEE Security & Privacy, vol. 4, no. 5, pp. 16-25, Sept.-Oct. 2006.

[52] Matthew Geiger, «Counter-Forensic Tools: Analysis and Data Recovery», PDT Forensics Team, CERT, Online, available http: https://www.first.org/conference/2006/papers/geiger-matthew-papers.pdf , accessed: 25-02-21.

[53] Differences Between the Privacy Laws in the EU and the US, Online, available http: https://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/#gref, accessed 04-05-20.

[54] D. Forte, «Dealing with forensic software vulnerabilities: is anti forensics a real danger? », Network Security, vol. 2008, pp. 18-20, 2008.

[55] Maria Karyda, Lilian Mitrou, «Internet Forensics: Legal and Technical Issues», University of the Aegean, Department of Information and Communication Systems, 2007.

[56] Suresh V.A, Venkatesh B. B, Anajaneyulu A.C, «Data Preservations by Using Digital Forensic Techniques», International Journal of Computer Systems (ISSN: 2394-1065), Volume 03– Issue 03, March, 2016.

[57] William Bradley Glisson, Tim Storer, Andrew Blyth, George Grispos and Matt Campbell, «In The Wild Residual Data Research and Privacy», Journal of Digital Forensics, Security and Law, 11(1), pp. 77-98, 2016.

[58] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine, «Threats to Privacy in the Forensic Analysis of Database Systems», University of Massachusetts, Amherst, Department of Computer Science, 2007.

[59] Wynand JC van Staden, «An investigation into reducing third party privacy breaches during the investigation of cybercrime», South African institute of electrical engineers, vol.106 (2), June 2015.

[60] Rahul Neware and Amreen Khan, «Cloud Computing Digital Forensic challenges», Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1, 2018.

[61] H. Burkert, «Privacy-enhancing technologies: Typology, critique, vision, in Technology and Privacy: The New Landscape», MIT Press, Cambridge, Massachusetts, pp.125–142, 1997.

[62] Waleed Halboob, Ramlan Mahmod, Nur Izura Udzir, Mohd Taufik Abdullah, «Privacy policies for computer forensics», Computer Fraud & Security, pp:9-13, August 2015.

[63] Frederik Armknecht, Andreas Dewald, «Privacy-preserving email forensics», Digital Investigation 14, pp:127-136, 2015.

[64] Dave Bullock, Aliyu Aliyu, Leandros Maglaras, Mohamed Amine Ferrag, «Security and privacy challenges in the field of iOS device forensics», AIMS Electronics and Electrical Engineering, Volume 4, Issue 3, pp: 249–258, 2020.

[65] Kerschbaum Florian , Schaad Andreas, «Privacy-preserving social network analysis for criminal investigations», Proceedings of the ACM Conference on Computer and Communications Security, pp: 9-14, 2008.

[66] Nieto Ana,Rios Ruben ,Lopez Javier, «IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations», Sensors, 2018.

[67] Nieto A. et al., «A Methodology for Privacy-Aware IoT-Forensics» , IEEE Trustcom/BigDataSE/ICESS, pp:626-633, 2017.

[68] Antoniou Giannakis , Wilson Campbell , Geneiatakis Dimitris, «PPINA – A Forensic Investigation Protocol for Privacy Enhancing Technologies», 2006.

[69] Kwecka Zbigniew , Buchanan William, «Minimising Collateral Damage: Privacy-Preserving Investigative Data Acquisition Platform», IJITSA, vol 4, pp:12-31, 2011.

[70] Verma Robin; Govindaraj Jayaprakash, Chhabra Saheb,Gupta Gaurav, «DF 2.0: An Automated, Privacy Preserving, and Efficient Digital Forensic Framework That Leverages Machine Learning for Evidence Prediction and Privacy Evaluation», Journal of Digital Forensics, Security and Law, Vol. 14 -No. 2, Article 3, 2019.

[71] N.J. Croft, M.S. Olivier, «Sequenced release of privacy-accurate information in a forensic investigation», digital investigation, vol: 7, pp: 95 – 101, January 2010.

[72] S. Hou, T. Uehara, S. M. Yiu, L. C. K. Hui, K. P. Chow, «Privacy Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics», Third International Conference on Multimedia Information Networking and Security, Shanghai, China, pp. 595-599, 2011.

[73] A. Gupta, «Privacy preserving efficient digital forensic investigation framework», Sixth International Conference on Contemporary Computing (IC3), Noida, India, pp. 387-392, 2013.

[74] Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi, «Network forensic frameworks: Survey and research challenges», digital investigation, vol 7, pp. 14 – 27, 2010.

[75] Casey E., «Network traffic as a source of evidence: tool strengths, weaknesses and future needs», Digit. Invest. ,vol 1, pp. 28-43, 2004.

[76] Garfinkel S.L., «Digital forensics research: the next 10 years», Digit. Invest., vol 7, pp.64-73, 2010.

[77] Harichandran V.S., Breitinger F., Baggili I., Marrington A., «A cyber forensics needs analysis survey: revisiting the domain's needs a decade later», Comput. Secur., vol 57, pp.1-13, 2016.

[78] Beebe N., «Digital forensic research: the good, the bad and the unaddressed», IFIP International Conference on Digital Forensics, Springer, pp. 17-36, 2009.

[79] Yong Guan, «Computer and Information Security Handbook», Third Edition, 2013.

[80] Ren W, Jin H., «Modeling the network forensics behaviors», Proceedings of the first international conference on security and privacy for emerging areas in communication networks, Secure Comm 2005; pp. 1–8, Sept. 2005.

[81] Garfinkel S., «Network forensics: tapping the Internet», Online, available http:https://www.academia.edu/2600338/Network_forensics_Tapping_the_internet, accessed: 25-02-21.

[82] Sira R. , «Network forensics analysis tools: an overview of an emerging technology», GSEC, version 1.4; Jan. 2003.

[83] Vicka Corey, Charles Peterman, Sybil Shearin, Michael S. Greenberg, James Van Bokkelen, «Network Forensics Analysis», IEEE Internet Computing, pp:60–66, November 2002.

[84] Cohen M.I., «PyFlag - an advanced network forensic framework», Digit. Invest. , vol 5, pp.112-120, 2008.

[85] Manesh T., Brijith B., Singh M.P., «An improved approach towards network forensic investigation of HTTP and FTP protocols», Advances in Parallel Distributed Computing, Springer, Heidelberg, pp. 385-392, available http: https://doi.org/10.1007/978-3-642-24037-9_38 , 2011.

[86] Kaushik A.K., Pilli E.S., Joshi R.C., «Network forensic analysis by correlation of attacks with network attributes», Information and Communication Technologies, Springer, Heidelberg, pp. 124-128, available http: https://doi.org/10.1007/978-3-642-15766-0_18, 2010.

[87] Nikkel BJ, «Generalizing sources of live network evidence», Digital Investigation (The International Journal of Digital Forensics & Incident Response); vol 2(3), pp: 193–200, Sept. 2005.

[88] Shilpika Mishra, «Privacy-Preserving Network Forensics», Biju Pattnaik University of Technology, March 2013.

[89] Bilal Shebaro, «Privacy-Preserving Techniques for Computer and Network Forensics», The University of New Mexico, May 2012.

[90] Stalla-Bourdillon S., Papadaki E., Chown T., «From porn to cybersecurity passing by copyright: how mass surveillance technologies are gaining legitimacy the case of deep packet inspection technologies», Computing Law Security, Rep. 30 (6), pp.670-686, available http: https://doi.org/10.1016/j.clsr.2014.09.006, 2014.

[91] Clarke N., Li F., Furnell S., «A novel privacy preserving user identification approach for network traffic», Computer Security, vol 70, pp. 335-350, available http: https://doi.org/10.1016/j.cose.2017.06.012, 2017.

[92] Afanasyev M., Kohno T., Ma J., Murphy N., Savage S., Snoeren A.C., Voelker G.M., «Privacy-preserving network forensics», Community ACM 54 (5), pp. 78-87, available http: https://doi.org/10.1145/1941487.1941508, 2011.

[93] GDPR and NISTIR 8053 Compliance for your Pcap files, Online, available http: https://omnipacket.com/safepcap, accessed:13 December 2020.

[94] Giannakis Antoniou, Stefanos Gritzalis, «RPINA- Network Forensics Protocol Embedding Privacy Enhancing Technologies», International Symposium on Communications and Information Technologies, 2006.

[95] B. Carrier, C. Shields, «A recursive session token protocol for use in computer forensics and TCP traceback», Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, New York, NY, USA, vol.3, pp. 1540-1546, doi: 10.1109/INFCOM.2002.1019405, 2002.

[96] He Ting, Tong Lang, «Detecting Encrypted Stepping-Stone Connections», Signal Processing, IEEE Transactions, Vol 55, pp:1612-1623, 2007.

[97] Yves Deswarte, Sébastien Gambs, «Towards a Privacy-preserving National Identity Card», Fourth International Workshop on Data Privacy Management, Saint Malo, France. pp.30-43, Sep 2009.

[98] SpyCloud, “60% Password Reuse: Password Security Needs a Forced Reset”, online, available http: https://spycloud.com/password-reuse/ , accessed 09-01-22.

[99] Christoforos Ntantogian, Dimitris Apostolopoulos, Giannis Marinakis, Christos Xenakis, «Evaluating the privacy of Android mobile applications under forensic analysis», Computers & Security, Volume 42,pp: 66-76,May 2014.

[100] G. Grispos, W.B. Glisson, J.H. Pardue, M. Dickson, «Identifying User Behavior from Residual Data in Cloud-based Synchronized Apps», Conference on Information Systems Applied Research (CONISAR 2014), Baltimore Maryland, USA, 6-9 November 2014.