Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ηλεκτρονικά έγγραφα ως αποδεικτικά στοιχεία**
Ονοματεπώνυμο Φοιτητή	**ΦΑΣΙΛΑΚΗΣ ΗΛΙΑΣ**
Πατρώνυμο	**ΕΥΣΤΑΘΙΟΣ**
Αριθμός Μητρώου	**ΜΠΠΛ/ 09035**
Επιβλέπων	**Επιβλέπων Καθηγητής Α.Σινανιώτη**

Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Ημερομηνία Παράδοσης Οκτωμβριος 2014

Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΓΡΑΦΑ ΩΣ ΑΠΟΔΕΙΚΤΙΚΑ ΣΤΟΙΧΕΙΑ

Φασιλάκης Ηλίας
ΜΠΠΛ 09035

Τριμελής επιτροπή

Περιεχόμενα

Πίνακας Εικόνων

Σκοπός

Σκοπός της παρούσας εργασίας είναι η αναζήτηση της σημασίας της χρήσης των νέων τεχνολογιών πληροφορικής και τηλεπικοινωνιών στην κύρια συζήτηση και την αποδεικτική διαδικασία των νομικών διαδικασιών. Μελετώνται νόμοι, οδηγίες και αποφάσεις οι οποίες εισάγουν στις νομικές διαδικασίες μέθοδος και τεχνικές που βασίζονται στην υψηλή τεχνολογία και διερευνάται το κατά πόσο αυτές μπορούν να χρησιμοποιηθούν στην προσπάθεια εφαρμογής του Δικαίου με αδιαμφισβήτητο και αντικειμενικό τρόπο.

Περίληψη

Η ραγδαία ανάπτυξη των τεχνολογιών πληροφορικής και τηλεπικοινωνιών έχει επιφέρει σημαντικές αλλαγές σε σχεδόν όλους του κλάδους της ανθρώπινης δραστηριότητας. Οι αλλαγές που επέφερε στην προσπάθεια του ανθρώπου να αποτελεί μέρος οργανωμένου κοινωνικού συνόλου είχαν σαν συνέπεια την ανάπτυξη μίας νέας διάστασης της πληροφορικής, την Νομική Πληροφορική. Ο κλάδος αυτός εστιάζει σε ζητήματα που προκύπτουν από την συσχέτιση της επιβολής του δικαίου και νέων τεχνολογιών. Με κριτήριο την πληροφορία ως έννομο αγαθό, διακρίνεται στην νομική πληροφορική του ουσιαστικού δικαίου, όπου περιγράφονται τα νέα ατομικά δικαιώματα όπως δικαίωμα στην κοινωνία της πληροφορίας, προστασία προσωπικών δεδομένων και απορρήτου επικοινωνιών και στην προσαρμογή των νομοθετημάτων για την αντιμετώπισης νόμιμης χρήσης της τεχνολογίας, και την νομική πληροφορική για το δίκαιο, που εξετάζει τα τεχνολογικά εκείνα εργαλεία από τα οποία πλέον εξαρτάται η γνώση του ισχύοντος δικαίου.

Βασικό στοιχείο για την απονομή δικαιοσύνης αποτελεί η διαδικασία εκείνη που ακολουθείται για την υποστήριξη των ισχυρισμών των αντιδίκων. Η χρήση των νέων τεχνολογιών και ειδικότερα του διαδικτύου από μεγάλο μέρος του πληθυσμού στην Ελλάδα και την Ευρωπαϊκή Ένωση φανέρωσε την ανάγκη να μπορεί να αποδεικνύεται η συμπεριφορά των χρηστών της. Έτσι έχουν θεσπιστεί νόμοι και διαδικασίες οι οποίες μπορούν να διασφαλίσουν την μη αποποίηση ευθύνης, την αυθεντικοποίηση και την εξασφάλιση του χρήστη κατά την χρήση των εφαρμογών της πληροφορικής. Τέτοιες είναι ο σαφής προσδιορισμός των προδιαγραφών τήρησης ιστορικού χρήσης, καθορισμός διαδικασιών υπογραφής ηλεκτρονικών αρχείων, του τρόπου χρήσης των τεχνολογικών επιτευγμάτων για την καταγραφή δραστηριοτήτων.

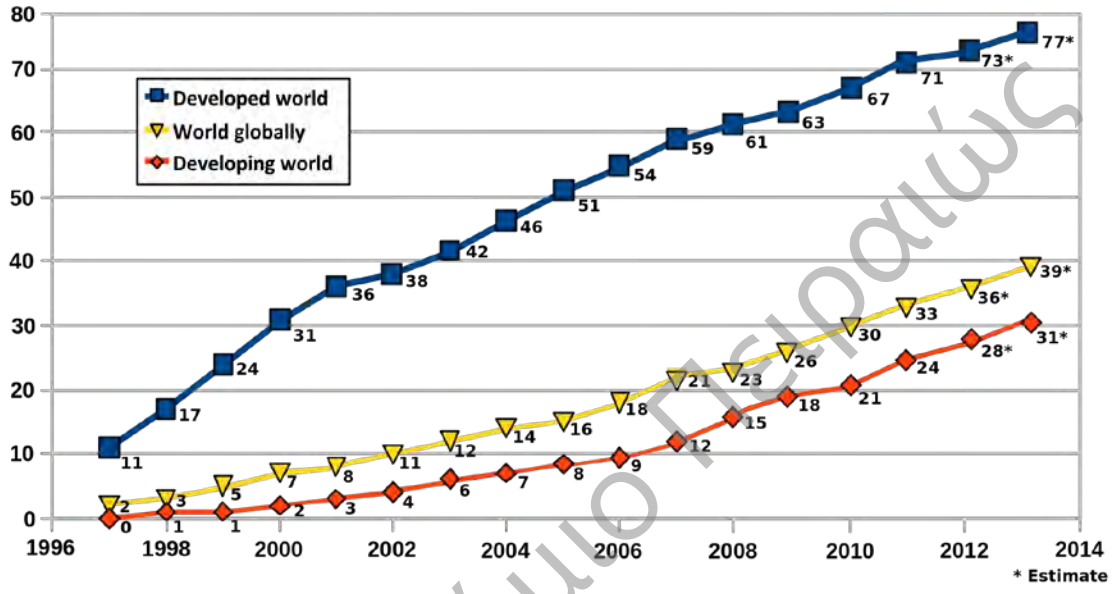
Abstract

The rapid development of information and telecommunication technologies has brought about significant changes in almost all sectors of human activity. The changes brought about in humans attempt to be part of organized society had as a consequence the development of a new dimension of computing, the Legal Informatics. This strand focuses on issues arising from the relationship between law enforcement and new technologies. In terms of information as a legal asset, is distinguished in legal informatics substantive law, which describes the new civil rights such as the right to information society, privacy and confidentiality of communications and the adaptation of instruments for addressing lawful use of technology, and legal informatics law, considering the technological tools of those who no longer depend on the knowledge of the existing law.

Key to the administration of justice is the process that is followed to support the claims of the parties. The use of new technologies and particularly the Internet by a large part of the population in Greece and the European Union revealed the need to establish that the conduct of its users. So have established laws and procedures that can ensure non-repudiation, authentication and secure user during use of computer applications. Such is the clear definition of standards compliance use history, signing determination processes electronic files, how to use technological advances to record activities.

Εισαγωγή

Οι νέες τεχνολογίες πληροφορικής και τηλεπικοινωνιών έχουν διεισδύσει τόσο στην καθημερινότητα των ανθρώπων όσο και σε σημαντικά θεσμικά ζητήματα της δημόσιας και κοινωνικής ζωής. Στο παρακάτω γράφημα αποτυπώνεται μία μόνο πτυχή που αφορά την χρήση του διαδικτύου παγκοσμίως[1].



Εικόνα 1: Χρήση του διαδικτύου παγκοσμίως

Η διείσδυση αυτή επηρέασε σε μεγάλο βαθμό τις διαπροσωπικές, κοινωνικές και διεθνείς σχέσεις σε όλα τα επίπεδα. Είναι αναπόφευκτο λοιπόν αν διατηρηθούν εκτός της προσπάθειας για την δίκαιη επίλυση των κάθε είδους διαφορών. Έτσι σήμερα είναι αναγκαία η ενσωμάτωση τους στις διαδικασίες για την εφαρμογή του Δικαίου. Στα επόμενα κεφάλαια επιχειρείται μία επισκόπηση του πως μπορεί η τεχνολογία να διευκολύνει την αποδεικτική διαδικασία.

Στο πρώτο κεφάλαιο γίνεται μία παρουσίαση των αρχείων καταγραφής των διαφόρων εφαρμογών. Μέσα από την παρουσίαση αυτή αποτυπώνεται η αποδεικτική τους αξία στην διερεύνηση αξιόποινων πράξεων. Ακολουθεί στο δεύτερο κεφάλαιο η παρουσίαση των ηλεκτρονικών αρχείων. Γίνεται ιδιαίτερη μνεία στην εφαρμογή της ψηφιακής υπογραφής ως μέσο απόδειξης της γνησιότητας του περιεχομένου και της ταυτοποίησης του εκδότη ηλεκτρονικών εγγράφων. Η τεχνική αυτή θεωρείται ζωτικής σημασίας για την καθιέρωση της ηλεκτρονικής

[1] http://www.businessinsider.com.au/whats-the-best-time-in-history-to-be-born-2014-9

διακυβέρνησης και της κοινωνίας της πληροφορίας. Στην συνέχεια γίνεται μία γενίκευση στους τρόπους με τους οποίους μπορεί να πιστοποιηθεί ο εκδότης των ηλεκτρονικών εγγράφων και η γνησιότητα των ηλεκτρονικών αρχείων αναζητώντας την αποδεικτική τους αξία στις δικαστικές αίθουσες. Στο τρίτο κεφάλαιο γίνεται αναφορά στους νόμους και τις οδηγίες που διέπουν την διατήρηση και επεξεργασία δεδομένων που καταγράφονται με ηλεκτρονικό τρόπο (βιντεοσκόπηση, φωτογράφηση, ηχογράφηση, λήψη δεδομένων μέσω διαδικτυακών φορμών κτλ.) και επιχειρείται να ξεκαθαριστεί το αν και πως τα στοιχεία αυτά μπορεί να αποτελέσουν δικανικό αποδεικτικό υλικό. Στο τέταρτο κεφάλαιο και με αφορμή την ευρεία διάδοση των κινητών τηλεφώνων και των έξυπνων συσκευών, παρουσιάζονται τρόποι με τους οποίους η χρήση τους από υποκείμενα που συμμετέχουν σε μία αποδεικτική διαδικασία, μπορεί να οδηγήσει στην αναζήτηση της αλήθειας για την απόδοση δικαιοσύνης. Στο τέλος κάθε κεφαλαίου αποτυπώνονται τα διδάγματα που προκύπτουν από την σχετική έρευνα. Τέλος παρουσιάζονται τα συμπεράσματα που προέκυψαν από την παρούσα μελέτη ως προς την χρήση της τεχνολογίας στην αποδεικτική διαδικασία.

ΚΕΦΑΛΑΙΟ 1 : ΑΝΑΛΥΣΗ ΙΣΤΟΡΙΚΟΥ (LOG RECORD) ΓΙΑ ΤΗΝ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΣΕ ΠΟΙΝΙΚΕΣ ΥΠΟΘΕΣΕΙΣ

1.1 Τι είναι τα log records (αρχεία καταγραφής).

Η ανάλυση των log records είναι ένας τομέας τεχνογνωσίας που θα μπορούσε να χρησιμοποιηθεί σε πολλές περιπτώσεις όπως μέσα σε κάποια ποινική έρευνα ή μια ποινική δίκη. Τα log records είναι υπεύθυνα για την αποθήκευση της επικοινωνίας και της σύνδεσης διάφορων συσκευών μέσα στο διαδίκτυο και κρατούν πληροφορίες για όλη την διαδρομή μετάδοσης πληροφοριών. Λόγω της χρησιμότητας της χρήσης και της επικοινωνίας μέσω του διαδικτύου, τα log records καταγράφουν μεγάλο αριθμό πληροφοριών και μπορεί να παρέχουν πολλά στοιχεία σε πολλές ποινικές υποθέσεις. Τα συνηθέστερα log records μπορεί να έχουν καταγράψει πληροφορίες σχετικές με την δραστηριότητα του χρήστη στο διαδίκτυο ή και λεπτομέρειες του τείχους προστασίας του υπολογιστή του.

Με τα log records μπορεί κάποιος ειδικός να δει διάφορες εντολές ή πληροφορίες που έχουν μεταβιβαστεί μέσω του διαδικτύου. Παραδείγματος χάρη, μπορούν να έχουν καταγράψει ποιες ιστοσελίδες επισκέφτηκε ο χρήστης του συγκεκριμένου υπολογιστή, ελέγχοντας ποιες υπερ-συνδέσεις ακολούθησε ή τι αναζητήσεις έκανε στον παγκόσμιο ιστό. Πέρα από αυτά, τα log records μπορούν να αποκαλύψουν και ποιο συγκεκριμένες πληροφορίες, όπως τι λειτουργικό σύστημα (operating system) έχει ο υπολογιστής από τον οποίο έγιναν οι παραπάνω αναζητήσεις ή ποιο πρόγραμμα περιήγησης (web browser) χρησιμοποιήθηκε. Αυτού του είδους οι πληροφορίες ονομάζονται «user-agent string».

Σε πολλές περιπτώσεις τα log records μπορούν να δείξουν τι δραστηριότητα πραγματοποιήθηκε σε έναν υπολογιστή ή κάποια άλλη συσκευή ακόμα και αν η συσκευή αυτή δεν είναι πλέον διαθέσιμη για τον οποιοδήποτε λόγο, ή αν σβήστηκαν τα αρχεία από τον υπολογιστή ή και ακόμα αν κάποιο πρόγραμμα malware (κακόβουλο λογισμικό) έτρεξε αποκλειστικά στην Random Access Memory (μνήμη RAM). Αν και το πιο κατάλληλο είναι να χρησιμοποιούνται log records σε συνδυασμό με τα αρχεία που αποθηκεύει ο κάθε υπολογιστής, τα δεύτερα μπορούν να χρησιμοποιηθούν και σε περίπτωση που δεν υπάρχει ο υπολογιστής γιατί τα αρχεία αυτά είναι εξωτερικά και δεν αποθηκεύονται στον υπολογιστή ή στην συσκευή που έκανε τις αναζητήσεις αλλά στον πάροχο[2].

Εκτός από την χρησιμότητα τους για την δραστηριότητα στο διαδίκτυο, τα log records είναι σημαντικά και στην περίπτωση εισβολής ή σε περιπτώσεις botnet. Τα Botnet είναι μια συλλογή υπολογιστών που είναι συνδεδεμένοι στο διαδίκτυο και έχουν δεχτεί επίθεση από κακόβουλα λογισμικά. Τα log records μπορούν να καταγράψουν τις συνδέσεις που έγιναν και να οδηγήσουν στον υπολογιστή που στέλνει τα κακόβουλα προγράμματα. Για παράδειγμα, σε μια περίπτωση που γίνεται χρήση HTTP (Hypertext Transfer Protocol) Command & Control (C&C)

[2] Jan Valdman, Log file analysis, σελ 4-7, διαθέσιμο στο http://www.kiv.zcu.cz/site/documents/verejne/vyzkum/publikace/technicke-zpravy/2001/tr-2001-04.pdf

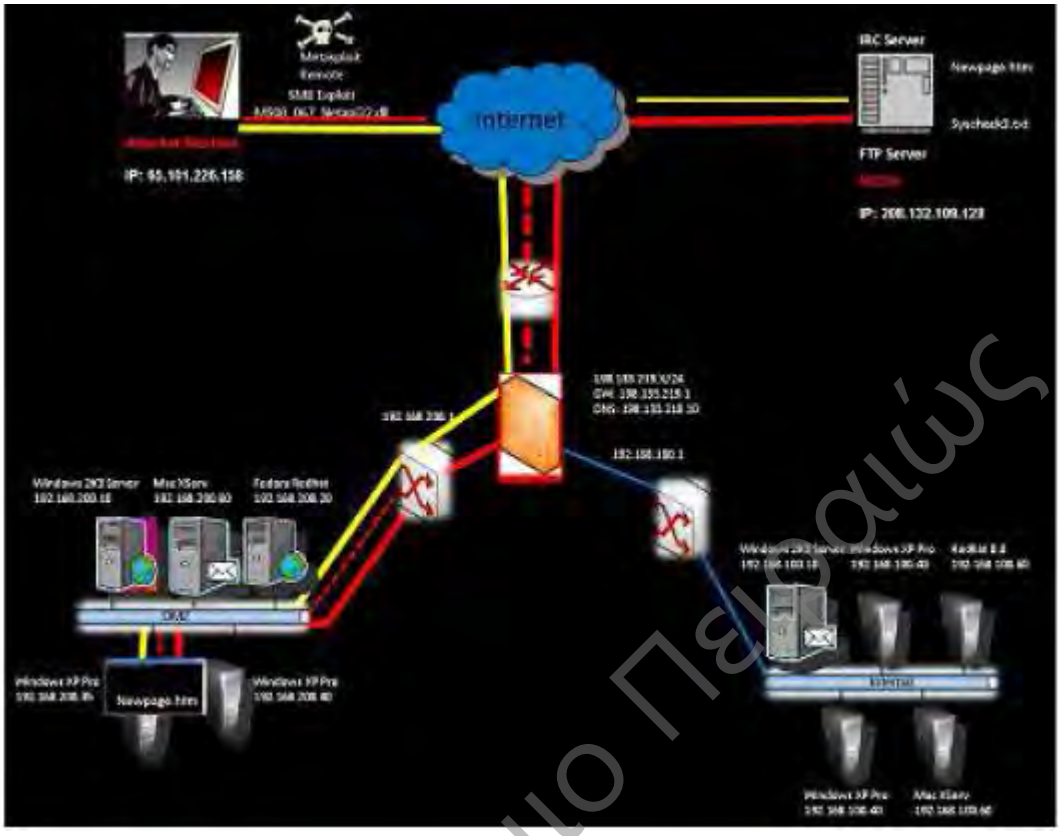
διακομιστή για την διαχείριση του botnet, ο C&C είναι ένας απλώς webserver (διακομιστής διαδικτύου) που απλώς βοηθάει στην συντήρηση και την διαχείριση του botnet. Όλα τα συστήματα – υπολογιστές που έχουν δεχτεί επίθεση κακόβουλου λογισμικού συνδέονται ανά τακτά διαστήματα με τον C&C. Κάθε σύνδεση δημιουργεί και μια συγκεκριμένη καταγραφή στα log records του διακομιστή. Όσον αφορά τον ιδιοκτήτη του υπολογιστή που δέχτηκε επίθεση, τα log records καταγράφουν στοιχεία όσον αφορά την τοποθεσία που είναι το «θύμα», το μέγεθος του botnet καθώς και τον τύπο συστημάτων που δέχτηκαν επίθεση (π.χ. λειτουργικό λογισμικό, πρόγραμμα περιήγησης κ.λ.π.). Από την πλευρά του attacker «επιτιθέμενος» τα log records είναι σε θέση να κρατήσουν λειτουργικές δραστηριότητες, όπως ποιες IP διευθύνσεις χρησιμοποιήθηκαν και άλλες πληροφορίες για τους υπολογιστές που είναι συνδεδεμένοι και χειρίζονται το botnet.

1.2 Δημιουργία log records

Για να καταλάβουμε πώς δημιουργούνται τα log records και πώς μπορούν να χρησιμοποιηθούν σε ποινικές υποθέσεις, ας εξετάσουμε έναν υποθετικό εναγόμενο που χρησιμοποίησε έναν ηλεκτρονικό υπολογιστή για να διαπράξει ένα αδίκημα που στοχεύει έναν άλλο υπολογιστή ή κάποιο δίκτυο. Η ίδια διαδικασία θα επαναλαμβάνονταν για οποιοδήποτε αδίκημα αφορούσε ηλεκτρονικό υπολογιστή, όπως μια εισβολή ή η μη-εξουσιοδοτημένη πρόσβαση στον υπολογιστή ,η υπεξαίρεση εμπορικών μυστικών πληροφοριών, η μετάδοση διακρατικής επικοινωνίας ή η κλοπή ταυτότητας. Η μεταβίβαση των πληροφοριών από τον υπολογιστή του εναγόμενου στον υπολογιστή του «θύματος» θα περάσει μέσα από μια διαδικτυακή διαδρομή που θα περιλαμβάνει δεκάδες ή περισσότερους υπολογιστές ή συσκευές. Το παρακάτω σχήμα δείχνει ένα απλουστευμένο παράδειγμα ενός εσωτερικού δικτύου. Σε κάθε σύστημα ή συσκευή κατά μήκος της διαδρομής, τα log records θα καταγράφουν ορισμένες δραστηριότητες και πληροφορίες που μπορεί να προσφέρουν πολύτιμα στοιχεία του θέματος.

1.2.1 Υποθετικό ποινικό σενάριο

Ένας εισβολέας εκμεταλλεύεται μια ευπάθεια στο τοίχο προστασίας για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα διαδικτυακό διακομιστή μιας εταιρείας. Τα αρχεία που κρατάει το τοίχος προστασίας μπορούν να δώσουν στον ερευνητή σημαντικές πληροφορίες σχετικές με την δραστηριότητα που πραγματοποιήθηκε. Τα στοιχεία που μπορούν να βρεθούν από τα logs μπορεί να δείχνουν την διεύθυνση IP του εισβολέα, τα ονόματα των αρχείων που στάλθηκαν μέσω FTP (File Transfer Protocol – χρησιμοποιείται για την μεταφορά δεδομένων μέσω του διαδικτύου), τις υπογραφές και του εισβολέα και του θύματος κ.λ.π. Όλα αυτά τα διάφορα συστήματα, που συχνά δεν πέφτουν στην αντίληψη του εισβολέα, κρατάνε συνεχόμενα στοιχεία από την επίθεση καθ' όλη την διάρκεια της. Κάθε διαδρομή ή δραστηριότητα μέσα στην διαδρομή δημιουργεί και ένα διαφορετικό log record που μπορεί να φανούν πολύ χρήσιμα για την έρευνα. Αυτά τα αρχεία μπορούν να ορίσουν το χρονοδιάγραμμα των διάφορων δραστηριοτήτων που πραγματοποιήθηκαν και να συσχετιστούν συνολικά μαζί με τα υπόλοιπα στοιχεία που θα βρεθούν.



Εικόνα 2: διαδρομή επίθεσης.

Οι μεταδόσεις μεταξύ του συστήματος του εισβολέα και του θύματος θα περάσει μέσα από τον τοίχο προστασίας κάθε φορά που θα πραγματοποιείται μια σύνδεση. Τα παρακάτω βήματα δείχνουν ένα υποθετικό σενάριο :

Πίνακας 1: Στάδια Υποθετικού Σεναρίου

ΒΗΜΑ	ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΠΛΗΡΟΦΟΡΙΕΣ LOG
1	Ο εισβολέας σαρώνει για τρωτά σημεία	Η σάρωση αναγνωρίζεται εύκολα στα log αρχεία του τοίχου προστασίας καθώς κάθε TCP/UDP (Transmission Control Protocol / User Datagram Protocol) προσπάθεια σύνδεσης καταγράφεται. Τα logs θα δείξουν ποιες υπηρεσίες δέχονται επίθεση, ποιες διευθύνσεις IP σαρώνονται, και από ποια IP ξεκίνησε η διαδικασία.
2	Ο εισβολέας προσπαθεί να εκμεταλλευτεί γνωστή ευπάθεια του συστήματος	Τα logs θα καταγράψουν την παραβίαση μιας γνωστής ευπάθειας του συστήματος.
3	Η ενέργεια εκμετάλλευσης αναγκάζει τον εσωτερικό πάροχο να ανακτήσει αρχεία από τον απομακρυσμένο FTP διακομιστή	Τα logs θα δείξουν την ώρα της δραστηριότητας, το όνομα αρχείου, τον λογαριασμό που χρησιμοποιήθηκε, την διεύθυνση IP του διακομιστή ή του πρώτου proxy (διακομιστή μεσολάβησης), το μέγεθος αρχείου κ.λ.π.
4	Ο εσωτερικός πάροχος συνδέεται με τον απομακρυσμένο Internal Relay Chat (IRC) εξυπηρετητή.	Τα logs θα περιέχουν εγγραφές τις κάθε μοναδικής IRC σύνδεσης που πραγματοποιήθηκε, την IP ή το πρώτο proxy της σύνδεσης, την διάρκεια, το συνολικό μέγεθος bytes που στάλθηκαν, την ώρα, κ.λ.π.

1.2.2 Τύποι συσκευών καταγραφής (log devices)

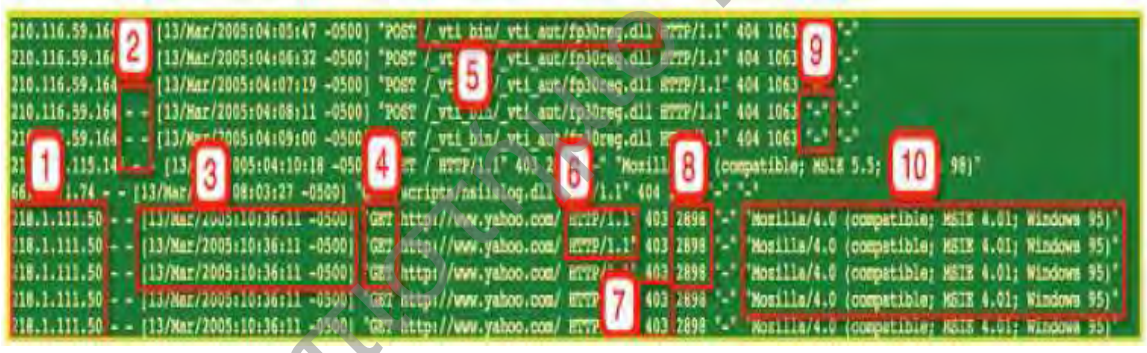
Ο τύπος συσκευών κατά μήκος της διαδρομής σύνδεσης μετάδοσης θα ποικίλει ανάλογα με τον στόχο της συσκευής ή του υπολογιστή. Για παράδειγμα, τα logs του τοίχου προστασίας μπορεί να δείξουν, μεταξύ άλλων, ποια διεύθυνση IP προσπάθησε να έχει πρόσβαση στο δίκτυο, ποια εσωτερικά συστήματα επισκέφτηκε και για πόση ώρα. Από την άλλη, τα logs ενός διαδικτυακού εξυπηρετητή μπορεί να καταγράφουν λεπτομέρειες σχετικά με την επίσκεψη σε μια τοποθεσία του διαδικτύου, τις σελίδες και τους πόρους που αναζητήθηκαν, την έκβαση της αίτησης, την διεύθυνση IP του επισκέπτη και γενικά όλες τις δραστηριότητες και ενέργειες που πραγματοποίησε σε μια σελίδα. Τέλος, τα proxy logs μπορούν να επιβεβαιώσουν την προέλευση του χρήστη και την δραστηριότητά του. Σε αυτή την περίπτωση θα ήταν χρήσιμο ένα διάγραμμα δικτύου για να μπορούν να βρεθούν βασικές συσκευές που θα μπορούν να έχουν βασικές καταγραφές.

Μερικά από τα πιο συνηθισμένα logs είναι :

- Firewall Logs (αρχεία καταγραφής τοίχου προστασίας)
- Web Server Access Logs (αρχεία καταγραφής διαδικτυακού εξυπηρετητή)
- Simple Mail Transfer Protocol / Internet Message Access Protocol Servers (email)
- FTP Servers (file transfer protocol) (εξυπηρετητής πρωτοκόλλου μεταφοράς αρχείων)
- Proxy Server Logs (αρχεία καταγραφής διαδικτυακού μεσολαβητή)
- Secure Shell Servers (remote access) (απομακρυσμένη βοήθεια)
- Routers and Switches
- Chat Servers
- Intrusion Detection Systems
- DNS Servers (Domain Name System)
- Victim and Attacker Systems

1.2.3 Πληροφορίες που αποθηκεύονται στα logs.

Ο τύπος των πληροφοριών που καταγράφονται στα log records εξαρτώνται από τον τύπο της συσκευής καταγραφής. Μερικά από τα πιο διαδεδομένα είναι :



Εικόνα 3: Πληροφορία από log record

Συνήθως οι πληροφορίες αυτές περιλαμβάνουν:

- Την ταυτότητα του χρήστη που είχε πρόσβαση σε υλικό ή λογισμικό.
- Τον εξοπλισμό που χρησιμοποίηση για την πρόσβαση.
- Την ημερομηνία, την ώρα και την διάρκεια της που έκανε χρήση του υλικού ή του λογισμικού.
- Την ηλεκτρονική διεύθυνση από την οποία είχε πρόσβαση.
- Τις ενέργειες τις οποίες έκανε καθ' όλη την διάρκεια της χρήσης του υλικού ή του λογισμικού.

1.3 Η διατήρηση και λήψη των log records

Τα log records συνήθως διατηρούνται για περιορισμένο χρονικό διάστημα, το οποίο εξαρτάται από την κάθε εταιρία. Σε παλαιότερες περιπτώσεις, ορισμένες εταιρίες κράταγαν τα logs για μόνο μερικές μέρες, άλλες εταιρίες για κάποιες μόνο βδομάδες ενώ άλλες δεν κράταγαν αρχεία με όλων των τύπων τις καταγραφές.

Λόγω λοιπόν της μικρής διάρκειας των log records είναι αναγκαίο να βρεθούν άλλα μέρη όπου θα μπορούν να καταγραφούν οι ίδιες ή παρόμοιες πληροφορίες. Ας υποθέσουμε ότι ένας εργαζόμενος μιας εταιρίας ήταν ύποπτος για την αποστολή ευαίσθητων δεδομένων σε κάποιον απομακρυσμένο χώρο αποθήκευσης μέσα στο διαδίκτυο. Τα διαδικτυακά logs (web access logs) που υπό κανονικές συνθήκες θα κατέγραφαν τις κινήσεις που πραγματοποιήθηκαν μπορεί να μην είναι εφικτά προς πρόσβαση. Αλλά αναλύοντας τα logs που κατέγραψε ο εξυπηρετητής DNS (Domain Name Service), κάποιος ερευνητής μπορεί άνετα να βρει την αρχική DNS εντολή αναζήτησης για την απομακρυσμένη σελίδα/χώρο αποθήκευσης. Αυτή η επιβεβαίωση θα βοηθούσε στην επιβεβαίωση της διαδικτυακής δραστηριότητας που πραγματοποιήθηκε και στην δημιουργία του χρονοδιαγράμματος κάθε ενέργειας.

1.4 Νομικά στάδια

Για να αποκτηθούν τα log records πρέπει αρχικά να αναγνωρισθεί τι τύπου είναι και που μπορεί να είναι αποθηκευμένα. Έπειτα θα ενημερωθούν οι πάροχοι ότι είναι αναγκαίο να τα κρατήσουν αποθηκευμένα και τελικά με κατάλληλη νομική διαδικασία να συγκεντρωθούν τα απαραίτητα log records.

Όπως έχει αναφερθεί παραπάνω, υπάρχουν πολλά είδη log records που μπορεί να κρατήσει μια εταιρία. Μετά την αναγνώριση των log records, σύμφωνα με τους κανονισμούς της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων, Εθνικής Επιτροπής Προστασίας του Απορρήτου των Επικοινωνιών , Ν.2225/1994, οι εταιρίες είναι υποχρεωμένες να διατηρούν τα logs που τους ζητήθηκαν για 90 μέρες. Η κυβέρνηση μπορεί να ζητήσει περαιτέρω παράταση για ακόμα 90 μέρες.

Μετά από την συλλογή των log records έρχεται το ερώτημα ποια νομική διαδικασία μπορεί να δικαιολογηθεί. Μέρος της απάντησης βασίζεται στο γεγονός αν τα log records έχουν κάποιο ενδιαφέρον περιεχόμενο σχετικό με την έρευνα. Σε γενικές γραμμές , το περιεχόμενο σχετικό με την διάταξη της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) αναφέρει ότι ¨..όταν χρησιμοποιείται σε σχέση με οποιαδήποτε σύνδεσμο, προφορικό ή ηλεκτρονικό και περιλαμβάνει οποιαδήποτε πληροφορία όσον αφορά την ουσία, την έννοια της επικοινωνίας…¨. Ορισμένα δικαστήρια, έχουν καταλήξει στο συμπέρασμα ότι το URL (Uniform Resource Locator) ή η διεύθυνση της σελίδας μπορεί να περιλαμβάνουν πληροφορίες.

1.5 Παραποίηση των log records

Όταν ασχολούμαστε με ηλεκτρονικά στοιχεία το ερώτημα που προκύπτει είναι αν αυτά μπορούν να παραποιηθούν. Αν και είναι δυνατό ορισμένα log records, όπως και άλλες μορφές ηλεκτρονικών στοιχείων, μπορούν να δεχτούν κάποιου είδους τροποποίησης, είναι αδύνατον όλα τα logs που έχουν καταγραφεί στην διαδρομή να περισυλλεχθούν και να αλλαχθούν διότι θα έπρεπε να υπάρχει πρόσβαση κάποιου βαθμού σε όλες τις συσκευές που τα έχουν κρατήσει, πράγμα αδύνατο.

Ας υποθέσουμε ότι ένας κακόβουλος εισβολέας, εισέβαλε σε ένα δίκτυο ή υπολογιστή μέσω διαδικτύου. Για να το καταφέρει αυτό, εισήλθε μέσα από τους εξυπηρετητές του τοίχου προστασίας, του διαδικτύου, και του διαμεσολαβητή κ.λ.π. Για να τροποποιηθούν τελείως οι

πληροφορίες που καταγράφτηκαν θα πρέπει να αλλαχθούν όλες οι εγγραφές σε όλα τα συστήματα του υπολογιστή ή του δικτύου. Πέρα από αυτό όλες οι πληροφορίες που ανταλλάχθηκαν μεταξύ του υπολογιστή του εισβολέα και του θύματος, που έχουν καταγραφεί θα πρέπει να τροποποιηθούν επίσης. Και τελικά τροποποιήσεις θα έπρεπε να δεχτούν και τα logs που κρατάνε οι πάροχοι μιας και κάθε φορά που γινόταν επιλογή ενός συγκεκριμένου σημείου ή μια αναζήτηση μέσα στο διαδίκτυο, οι εταιρίες κρατάνε log records.

Όπως φαίνεται λοιπόν και από το παράδειγμα, είναι πάρα πολλά αρχεία που πρέπει να τροποποιηθούν για να αλλάξει η δομή της δραστηριότητας που πραγματοποιήθηκε. Άρα βγαίνει το συμπέρασμα ότι είναι αδύνατο να μπορέσουν να τροποποιηθούν τα ηλεκτρονικά αρχεία σε τέτοιο βαθμό που να μην μπορούν να χρησιμοποιηθούν σαν αποδεικτικά στοιχεία σε μια δίκη. Σε περίπτωση που γινόταν ένσταση κατά την διάρκεια της δίκης, ότι τα log records που χρησιμοποιούνται σαν αποδεικτικά στοιχεία έχουν υποστεί αλλαγές, κάποιος ειδικός αναλυτής μπορεί να αποδείξει την ύπαρξη τους, συγκρίνοντας τα με άλλα log records που καταγράφηκαν από άλλες συσκευές κατά την διάρκεια της διαδρομής. Στην περίπτωση που όντως κάποιο log records τροποποιήθηκε, συγκρίνεται με κάποιο από τα υπόλοιπα που υπάρχουν στον υπολογιστή του εισβολέα ή του θύματος και εξακριβώνεται το τι είδους αλλαγές δέχτηκε το συγκεκριμένο έγγραφο.

Στο δικαστήριο, όταν σαν αποδεικτικά στοιχεία υπάρχουν ηλεκτρονικά έγγραφα τα ερωτήματα σχετικά με την αξιοπιστία των εγγραφών συνήθως φαίνεται από τα στοιχεία και τις συγκρίσεις που πραγματοποιούνται και όχι από τι μαρτυρίες των εμπλεκόμενων.

Παρακάτω ακολουθείται ένα απόσπασμα του δικαστή εν ώρα δίκης σε ένα δικαστήριο των Ηνωμένων Πολιτειών όσον αφορά την χρήση ηλεκτρονικών εγγράφων ως αποδεικτικά στοιχεία:

Ο κατηγορούμενος ισχυρίζεται ότι η αξιοπιστία αυτών των e-mails (ηλεκτρονικών μηνυμάτων) δεν μπορεί να αποδειχθεί, και συγκεκριμένα αυτά τα e-mails που βρίσκονται ενσωματωμένα μέσα σε άλλα e-mails, επειδή έχουν προαχθεί (forwarded) σε ή από άλλους χρήστες, ή έχουν σταλθεί σαν απάντηση σε ένα προ-σταλμένο μήνυμα. Το δικαστήριο απορρίπτει αυτή την κατηγορία ενάντια στην αυθεντικότητα των e-mails. Το επιχείρημα του κατηγορούμενου θα πρέπει να τείνει ως προς τον τρόπο που το δικαστήριο θα αξιολογήσει τα αποδεικτικά στοιχεία και όχι ως προς την αυθεντικότητα των στοιχείων. Ενώ ο κατηγορούμενος έχει δίκιο όσον αφορά ότι τα προ-σταλμένα μηνύματα που έχουν σταλθεί και έχουν λάβει απάντηση μπορεί να έχουν τροποποιηθεί, αυτό ούτως ή άλλως δεν είναι συγκεκριμένο για τα αποδεικτικά στοιχεία των e-mails. Το ίδιο μπορεί να γίνει και σε χειρόγραφα έγγραφα θεωρούνται αποδεικτικά στοιχεία, όπως γράμματα, τιμολόγια ή συμβόλαια, τα οποία μπορούν να τροποποιηθούν με την βοήθεια των νέων τεχνολογιών ή με φωτοτυπίες, διορθωτικό ή πλαστογραφία. Η πιθανότητα λοιπόν, της τυχόν τροποποίησης του ηλεκτρονικού εγγράφου δεν μπορεί να το αποκλείσει ως πηγή αποδείξεων, όπως δεν αποκλείονται τα χειρόγραφα έγγραφα ως αποδεικτικά στοιχεία, γιατί έχουν την ίδια πιθανότητα τροποποίησης. Ζούμε σε μια εποχή που οι ηλεκτρονικοί υπολογιστές έχουν εισβάλει στην καθημερινότητα μας και οι ανταλλαγή ηλεκτρονικών μηνυμάτων αποτελεί σύνηθες φαινόμενο, οπότε δεν μπορεί να υπεξαιρεθεί από κανένα τομέα. Ο κατηγορούμενος μπορεί να θέσει αυτό το ζήτημα ως θέμα συζήτησης εν ώρα δίκης ωστόσο τα μη-επαρκή στοιχεία ότι όντως υπήρχε τροποποίηση στο ηλεκτρονικό μήνυμα δεν θα το θέσει εκτός εξέτασης μιας και υπάρχει μεγάλη πιθανότητα όλες αυτές οι δραστηριότητες όντως να είχαν πραγματοποιηθεί και να μην είναι πλαστές.

1.6 Ανάλυση των log records.

Το πρωταρχικό στάδιο για την ανάλυση των log records είναι η περισυλλογή των δεδομένων από κάθε είδους συσκευή που τα έχει καταγράψει. Μαζί με αυτά συλλέγονται και όσες πληροφορίες

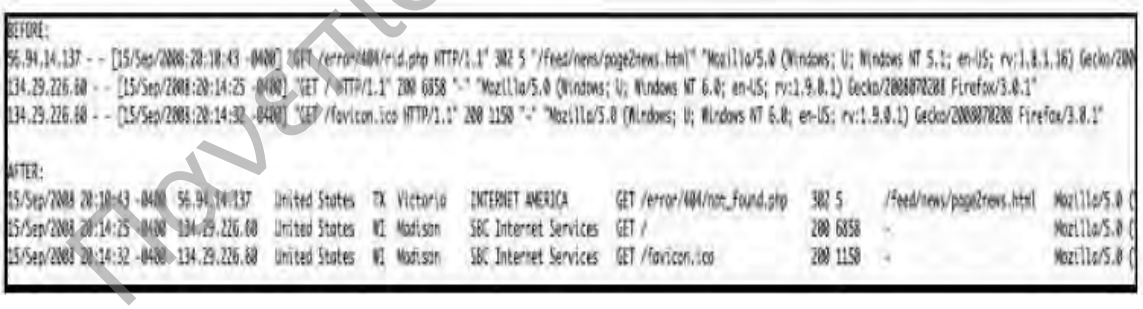
είναι σχετικές με την υπόθεση των log records , μέσα από τον υπολογιστή η τον σκληρό δίσκο για να μπορέσει να γίνει η ταυτοποίηση των δύο πηγών.

Η συλλογή μόνο των αρχείων που μπορούν να βρεθούν μέσα σε έναν υπολογιστή ή τον σκληρό δίσκο δεν επαρκούν για να βγει κάποιο πόρισμα, όπως και η συλλογή μόνο μερικών log records δεν είναι αξιόπιστη. Η πρόκληση όσον αφορά τα αρχεία από τους υπολογιστές, εμφανίζεται στο ότι πρέπει να βρεθούν γρήγορα ποια στοιχεία σχετίζονται με την υπόθεση και να συλλεχθούν πριν σβηστούν ή αντικατασταθούν από άλλα. Ο ερευνητής χρειάζεται την βοήθεια ειδικού αναλυτή για να μπορέσει να ψάξει όχι μόνο στον σκληρό αλλά και στο διαδίκτυο σε μέρη που μπορεί να έχουν αποθηκευτεί χρήσιμα δεδομένα.

Η συλλογή στιγμιότυπων της ίδιας δραστηριότητας από διάφορες συσκευές ή συστήματα καθιστούν την έρευνα πιο αξιόπιστη. Για παράδειγμα, η εντολή που κάνει κάποιος για να εισέλθει σε έναν πάροχο ηλεκτρονικών μηνυμάτων όπως το Gmail, μπορεί να φανεί από αρχεία που καταγράφτηκαν στον εξυπηρετητή της Gmail και στον μεσολαβητή επικοινωνίας (proxy server). Αυτή η ταύτιση των ίδιων κινήσεων από διαφορετικά συστήματα δείχνει την αυθεντικότητα των στοιχείων, γιατί μιας και έχουν ελέγχει και επιβεβαιωθεί από μια αρχή μπορούν να αξιοποιηθούν στην δίκη.

Το δεύτερο βασικό στάδιο που πρέπει να πραγματοποιηθεί μετά την συλλογή και ταυτοποίηση των στοιχείων είναι η διαδικασία φιλτραρίσματος των δεδομένων. Στην συνέχεια ακολουθεί η αποκωδικοποίηση και ο έλεγχος των μετα- δεδομένων (metadata). Για παράδειγμα, πολλές φορές η συλλογή αρχείων γίνεται από logs που έχουν καταγραφεί σε διαφορετικές χώρες και άρα υπάρχει μια διαφορά στην ώρα. Με το φιλτράρισμα συγχωνεύονται όλα αυτά τα δεδομένα σε ένα χρονοδιάγραμμα κοινής ώρας και έτσι ολοκληρώνεται η διαδρομή της αναζήτησης. Πέρα από την ώρα με τον έλεγχο των μετα-δεδομένων, μπορούν αν αποκωδικοποιηθούν και κρυφές πληροφορίες, όπως την γεωγραφική περιοχή από όπου προέρχεται η διεύθυνση IP, πληροφορίες ISP κ.λ.π.

Όλα αυτά τα δεδομένα είναι κρυμμένα σε αρχεία πολλών γραμμών κώδικα και πληροφοριών και έτσι χρειάζονται γρήγορα και έξυπνα μηχανήματα για να πραγματοποιήσουν την αναζήτηση με κάποια φίλτρα. Πέρα από αυτό όμως χρειάζονται και ειδικοί γνώμονες κάποιας script γλώσσας (Perl, Python) για να μπορούν να αναγνωρίσουν τα στοιχεία που τους βγάζει το πρόγραμμα.



Εικόνα 4: μετα-δεδομένα

Το τμήμα “after” των μετα-δεδομένων δίνει στοιχεία που μπορούν να αποκαλύψουν τις κινήσεις που πραγματοποιήθηκαν. Στην πρώτη γραμμή μετά το “after” φαίνεται η ακριβής ημερομηνία και ώρα που έγινε μια συγκεκριμένη αναζήτηση (September 15, 2008 at 20:10:43), η

διεύθυνση IP από τη οποία έγινε η αναζήτηση, γεωγραφική περιοχή και πληροφορίες ISP σχετικές με την IP.

1.7 Ανάλυση

Η ανάλυση των στοιχείων των logs πραγματοποιείται με τρόπο σχετικό με την περίπτωση που εξετάζεται. Σε κάθε log είναι αποθηκευμένες πάρα πολλές πληροφορίες οπότε ο αναλυτής θα πρέπει να είναι εξειδικευμένος για να μπορέσει να βρει τις πληροφορίες που χρειάζεται πριν ξεκινήσει να ψάχνει πιο βαθιά στο θέμα.

Μερικές από τις ερωτήσεις που θα πρέπει να απαντηθούν πριν γίνει η έρευνα είναι :

- Τι είδους σύστημα καταχώρησε τα δεδομένα ?
- Τι είδους log records χρησιμοποιούνται ?
- Από ποια πεδία καταχωρήθηκαν δεδομένα και πώς ορίζονται ?
- Πώς σχετίζονται μεταξύ τους τα δεδομένα ? Ανήκουν στο ίδιο δίκτυο, προέρχονται από τον ίδιο εισβολέα ή αν τα στοιχεία προέρχονται από το ίδιο θύμα ?

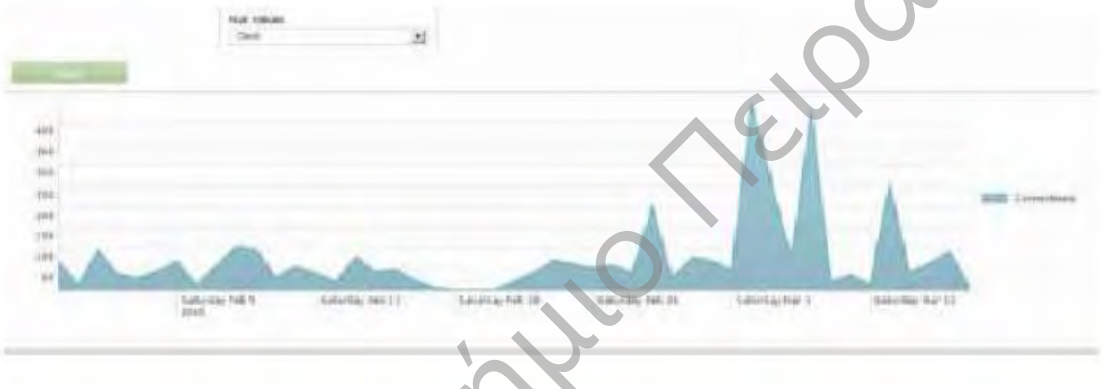
Χρησιμοποιώντας γενικές στατιστικές ο αναλυτής μπορεί να αναλύσει τα δεδομένα που βρήκε. Με την ανάλυση εξ αρχής μπορεί να εξακριβωθεί από την αρχή η οποιαδήποτε ύποπτη δραστηριότητα πραγματοποιήθηκε και να γίνει περισσότερο αντιληπτή όταν η ανάλυση γίνει βαθύτερη. Μερικές από τις πληροφορίες που μπορεί να διαπιστώσει ο αναλυτής μέσα από την στατιστική έρευνα είναι :

- Συνηθισμένη περίοδος στην μέρα που γίνονται οι επιθέσεις
- Είδους συνηθισμένων επιθέσεων
- Αυτοματοποιημένες ή επι τόπου επιθέσεις
- Υπογραφές γνωστών προγραμμάτων επιθέσεων

Εικόνα 5: στατιστική ανάλυση δεδομένων

Το επόμενο στάδιο είναι η βαθύτερη ανάλυση των δεδομένων. Είναι απαραίτητη η χρήση προγραμμάτων που επιτρέπουν την περιήγηση του αναλυτή στα διάφορα τμήματα των πληροφοριών που έχουν καταγραφεί για να μπορεί να τα αξιολογήσει. Το βασικότερο εργαλείο της βαθύτερης ανάλυσης είναι ότι δεν επιτρέπει στον αναλυτή να χαθεί μέσα στις αράδες των πληροφοριών που δεν είναι σχετικές με την υπόθεση που εξιχνιάζεται.

Παρακάτω φαίνεται ένα πρόγραμμα που ονομάζεται Splunk και βοηθάει τους αναλυτές να περιηγηθούν μέσα στα log records. Αυτό που κάνει είναι να δημιουργεί ένα γράφημα που ακολουθεί την χρονοσειρά που έγιναν οι διάφορες ενέργειες και να δημιουργεί κορυφές στις στιγμές που παρουσιάζεται μεγάλη δραστηριότητα.



Εικόνα 6: Splunk – πρόγραμμα βαθύτερης ανάλυσης log records

1.8. Συσχέτιση log records

Η φάση της συσχέτισης περιλαμβάνει την σύγκριση και επιβεβαίωση των κοινών αρχείων ή της δραστηριότητας σε διαφορετικά αρχεία καταγραφής ή σε αρχεία του υπολογιστή. Για παράδειγμα , τα log records μπορούν να δείξουν ότι ένας χρήστης ξεκίνησε να κάνει μια αναζήτηση μέσα από ένα δίκτυο κοινωνικής δικτύωσης, χρησιμοποιώντας ένα proxy για να αποκρύψει το σημείο προέλευσης της αναζήτησης και τελικά πραγματοποίησε μη-εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο υπολογιστών. Τα logs που καταχωρήθηκαν στον υπολογιστή του θύματος μπορούν να συσχετιστούν με τα log records της proxy εταιρίας και αυτά της σελίδας κοινωνικής δικτύωσης. Αυτή η συσχέτιση μπορεί να φέρει στο φως χρήσιμες πληροφορίες ως προς το που θα πρέπει να οδηγηθεί η έρευνα και τι είδους σχέσεις εντοπίζονται. Η συσχέτιση μπορεί ακόμα να χρησιμοποιηθεί και σαν αποδεικτικό στοιχείο στην δίκη μιας και η δραστηριότητα επιβεβαιώνεται από πολλές διαφορετικές μη συσχετιζόμενες εταιρίες .

1.9. Σύνταξη δικαστικής αναφοράς

Στο στάδιο της αναφοράς θα πρέπει να γραφτούν η ανάλυση και τα συμπεράσματα που προέκυψαν συνοδευόμενα από τα στοιχεία που χρησιμοποιήθηκαν. Αυτή η αναφορά θα χρησιμοποιηθεί για την δικαστική απόφαση και για να καλύψει τις προ-ανακριτικές απαιτήσεις του νόμου περί της Σύμβασης κατά του Εγκλήματος μέσω του Διαδικτύου (Κυρωτικός) Νόμος του 2004 -22(III)/2004.

Η σύνταξη της αναφοράς είναι ένα θέμα περίπλοκο εξίσου σημαντικότητας όσο και αυτό της ανάλυσης. Ο τεχνικός αναλυτής θα πρέπει να γράψει τα συμπεράσματα που έβγαλε και τα βήματα που ακολούθησε με τρόπο κατανοητό για άτομα που δεν γνωρίζουν τίποτα σχετικά με τις αναλύσεις ηλεκτρονικών αποδεικτικών στοιχείων. Η αναφορά θα πρέπει να αναφέρεται στα αρχικά ευρήματα και στην αιτιολόγηση των βημάτων και των τελικών αποτελεσμάτων.

Σύμφωνα με τις προ-ανακριτικές υποχρεώσεις, ο δικαστικός υπάλληλος μετά από αίτηση του κατηγορούμενο, πρέπει να παραχωρήσει στον δεύτερο την αναφορά με τα ευρήματα που θα χρησιμοποιηθούν στην δίκη κάτω από τους νόμους του 2004 -22(III)/2004 περί Εγκλήματος μέσω Διαδικτύου (συγκεκριμένα Ν.3115/2003 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών). Πέρα από την αναφορά θα πρέπει να του δοθεί και αντίγραφο της περιγραφής της άποψης του μάρτυρα της δίκης, τους λόγους που τον οδήγησαν στην συγκεκριμένη άποψη και τα στοιχεία που έχει καθώς και τα προσόντα του μάρτυρα , δηλαδή κατά πόσο συμπίπτουν με την υπόθεση.

Στην αναφορά θα καταγράφεται μεταξύ των άλλων, και τι είδους log records ή μέσα χρησιμοποιήθηκαν για την ανάλυση των δεδομένων. Επίσης μέσα στα συμπεράσματα θα πρέπει να αναγράφονται όλες οι δραστηριότητες που εντοπίστηκαν, η μεταφορά δεδομένων, οι ιστοσελίδες που καταγράφτηκαν και όλων των ειδών οι επικοινωνίες που ήταν καταγεγραμμένες μέσα στα log records. Σημαντικό επίσης είναι να βρίσκεται μέσα στην αναφορά και το χρονοδιάγραμμα δραστηριοτήτων που εξακριβώθηκε από την ανάλυση των διάφορων logs που ανακτήθηκαν από τα διάφορα συστήματα. Στην περίπτωση που στην δικαστική απόφαση θα χρησιμοποιηθούν και δεδομένα τα οποία είχαν σβηστεί από τον σκληρό δίσκο του κατηγορούμενου αλλά καταγράφηκαν από άλλες συσκευές, ο τεχνικός αναλυτής θα πρέπει να τα συμπεριλάβει μέσα στην αναφορά του. Όλα αυτά βεβαίως θα πρέπει να συνοδεύονται από τους πίνακες και τα γραφήματα που προέκυψαν από την ανάλυση και να αναφέρονται και στα αρχικά ευρήματα.

1.10 Πρόσφατες δικαστικές περιπτώσεις

Η σημαντικότητα της χρήσης των log records στην διεξαγωγή ερευνών μπορεί να φανεί μέσα από πρόσφατες ποινικές περιπτώσεις. Οι περισσότερες ασχολούνται με δραστηριότητα σε λογαριασμούς e-mail, στην αποστολή και διαγραφή πληροφοριών στο διαδίκτυο, εύρεση πληροφοριών για τον χρήστη και τέλος διακρατικές εμπορικές δραστηριότητες.

1.10.1. E-mails

Τα log records που καταγράφονται σε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου μπορούν να αποκαλύψουν την δραστηριότητα που πραγματοποιήθηκε, όπως ποιες σε ποιες περιοχές εισήλθε ο χρήστης ή αν στάλθηκε κάποιο e-mail κατά την διάρκεια παραμονής του στην ταχυδρομική του θυρίδα. Άλλου τύπου logs όμως που καταγράφονται από τον πάροχο του e-mail

και αποθηκεύει πληροφορίες που αφορούν ποιες IP διευθύνσεις είχαν πρόσβαση στον λογαριασμό συγκεκριμένη ώρα και μέρα, δεν αποκαλύπτουν τις παραπάνω πληροφορίες.

Ας υποθέσουμε ένα σενάριο στο οποίο κάποιος χρήστης στέλνει κάποιο e-mail μέσα από μια διαδικτυακή θυρίδα αποστολής μηνυμάτων όπως τα Gmail, Hotmail ήYahoo! Τα web access logs που θα καταχωρηθούν αποθηκεύουν την πληροφορία της αποστολής και αποδοχής ηλεκτρονικών μηνυμάτων. Οι δύο παρακάτω εγγραφές δείχνουν την δραστηριότητα που πραγματοποίησε ένας χρήστης μέσα σε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου. Αρχικά επισκέφτηκε την διαδικασία δημιουργίας μηνύματος (compose) και έπειτα έστειλε ένα μήνυμα.

IP Address	Status Code	HTTP Method	Uniform Resource Identifier (URI)
113.23.10.11	200	GET	http://us.mc1100.mail.yahoo.com/mc/compose?..
113.23.10.11	200	POST	http://us.mc1100.mail.yahoo.com/mc/compose?...

Εικόνα 7: Log Records

Όπου :

- IP Address : Η IP από όπου ξεκίνησε η δραστηριότητα.
- Status code : το αποτέλεσμα της ζήτησης. Το «200» δείχνει ότι ο διαδικτυακός εξυπηρετητής ολοκλήρωσε με επιτυχία την διαδικασία.
- HTTP Method : η διαδικασία HTTP που στάλθηκε στον διαδικτυακό εξυπηρετητή. Το GET είναι η έναρξη της διαδικασίας δημιουργίας του e-mail, ενώ το POST είναι η αποστολή του μηνύματος
- URI : η αποστολή του περιεχομένου που ζήτησε ο χρήστης, στην συγκεκριμένη περίπτωση είναι το άνοιγμα παραθύρου για την εγγραφή ενός νέου μηνύματος.

Οπότε βάση των παραπάνω πληροφοριών φαίνεται ότι ο χρήστης εισήλθε στον λογαριασμό του και αφού δημιούργησε ένα e-mail το έστειλε. Αν και οι πληροφορίες βρίσκονται αποθηκευμένες σε κάποιο εξωτερικό μέρος μακριά από τον υπολογιστή, σε περίπτωση έρευνας θα βοηθήσουν στην εξιχνίαση της υπόθεσης.

1.10.2. Αποστολή και διαγραφή περιεχομένου στο διαδίκτυο

Η ανάλυση των log records μπορούν να εξακριβώσουν και την δραστηριότητα που πραγματοποίησε ο χρήστης για να στείλει ή να σβήσει κάποιες πληροφορίες από το διαδίκτυο. Για να γίνει κατανοητή η όλη διαδικασία θα πρέπει να δούμε πώς λειτουργεί το διαδίκτυο. Οι χρήστες κάθονται πίσω από μια οθόνη και βλέπουν δυναμικό περιεχόμενο στις σελίδες που επισκέπτονται, το περιεχόμενο αυτό το έχουν στείλει κάποιοι άλλοι χρήστες από τον υπολογιστή τους. Συνήθως γίνονται αιτήματα επικοινωνίας μεταξύ των συστημάτων και των υπολογιστών χωρίς να πρέπει να ενεργήσουν καθόλου οι χρήστες. Κάθε φορά που μοιράζεται περιεχόμενο στο διαδίκτυο, οι εξυπηρετητές που χρησιμοποιήθηκαν μέσα στην διαδρομή αποστολής καταχωρούν και ένα log record . Αυτά τα logs μπορούν να μας ενημερώσουν για το είδος αναζήτησης που

πραγματοποιήθηκε, από ποια σελίδα ή πηγή παράχθηκε το περιεχόμενο που στάλθηκε, πληροφορίες σχετικές με το σύστημα που έστειλε το αίτημα και το αποτέλεσμα του αιτήματος. Οποιαδήποτε αλλαγή και αν πραγματοποιηθεί σε κάποια διαδικτυακή σελίδα καταχωρείται σε ένα log.

1.10.3. Μοναδικά αναγνωριστικά στοιχεία

Το βασικότερο σε μια έρευνα είναι ο εντοπισμός του χρήστη του υπολογιστή. Τα log records περιέχουν σημαντικές πληροφορίες όσον αφορά τον χρήστη. Μερικές από τις βασικότερες είναι η διεύθυνση IP που χρησιμοποίησε άρα και ο εντοπισμός της περιοχής από όπου ξεκίνησε η δραστηριότητα. Πέρα από αυτό στα logs μπορούν να καταγραφούν και το υλικό και λογισμικό του συγκεκριμένου υπολογιστή. Αυτές οι πληροφορίες συνήθως καταχωρούνται από τον διαδικτυακό εξυπηρετητή (web server):

```
Mozilla/5.0 (BlackBerry; U; BlackBerry 9800; zh-TW) AppleWebKit/534.8+ (KHTML, like Gecko)
Version/6.0.0.448 Mobile Safari/534.8+
```

Εικόνα 8: web server log record

Το παραπάνω μας δείχνει τα εξής στοιχεία:

- Ο χρήστης χρησιμοποιεί ένα Blackberry με λογισμικό Blackberry OS version 6.0.0.448.
- πάροχος του χρήστη χρησιμοποιεί σαν γλώσσα (zh-TW – Chinese –Taiwan)
- Έγινε χρήση του Safari- browser
- AppleWebKit τύπου 534.8[3]

1.11. Συμπεράσματα

Όπως φαίνεται και από τα παραδείγματα, τα log records μπορούν να αποτελέσουν σημαντικά αποδεικτικά στοιχεία σε μια έρευνα ή μια δίκη. Άλλοι τύποι δεδομένων δεν είναι τόσο χρήσιμοι όσο τα log records διότι καταγράφουν σχεδόν κάθε δραστηριότητα που πραγματοποιείται και είναι δύσκολο να τροποποιηθούν, άρα είναι αξιόπιστα. Οι ισχυρισμοί για τυχόν παραποίηση των

[3] M. Krotoski, J. Passwaters, Using log record analysis to show internet and computer activity in criminal classes, σελ 16 - 34, διαθέσιμο στο http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf

log records είναι αβάσιμοι διότι με την διαδικασία της συσχέτισης από διαφορετικά log άλλων εταιριών και συσκευών μπορεί να ταυτοποιηθεί η δραστηριότητα και τα βήματα που ακολούθησε. Τα logs μπορούν επίσης να καλύψουν το κενό, εκεί που δεν υπάρχουν αρχεία λόγω απώλειας ή καταστροφής. Οπότε ουσιαστικά αποτελούν ένα αξιόπιστο σύνολο αποδεικτικών στοιχείων πάνω στο οποίο μπορεί να βασιστεί μια ολόκληρη έρευνα ή ποινική δίκη.

ΚΕΦΑΛΑΙΟ 2: ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΠΡΙΝ ΚΑΙ ΚΑΤΑ ΤΗ ΔΙΚΗ

2.1 Ηλεκτρονικά Αποδεικτικά Στοιχεία

Τα ηλεκτρονικά αποδεικτικά στοιχεία παρέχουν μοναδικές πληροφορίες που μπορεί να μην είναι διαθέσιμες με άλλο τρόπο αφού τα ηλεκτρονικά αρχεία περιλαμβάνουν συνήθως ένα ικανό πλήθος μεταδεδομένων. Η ηλεκτρονική έκδοση συλλαμβάνει πολλές λεπτομέρειες που μπορεί διαφορετικά να μην ήταν διαθέσιμες. Τα μετα-δεδομένα της ηλεκτρονικής έκδοσης που μπορεί να αναφέρουν το όνομα του συγγραφέα και του τίτλου, την ημερομηνία δημιουργίας και τελευταίας αποθήκευσης και την ημερομηνία της τελευταίας έντυπης μορφής, οι αλλαγές που πραγματοποιήθηκαν καθώς και πλήθος άλλων εξειδικευμένων πληροφοριών. Τα ηλεκτρονικά αποδεικτικά στοιχεία χρησιμοποιούνται ευρέως τόσο σε αστικές όσο σε ποινικές υποθέσεις κυρίως μετά από το 2006 όταν και καθορίστηκαν νέοι κανόνες σχετικά με τις ηλεκτρονικές πληροφορίες. Έτσι γίνονται ολοένα και πιο απαραίτητα για τη διερεύνηση, την κατασκευή, και για την επίλυση πολλών ποινικών υποθέσεων. Προκειμένου να καθοριστεί ο τρόπος με τον οποίο μπορεί να γίνει η εκμετάλλευση των ηλεκτρονικών αποδεικτικών στοιχείων χρειάζεται να προσδιοριστεί το τι νοείται ως ηλεκτρονικό έγγραφο καθώς και το ποιες είναι οι προδιαγραφές του.

2.2 Έννοια του ηλεκτρονικού εγγράφου

Υπό μία έννοια ως ηλεκτρονικό έγγραφο θεωρείται ως ηλεκτρονικό έγγραφο

νοείται «κάθε έγγραφο του οποίου η υπογραφή παράγεται (εξ ολοκλήρου ή απλώς αποτυπώνεται) με τη βοήθεια της ηλεκτρονικής τεχνολογίας». Σύμφωνα με τον ορισμό αυτό μπορεί να γίνει διάκριση των ηλεκτρονικών εγγράφων σε:

- γνήσια ηλεκτρονικά έγγραφα (ή ηλεκτρονικά έγγραφα με στενή έννοια), τα οποία έχουν εξ' ολοκλήρου ηλεκτρονική υπόσταση, δηλαδή καταχωρήσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό (π.χ. σκληρός δίσκος, δισκέτα, zip, cd κ.λπ.)
- μη γνήσια ηλεκτρονικά έγγραφα, τα οποία είναι έγχαρτα με περιεχόμενο και υπογραφή ηλεκτρονικά αποτυπωμένη σ' αυτά (π.χ. το fax και το telex)[4].

Κατά έναν άλλο ορισμό, ηλεκτρονικό έγγραφο συνιστούν «το σύνολο των δεδομένων τα οποία, αφού εγγραφούν στο μαγνητικό δίσκο ενός Η/Υ και γίνουν αντικείμενο ηλεκτρονικής επεξεργασίας από την κεντρική μονάδα, αποτυπώνονται εν συνεχεία, με βάση τις εντολές του προγράμματος, κατά τρόπο αναγνώσιμο από τον άνθρωπο είτε στην οθόνη του μηχανήματος είτε στον προσαρτημένο εκτυπωτή»[5]. Κατά αυτόν τον ορισμό το ηλεκτρονικό κείμενο είναι περιεχόμενο το οποίο μπορεί να εμφανίζεται στην οθόνη ηλεκτρονικού υπολογιστή και το οποίο δύναται να εκτυπωθεί ή να αποσταλλεί ηλεκτρονικά. Κατά το άρθρο 444 αρ. 3 και το άρθρο 448

[4] Χριστοδούλου, Κ.. Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία.

[5] Σ. Κουσούλης, Σύγχρονες μορφές έγγραφης συναλλαγής, 1992

παρ. 2 ΚΠολΔ, κάθε ηλεκτρονικό έγγραφο αποτελείμηχανική απεικόνιση η οποία συνιστά πλήρη απόδειξη, δεκτική ανταποδείξεως για τα γεγονότα ή πράγματα που αναφέρονται σε αυτή. Αυτό που χρήζει διερεύνησης είναι αν ενέχει την ιδιότητα ιδιωτικού εγγράφου δηλαδή αν δύνται να έχει πλήρη αποδεικτική δύναμη εκπορευόμενης από την πιστοποίηση της προελευσής του από σαφώς προσδιορισμένου εκδότη, δεδομένού ότι η ιδιοχειρη υπογραφή (απαιτητή βάση του 443 ΚΠολΔ) αντικαθίσταται από μηχανικό ισοδύναμο. Δεν πληρεί τις προδιαγράφες του επί χάρτου αποτυπωμένου εγγράφου καθώς δεν μπορεί παρέχει σταθερότητα κατά την ενσωματωσή του σε υλικό με μεγάλη διάρκεια ζωής. Ωστόσο παίζει τον ρόλο μίας ενδιάμεσης μορφής που μπορεί να εξομοιωθεί με τα ιδιωτικά έγγραφα. Ένα ισχυρό παράδειγμα είναι η αποστολή αρχείων ή/και κειμένων με την χρήση του ηλεκτρονικού ταχυδρομείου. Ο αποστολέας προσδιορίζεται μοναδικά από την διεύθυνηση ηλεκτρονικού ταχυδρομείου που του παραχορήθηκ να χρησιμοποιεί από έναν πάροχο συναφών υπηρεσιών οπότε η ταύτιση του με φυσικό πρόσωπο έγκειται στην πολιτική που ακολουθεί ο πάροχος για την διευθυνσιοδότηση (αν δηλαδή ο πάροχος απαιτεί από τον πελάτη την φυσική του ταυτοποίηση για την απόδοση δειυθυνσης ηλεκτρονικού ταχυσρομείου). Στην περίπτωση αυτή το θέμα της γνησιότητας του ηλεκτρονικού εγγραφού μεταπίπτει στο κατά πόσο ο αποστολέας είναι αυτό που φαίνεται να είναι όπου εμπίπτει πλέον στις διατάξει πέρι πλαστότητας (460 επ. ΚΠολΔ) μεταβιβάζοντας το βάρος αποδείξεως σε αυτόν που επικαλέιται την πλαστοπροσωπία[6].

2.2 Υπογραφή Ψηφιακών Εγγράφων

2.2.1 Τεχνική Περιγραφή των Ψηφιακών Υπογραφών

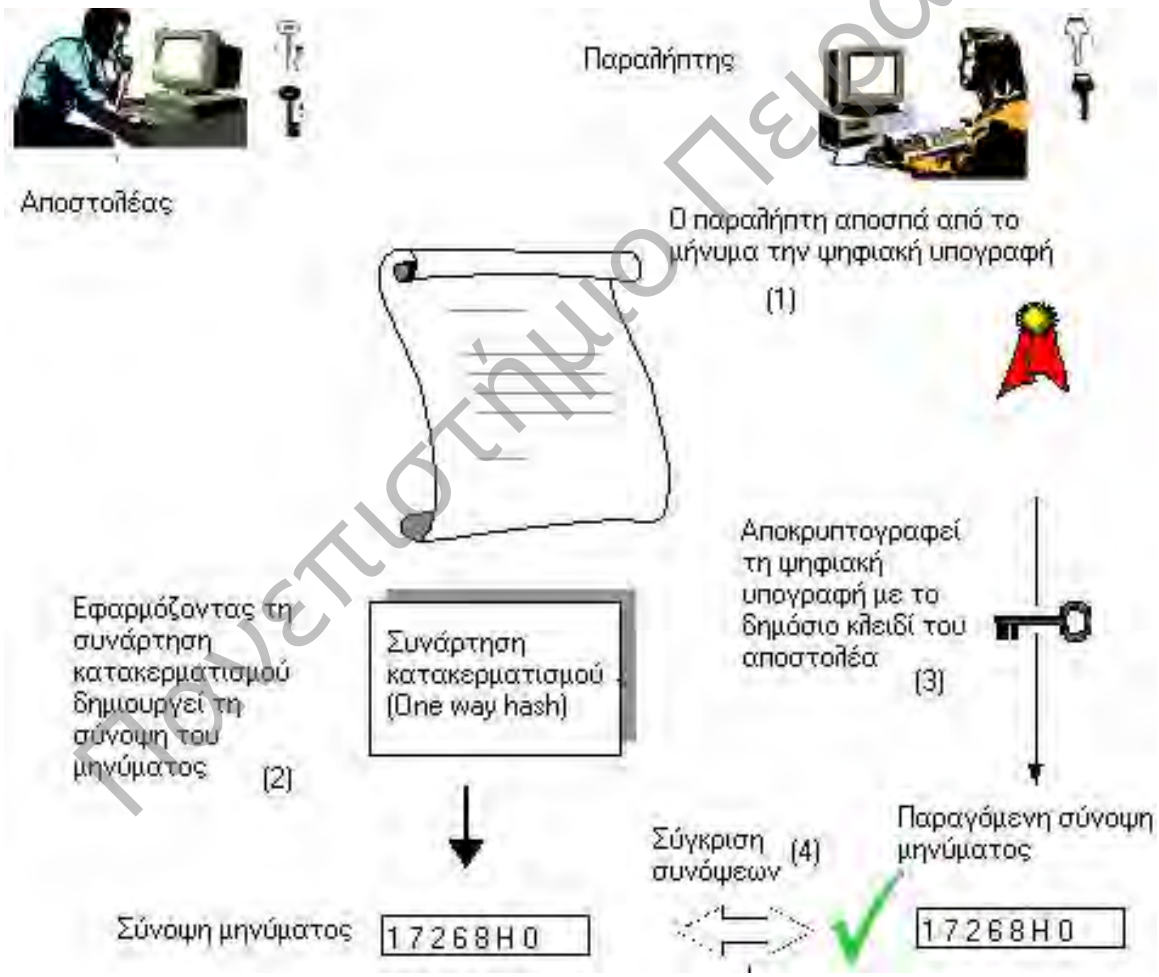
Η ψηφιακή υπογραφή πιστοποιεί στον παραλήπτη ότι ο αποστολέας είναι αυτός που υποστηρίζει ότι είναι όταν ο πρώτος πρέπει να είναι σίγουρος ότι τα στοιχεία του λαμβάνονται από την οντότητα που πιστεύει ότι επικοινωνεί μαζί της. Η χρήση των ψηφιακών υπογραφών βασίζεται στην κρυπτογραφία δημοσίου κλειδιού. Η διαδικασία αποστολής και λήψης ψηφιακά υπογεγραμμένων εγγράφων περιγράφεται ως εξής: Ο χρήστης διαθέτει δύο κλειδιά, το δημόσιο και το ιδιωτικό, τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής χρησιμοποιείται μία one-way συνάρτηση με την εφαρμογή της οποία σε ένα μήνυμα, παράγεται η σύνοψή του, η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους. Η σύνοψη του μηνύματος είναι μία μοναδική ψηφιακή αναπαράσταση του μηνύματος από το οποίο είναι υπολογιστικά αδύνατον με κάποιον τρόπο να αναπαραχθεί το αρχικό μήνυμα ενώ και η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι μικρή. Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης. Η ηλεκτρονική υπογραφή, αποτελεί την κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δεδομένου ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη

[6] Δ. Μανιώτης, Η ψηφιακή υπογραφή ως μέσο διαπίστωσης της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο, 1998

δημιουργία της υπογραφής και την επαλήθευσή της. Οι ενέργειες αποστολέα και παραλήπτη περιγράφονται παρακάτω:

- Αποστολέας: Χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Με το ιδιωτικό του κλειδί, κρυπτογραφεί τη σύνοψη. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται
- Παραλήπτης: Αποσπά από το μήνυμα την ψηφιακή υπογραφή και εφαρμόζει στο μήνυμα τον ίδιο αλγόριθμο κατακερματισμού ώστε να δημιουργήσει την σύνοψη του μηνύματος, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος. Αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος και συγκρίνεται η προκύπτουσα σύνοψη με αυτήν που έλαβε από τον αποστολέα.

Στην επόμενη εικόνα φαίνεται σχηματικά η διαδικασία ψηφιακής υπογραφής ηλεκτρονικών εγγράφων.



Εικόνα 9: Διαδικασία Ψηφιακής Υπογραφής

Για την διασφάλιση της όλης διαδικασίας είναι απαραίτητη η χρήση ψηφιακών πιστοποιητικών. Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε. Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία έμπιστη τρίτη οντότητα που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί. Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει. Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο[7].

2.2.2 Υπογραφή Ψηφιακών Εγγράφων

Η υπογραφή των ηλεκτρονικών εγγράφων μπορεί να γίνει με ασφάλεια με την χρήση της προηγμένης ηλεκτρονικής υπογραφής όπως αυτή ορίζεται στο ΠΔ 150/2001. Σύμφωνα με αυτό ηλεκτρονική υπογραφή χαρακτηρίζονται δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Κατά αυτήν την έννοια ηλεκτρονική υπογραφη μπορει να είναι εικόνα της χειρογταφής υπογραφής που είναι επικολλημένη σε ηλεκτρονικό έγγραφο ή η ηλεκτρονική δειυθυνης του αποστολέα του εγγράφου. Οι προηγμένες ηλεκτρονικές υπογραφές αποτελούν περισσότερο σαφές εργαλείο για την πιστοποίηση τους

[7] Δ. Πουλάκης, Κρυπτογραφία, 2004

εκδότη καθώς διαφέρουν από τις απλές ψηφιακές υπογραφές από το γεγονός ότι παράγονται από ισχυρούς κρυπτογραφικούς αλγορίθμους που τις καθιστούν ανθεκτικές σε προσπάθειες πλαστογράφησης. Το ΠΔ καθορίζει ως προηγμένη ψηφιακή υπογραφή ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:

- συνδέεται μονοσήμαντα με τον υπογράφοντα,
- είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος,
- δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και
- συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Ως υπογράφων χαρακτηρίζεται το φυσικό ή νομικό πρόσωπο, που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε στο δικό του όνομα είτε στο όνομα άλλου φυσικού ή νομικού προσώπου ή φορέα ενώ τα δεδομένα δημιουργίας υπογραφής μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής με μία διάταξη δημιουργίας υπογραφής (διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής). Για την παραγωγή της ψηφιακής υπογραφής είναι αναγκαία η ύπαρξη αναγνωρισμένου πιστοποιητικού το οποίο στην ουσία αποτελεί ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του και θα πρέπει κατ' ελάχιστο να πληροί τις ακόλουθες προδιαγραφές:

- ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό
- τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος, στο οποίο είναι εγκατεστημένος,
- το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο,
- πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό
- δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος,
- ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού,
- τον κωδικό ταυτοποίησης του πιστοποιητικού
- την προηγμένη ηλεκτρονική υπογραφή του παρόχου των υπηρεσιών πιστοποίησης που το εκδίδει,
- τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού,
- τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

Οι παραλήπτες των ψηφιακά υπογεγραμμένων εγγράφων μπορούν να επαληθεύουν την γνησιότητά τους με τα δεδομένα επαλήθευσης υπογραφής, τα οποία μπορεί να είναι κώδικες, ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής μέσω κατάλληλη διάταξης επαλήθευσης (διατεταγμένο υλικό ή λογισμικό, που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής). Οι προηγμένες ηλεκτρονικές υπογραφές συναντούν με μεγάλη ακρίβεια τις απαιτήσεις για πιστοποίηση του εκδότη δηλαδή την γνησιότητα του εγγράφου την ακεραιότητα του, την εμπιστευτικότητα του και την μη αποποίηση της ευθύνης του εκδότη. Κύριο χαρακτηριστικό

των προηγμένων ηλεκτρονικών υπογραφών είναι το ότι δεν αλλοιώνουν το κείμενο, σχετίζονται λογικά με αυτό αλλά και τον εκδότη του με τρόπο τέτοιο ώστε οποιαδήποτε επέμβαση σε αυτό μετά την υπογραφή του να μην είναι δυνατό να αποκρύπτεται.

Κατόπιν των παραπάνω η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρής υπογραφής. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων είναι η αρμόδια αρχή για την συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής ή δημόσιοι και ιδιωτικοί φορείς που ορίζονται από αυτήν. Οι πάροχοι υπηρεσιών πιστοποίησης υπόκεινται στις διατάξεις του ν. 2472/1997 (Α 50) και του Ν. 2774/199 (287) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το ΠΔ ορίζει ρητά ότι κάθε πάροχος δύναται να συγκεντρώνει δεδομένα προσωπικού χαρακτήρα για την έκδοση πιστοποιητικών μόνο απευθείας από το ενδιαφερόμενο πρόσωπο ή κατόπιν ρητής συγκατάθεσής του και μόνο στο βαθμό που είναι απαραίτητο για την έκδοση και διατήρηση του πιστοποιητικού[8] . Τεχνικά η πιστοποίηση των εκδοτών των ηλεκτρονικών εγγράφων περιγράφεται στο Παράρτημα Β.

Έγγραφα ηλεκτρονικά υπογεγραμμένα με απλή ηλεκτρονική υπογραφή μπορεί υπό προϋποθέσεις να αποτελέσουν αποδεικτικά στοιχεία. Ένα ηλεκτρονικό έγγραφο που περιέχει μια ψηφιακή ή απλή ηλεκτρονική υπογραφή που προσάγεται ως αποδεικτικό μέσο, δεν μπορεί να απορριφθεί με μοναδική αιτιολογία ότι δεν πληροί τις προδιαγραφές μιας προηγμένης ηλεκτρονικής υπογραφής αλλά είναι στην δικαιοδοσία των δικαστών να αποφανθούν για την αποδοχή του ή όχι. Όσο η χρήση της προηγμένης ηλεκτρονικής υπογραφής δεν επεκτείνεται σε μεγαλύτερο μέρος των συναλλαγών και της αλληλογραφίας τόσο θα είναι ανάγκη να εκτιμάται η γνησιότητα των εγγράφων με άλλου είδους ηλεκτρονικές υπογραφές. Η αναγραφή της διεύθυνσης του ηλεκτρονικού ταχυδρομείου του αποστολές είναι μία τέτοια υπό την έννοια ότι για την πρόσβαση στις λειτουργίες αποστολή και λήψης μηνυμάτων είναι απαραίτητη η εκτέλεση μία διαδικασίας αυθεντικοποίησης του χρήστη της αντίστοιχης εφαρμογής. Δεδομένων αυτών και του γεγονότος ότι η αναγραφή της ηλεκτρονικής διεύθυνσης του αποστολέα στο μήνυμα διαμορφώνεται κατά πρωτότυπο τρόπο από τον ίδιο τον καθιστά απολύτως προσδιορισμένο στον αποδέκτη. Αν και – υπό προϋποθέσεις πάντα – μπορεί να καθοριστεί η ταυτότητα του αποστολέα, δεν συμβαίνει το ίδιο με την γνησιότητα του περιεχομένου αφού αυτό είναι δυνατόν να μεταβληθεί χωρίς να είναι δυνατή η ανίχνευση των μεταβολών αυτών. Η ηλεκτρονική διεύθυνση του παραλήπτη μπορεί να προσδιορίσει και αυτόν αφού αυτή αντιστοιχεί μόνο σε ένα φυσικό πρόσωπο. Αυτό συμβαίνει διότι πρόσβαση στην ανάγνωση των μηνυμάτων που προορίζονται σε μία διεύθυνση ηλεκτρονικού ταχυδρομείου έχει μόνο ένας συγκεκριμένος χρήστης με την χρήση credentials που μόνος αυτός μπορεί – θεωρητικά – να γνωρίζει [9].

[8] ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ. (2001). ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ' ΑΡΙΘ. 150/2001 (ΦΕΚ 125 Α΄/25-6-2001) . ΑΘΗΝΑ: ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

[9] ΠΡΩΤΟΔΙΚΕΙΟ ΑΘΗΝΩΝ. (2004). Αριθμός απόφασης 1963/2004. Ανάκτηση από Δικηγορικός Σύλλογος Αθηνών: ΠΡΩΤΟΔΙΚΕΙΟ ΑΘΗΝΩΝ

2.3 Χρήση των ηλεκτρονικών αρχείων

Οι ηλεκτρονικές αποδείξεις ή στοιχεία έρχονται σε πολλά διαφορετικά είδη. Κατά την έναρξη των ερευνών σε ποινικές υποθέσεις που αφορούν τη χρήση των ηλεκτρονικών αποδεικτικών στοιχείων, είναι χρήσιμο να εξεταστεί και προσδιοριστεί ποιες από αυτές μπορεί να είναι χρήσιμες για την υπόθεση.

Κατά κύριο λόγο, οι ηλεκτρονικές αποδείξεις είναι απλά μια σειρά καταγραφών από έναν υπολογιστή. Το ερώτημα είναι, ποια γεγονότα και ποιες λεπτομέρειες μπορούν να βοηθήσουν την υπόθεση; Η κατανόηση σχετικά με το γιατί και το πώς συγκεκριμένα αρχεία δημιουργούνται και ποιες πληροφορίες συλλέγονται μπορεί να προσφέρει κάποια χρήσιμα στοιχεία και, ενδεχομένως, νέα κατεύθυνση στην υπόθεση. Για παράδειγμα, τα αρχεία μπορεί να παρέχουν αναγνωριστικά χαρακτηριστικά για το άτομο που πραγματοποίησε μια συναλλαγή (όπως τη διεύθυνση πρωτοκόλλου Internet, το λογαριασμό του πελάτη, το ιστορικό συναλλαγών του). Η εταιρεία και ο ιδιοκτήτης των αρχείων του υπολογιστή μπορεί να έχουν κρατήσει τα στοιχεία του λογαριασμού του πελάτη όταν ο λογαριασμός άνοιξε για πρώτη φορά. Ή μπορεί να φανεί ότι κάποια συγκεκριμένη πιστωτική κάρτα μπορεί να συνδέεται με το λογαριασμό. Άλλα αναγνωριστικά μπορεί να περιλαμβάνουν το όνομα, και το ιστορικό των αρχείων που αποστέλλονται μέσω των συναλλαγών .Αυτή η πληροφορία μπορεί να ρίξει φως σχετικά με το ποιος ήταν πίσω από τη συναλλαγή ή μπορεί να συνδεθεί με άλλα αποδεικτικά στοιχεία της υπόθεσης. Η χρονοθέτηση πληροφοριών συχνά δίνει χρήσιμες πληροφορίες για τη δημιουργία μιας χρονοσειράς ή δείχνει την ακολουθία των εν εξελίξει γεγονότων.

Από την πλευρά του εισαγγελέα, ένα από τα οφέλη των ηλεκτρονικών αποδείξεων είναι ότι μπορεί να χρησιμοποιηθούν για τη δοκιμή των θεωριών στην κάθε περίπτωση, συμπεριλαμβανομένων των καταθέσεων των ενόρκων. Εάν ορισμένα γεγονότα φέρεται να έχουν συνέβη, μπορεί να ελεγχθούν από την καταγραφή αρχείων.

Ένα παράδειγμα έρχεται από την ποινική δίωξη της παιδικής πορνογραφίας στις Ηνωμένες Πολιτείες. Ένας κατηγορούμενος ονομάτι Ganoe χρεώθηκε κατηγορίες για κατοχή υλικού παιδικής πορνογραφίας. Μια έρευνα διαπίστωσε ότι ένα πρόγραμμα ανταλλαγής αρχείων (LimeWire) χρησιμοποιήθηκε για τον διαμοιρασμό της παιδικής πορνογραφίας. Λήφθηκε ένα ένταλμα έρευνας στην οικία του κατηγορουμένου για να πάρουν τον υπολογιστή και τα αποδεικτικά στοιχεία γιατί η διεύθυνση IP που είχαν βρει ήταν ίδια με αυτή της οικίας του Ganoe. Κατά τη διάρκεια της έρευναw, ο κατηγορούμενος παραδέχθηκε ότι είχε «κατά λάθος κάνει λήψη της παιδικής πορνογραφίας" και ότι τα "«κακά πράγματα», θα μπορούσαν να τα βρουν στο φάκελο «z» του υπολογιστή του. Αφού του κυρώθηκαν κατηγορίες ένας εμπειρογνώμονας αναλυτής υπολογιστών κατέθεσε στη δίκη ότι βρέθηκαν "72 φωτογραφίες και βίντεο που απεικόνιζαν παιδική πορνογραφία σε έναν υποφάκελο με τίτλο «z», που βρισκόταν μέσα στο φάκελο iTunes. Κατά τη διάρκεια της δίκης, αδελφή του κατηγορουμένου, ο φίλος της, και ένας άλλος φίλος κατέθεσαν ότι «ένας άνθρωπος που ονομάζεται Ray Rodriguez" είχε διαμείνει στην κατοικία ", αλλά εξαφανίστηκε μετά" όταν έμαθε για τη κατάσχεση του υπολογιστή. Ο φίλος της αδερφής του κατηγορουμένου, κατέθεσε ότι «είχε παρατηρήσει προσωπικά τον Rodriguez να κάνει αναζήτηση και λήψη παιδικής πρνογραφίας στον υπολογιστή ".Ο Rodriguez δεν βρέθηκε ποτέ ενώ ο κατηγορούμενος Ganoe προσκόμισε άλλοθι της απουσίας του κατά τη διάρκεια των περιόδων της παιδικής πορνογραφίας.

Πώς θα μπορούσαν οι εγκληματολόγοι ηλεκτρονικών υπολογιστών να αντιμετωπίσουν την συγκεκριμένη δίκη; Κατά τη διάρκεια της διάψευσης, το ποινικό εφετείο ξανακάλεσε τον αναλυτή που κατέθεσε σχετικά με τη δραστηριότητα του υπολογιστή του χρήστη. Ο αναλυτής ανέφερε ότι ερευνώντας την δραστηριότητα του υπολογιστή ,όποιος τον χρησιμοποιούσε κατά τη περίοδο λήψης της παιδικής πορνογραφίας, είχε επίσης πρόσβαση στον λογαριασμό PayPal του Ganoe , στην κάρτα American Express του και είχε επίσης συνδεθεί στον λογαριασμό e-mail του

Ganoe και είχε στείλει ηλεκτρονικά μηνύματα σε ανθρώπους που συνδέονται με τον Ganoe, γεγονός που υποδηλώνει ότι θα πρέπει να ήταν ο Ganoe αυτός που χρησιμοποιούσε τον υπολογιστή εκείνη την περίοδο.

Ως απάντηση των παραπάνω κατέθεσε ο φίλος της αδερφής και στην μαρτυρία του σχολίασε ότι δίπλα στον υπολογιστή υπήρχε μια λίστα με όλους τους κωδικούς του κατηγορουμένου άρα οποιοσδήποτε χρησιμοποίησε τον υπολογιστή θα μπορούσε να έχει πρόσβαση σε αυτές τις ιστοσελίδες. Η κριτική επιτροπή τον κατηγόρησε για αδίκημα δευτέρου βαθμού, ωστόσο ανέκτησε ποινή αδικήματος πρώτου βαθμού.

Η υπόθεση Ganoe τονίζει πως τα ηλεκτρονικά αποδεικτικά στοιχεία βοήθησαν στην εξακρίβωση της μαρτυρίας ότι άλλοι χρήστες ήταν υπεύθυνη για την παιδική πορνογραφία που βρέθηκαν στο κατασχέθηκαν υπολογιστή. Χωρίς περαιτέρω αναθεώρηση των ηλεκτρονικών αποδεικτικών στοιχείων, η κριτική επιτροπή δεν θα γνώριζε για τη δραστηριότητα στον υπολογιστή. Η υπόθεση τονίζει επίσης τη συνεχιζόμενη ανάγκη να χρησιμοποιούνται ηλεκτρονικοί αναλυτές για να αναλύουν τα συγκεκριμένα ζητήματα στην υπόθεση καθώς και ηλεκτρονικά αποδεικτικά στοιχείων για την επιβεβαίωση παρόμοιων περιπτώσεων[10].

Η διαρκής αύξηση της ηλεκτρονικής εγκληματικότητας εισήγαγε στην νομική αλλά και στην πληροφορική τον όρο Computer Forensics (Νομική Δικαστική). Ο όρος αυτός περιλαμβάνει την διατήρηση, ταυτοποίηση, εξαγωγή, τεκμηρίωση και διερμήνευση των υπολογιστικών μέσων για εύρεση αποδεικτικών στοιχείων ή/και ανάλυση αιτίων συμβάντος. Ένα υπολογιστής μπορεί να χρησιμοποιηθεί με δύο τρόπους σε εγκληματικές δραστηριότητες:

- Ως εργαλείο τέλεσης αδικημάτων
- Ως θύμα εγκληματικής πράξης

Πρόκειται για κλάδο που παρακολουθεί συνεχώς τις ραγδαίες εξελίξεις στους τομείς της πληροφορικής και των τηλεπικοινωνιών και προσπαθεί να προσαρμόζει τις μεθόδους της σε αυτές.

Η βασική μεθοδολογία της δικαστικής πληροφορικής αποτελείται από τα εξής στοιχεία:

- Απόκτηση των αποδεικτικών στοιχείων χωρίς την καταστροφή των αυθεντικών
- Πιστοποίηση ότι τα αποκτηθέντα στοιχεία είναι τα ιδιά με τα αυθεντικά στοιχεία
- Ανάλυση των δεδομένων χωρίς αυτά να τροποποιηθούν

Τα στοιχεία πρέπει να συλλέγονται από ενεργά συστήματα υπό το φόβο της καταστροφής τους. Η διαδικασία της εξασφάλισης τους πρέπει να δίνει απαντήσεις στα εξής ερωτήματα:

- Ποιος τα συνέλλεξε
- Πως και που
- Ποιος τα κατείχε
- Πως αποθηκεύτηκαν και προστατεύτηκαν κατά την αποθήκευση τους
- Ποιος τα εξήγαγε από την αποθήκευση και γιατί

[10] M. Krotoski, Effectively Using Electronic Edidence before and at trial, σελ 52-71, διαθέσιμο στο http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf

Η διαδικασία εκμετάλλευσης αρχείων ηλεκτρονικού υπολογιστή και συναφών συσκευών (smartphones, tablets κτλ.) περιλαμβάνει τα εξής στάδια:

- Συλλογή: Ανάκτηση των αρχείων με τρόπο τέτοιο ώστε να μην υπόκεινται σε οποιαδήποτε αλλοίωση και να δύνανται να υποστηρίζουν την υπόθεση στην οποία θα χρησιμοποιηθούν.
- Ταυτοποίηση: Τοποθέτηση ετικετών σε κάθε ένα από αυτά που να τα χαρακτηρίζει.
- Μεταφορά: Προσεκτική μεταφορά ώστε να μην αλλοιωθούν.
- Αποθήκευση: Αποθήκευση των αποδείξεων σε μέρος το οποίο να καλύπτει τις ελάχιστες προδιαγραφές φύλαξης ανάλογα με το μέσο που περιέχει τις αποδείξεις
- Τεκμηρίωση της διερεύνησης: Καταγραφή και τεκμηρίωση της μεθοδολογίας και διαδικασίας ανάκτησης των αποδεικτικών στοιχείων σε γλώσσα κατανοητή από μη εξειδικευμένους με θέματα υλικού και λογισμικού ανθρώπους[11].

Η δικαστική των ηλεκτρονικών υπολογιστών δεν περιορίζεται στην μελέτη του υλικού για την απόκτηση και αξιολόγηση αποδεικτικών στοιχείων, αλλά και στην μελέτης δικτυακής και διαδικτυακής δραστηριότητας. Περιλαμβάνει επίσης – σε πολλές περιπτώσεις - και την προσπάθεια αποκρυπτογράφησης των αποδεικτικών στοιχείων που συλλέγονται. Η πραγματογνωμοσύνη των ειδικών επί τέτοιού είδους αποδεικτικών στοιχείων γίνεται δεκτή από τα δικαστήρια. Μια σημαντική πρακτική που έχει αποδειχθεί αποτελεσματική είναι να ενθάρρυνση μια αρχικής τριμερής συζήτηση μεταξύ του εξεταστή, του πράκτορα, και του εισαγγελέα. Αυτή η συζήτηση θα επικεντρωθεί στην εύρεση των βασικών αποδεικτικών στοιχείων της υπόθεσης. Ο πράκτορας θα είναι σε θέση να προσδιορίσει τα βήματα και τα μέρη της έρευνας. Ο εισαγγελέας ελέγχει για την ταυτοποίηση των στοιχείων και άλλων νομικών ζητημάτων της υπόθεσης και τελικά ο εξεταστής μπορεί να εντοπίσει τα σχετικά αρχεία και τις τεχνικές που μπορούν να παράγουν βασικά στοιχεία. Αυτή η τριμερής συζήτηση θα χρησιμεύσει για να φέρει μια πρώιμη έμφαση στα ζητήματα της υπόθεση. Αν εντοπιστούν έγκαιρα τα βασικά στοιχεία της έρευνας μπορεί να παρθεί απόφαση προ-κατηγορητήριο. Αν όμως, αποκαλύπτει ότι η περίπτωση αυτή είναι μεγαλύτερη (σε έκταση και συμμετέχοντες) από ότι αρχικά αναμενόταν, τότε μπορεί να χρειαστούν νέες ερευνητικές μέθοδοι άμεσα. Αυτή η τριμερής συζήτηση διασφαλίζει ότι η οι κινήσεις που θα γίνουν αφορούν τις ανάγκες της συγκεκριμένης υπόθεσης. Μερικές ερωτήσεις της πρώιμης συζήτησης μπορεί να περιλαμβάνουν:

- Ποια είναι τα κύρια γεγονότα στην υπόθεση; Τι στοιχεία μπορεί να τα επιβεβαιώσουν ?
- Πόσοι από τους συμμετέχοντες συμμετείχαν; Υπάρχουν συν-συνωμότες ; Ποιοι είναι οι ρόλοι κάθε ατόμου;
- Ποια βασικά έγγραφα, πράξεις, ή αποδεικτικά στοιχεία, όπως ένα συγκεκριμένο αρχείο, εικόνα, ή το ηλεκτρονικό ταχυδρομείο,
- μπορούν να βρεθούν ;
- Τι αποδείξεις μπορούν να βρεθούν ;

[11] Παπαδημητρίου, Γ. (2010). Network Forensics. Ανάκτηση από https://www.cs.ucy.ac.cy/courses/EPL674/lectures/Forensics-GR.pdf

- Τι ρόλο έπαιξαν οι διάφορες συσκευές στην υπόθεση; Ήταν ο φορητός υπολογιστής που χρησιμοποιήθηκε ως ένα εργαλείο για να
- διαπραχθεί το αδίκημα ή δεν έχει δεδομένα που σχετίζονται με το έγκλημα;
- Υπάρχουν οικονομικές ή συναισθηματικές σχέσεις με τον υπολογιστή;
- Ποιες είναι οι αναμενόμενες ερωτήσεις και πορίσματα της έρευνας ;

Πρόσφατες έρευνες έχουν δείξει τα οφέλη από την ανταλλαγή πληροφοριών και νέων μεταξύ του εξεταστή και του ερευνητή της έρευνας. Ο εξεταστής μπορεί να εντοπίσει πρόσθετες πληροφορίες που να γεμίζουν τα κενά ή να παρέχουν νέα που μπορεί να βοηθήσουν τους ανακριτές και διαφορετικά δεν θα μπορούσαν να έχουν βρεθεί. Οι ερευνητές από την άλλη, μπορούν να προσδιορίσουν βασικούς τομείς στους οποίους μπορεί να επικεντρωθεί για ο εξεταστής στο πεδίο εφαρμογής του εντάλματος έρευνας. Για παράδειγμα, ο εξεταστής μπορεί να εντοπίσει νέους λογαριασμούς ηλεκτρονικού ταχυδρομείου που μπορεί να ήταν άγνωστοι στους ερευνητές. Οι ερευνητές από την πλευρά τους, μπορούν να χρησιμοποιήσουν κατάλληλες νομικές διαδικασίες για τη συγκέντρωση των αποδεικτικών στοιχείων που σχετίζονται με το νέο λογαριασμό. Εναλλακτικά, ο εξεταστής μπορεί να αποκαλύψει ότι ένα βασικό έγγραφο ήταν το προϊόν πολλών αναζητήσεων για ένα μεγάλο χρονικό διάστημα ή είχε συνεισφορές από άλλους. Αυτά τα στοιχεία μπορεί διαφορετικά να παρέμεναν αναξιοποίητα. Αυτή η ανταλλαγή πληροφοριών μπορεί επίσης να ωφελήσει τον εξεταστή ενώ οι ερευνητές προτείνουν πληροφορίες σχετικές με συναλλαγές, τις χρονικές περιόδους, καταθέσεις μαρτύρων, ή εξωτερικά γεγονότα τα οποία μπορεί να ψάξει και να ταυτοποιήσει μέσα από ηλεκτρονικά έγγραφα ο ερευνητής. Τα αμοιβαία οφέλη από αυτή την αμφίδρομη ανταλλαγή πληροφοριών είναι δεν είναι μόνο για την αρχή της έρευνας. Δεδομένου ότι οι περισσότερες ενδείξεις και αποδεικτικά στοιχεία που συγκεντρώθηκαν ελέγχθηκαν σε βάθος, μπορεί να είναι απαραίτητο να επανεξετασθούν και να οδηγήσουν στην επανεξέταση άλλων στοιχείων που αρχικά θεωρήθηκαν άσχετα με την υπόθεση. Ένα επαναλαμβανόμενο θέμα αποδεικνύεται αν ο κατηγορούμενος ήταν ο χρήστης του υπολογιστή κατά τη διάρκεια της παράβασης. Η φάση της έρευνας μπορεί να βοηθήσει στην αντιμετώπιση αυτού του ζητήματος. Μερικές ερωτήσεις για να εξετάσει μπορεί να περιλαμβάνουν:

- Ποιες ηλεκτρονικές αποδείξεις επιβεβαιώνουν ποιος είναι ο χρήστης ή κάτοχος του κατασχεθέντος υπολογιστή ;
- Ποιες ενδείξεις δείχνουν ποιος ήταν ο συγγραφέας του ηλεκτρονικού μηνύματος ή chat μηνύματος (π.χ., ψευδώνυμο ή άλλα ταυτοποίηση ή εξοικείωση με μοναδικά γεγονότα);
- Μπορούν τα μετα-δεδομένα παρέχουν πληροφορίες για τον συγγραφέα ενός αρχείου;
- Ποιες αποδείξεις εξωτερικά με τον υπολογιστή ή το ηλεκτρονικό μήνυμα παρέχουν πληροφορίες σχετικά με το συγγραφέας;
- Μπορεί ένα μοτίβο πρόσβασης στους λογαριασμούς των πελατών πριν και μετά από ένα σημαντικό γεγονός να ρίξει φως σχετικά με τον χρήστη του υπολογιστή, όπως το ιστορικό περιήγησης στο Internet ή η πρόσβαση σε λογαριασμούς που ελέγχονται από ένα συγκεκριμένο πρόσωπο;
- Μπορεί ο αποδέκτης του μηνύματος ή της ηλεκτρονικής επικοινωνίας να εντοπίσει τον συγγραφέα;
- Οι ηλεκτρονικές αποδείξεις έχουν αποδειχθεί χρήσιμες για να εντοπιστούν τα κενά στα αποδεικτικά στοιχεία. Για παράδειγμα, σε μια σειρά μηνυμάτων τύπου embedded messages, ίσως να βρεθούν μόνο λίγα μηνύματα. Κατά τη φάση της έρευνας, μερικά από αυτά τα κενά μπορούν να καλυφθούν από πληροφορίες που βρέθηκαν από άλλες πηγές.

Στην Ελληνική Νομοθεσία γίνονται δεκτά ηλεκτρονικά αρχεία ως αποδεικτικά στοιχεία παρανόμων πράξεων. Ένα παράδειγμα είναι η βεβαίωση παραβάσεων του Κώδικα Οδικής

Κυκλοφορίας με ηλεκτρονικά μέσα (φωτογραφίες και βίντεο) που προβλέπει το ΠΔ 287/2001[12]. Χαρακτηριστικά σε αυτό αναφέρεται ότι η βεβαίωση των παραβάσεων γίνεται με τη λήψη φωτογραφιών ή με βιντεοσκόπηση, ανάλογα με το είδος της συσκευής, που θα απεικονίζουν τον αριθμό κυκλοφορίας και κάθε άλλο στοιχείο αναγκαίο και πρόσφορο για την εξατομίκευση του οχήματος και του παραβάτη που μπορεί να καταγράψει η φωτογραφική μηχανή ή το βίντεο και θα αποτυπώνουν και την ημερομηνία και ώρα της παράβασης και στην περίπτωση ελέγχου ταχύτητας, την καταγραφεί σα ταχύτητα σε χ/ω. Οι φωτογραφίες ή οι ταινίες είναι για κάθε περίπτωση αποδεικτικό στοιχείο της διάπραξης της παράβασης. Κάθε έκθεση παράβασης επιδίδεται στον παραβάτη από το Αστυνομικό Τμήμα του τόπου της μόνιμης κατοικίας του, με αποδεικτικό επίδοσης το οποίο επιστρέφεται στην αποστέλλουσα Υπηρεσία, προκειμένου, στην περίπτωση που δεν καταβληθεί το πρόστιμο, να υποβληθεί στον αρμόδιο Δημόσιο Κατήγορο ή σε πλημμελληματικές παραβάσεις στον αρμόδιο Εισαγγελέα. Όσο αφορά τα ευαίσθητα προσωπικά δεδομένων των παραβατών εφαρμόζονται οι διατάξεις του Ν. 2472/1997.

Οι ηλεκτρονικές τεχνικές συσκευές διαπίστωσης, καταγραφής και βεβαίωσης των παραβάσεων του Κ.Ο.Κ. αποτελούνται ανάλογα με τη συγκεκριμένη για κάθε περίπτωση μελέτη, από τις ακόλουθες βασικές μονάδες:

- Τη μονάδα των αισθητηρίων με τα οποία γίνεται η ανίχνευση του στοιχείου ή των στοιχείων εκείνων που, με βάση τη μελέτη του συστήματος, είναι απαραίτητα για να μπορεί να διαπιστωθεί η πραγματοποίηση της συγκεκριμένης παράβασης.
- Τη μονάδα επεξεργασίας των στοιχείων που συλλέγονται από τη μονάδα των αισθητηρίων, ώστε να διαπιστωθεί αν συντελέστηκε η παράβαση.
- Τη μονάδα καταγραφής του στοιχείου ή των στοιχείων εκείνων που θα αποδεικνύουν την παράβαση, αν αυτή έχει συντελέστει.
- Τη μονάδα παραγωγής των αποδεικτικών στοιχείων που βεβαιώνουν τη πραγματοποίηση της παράβασης.

Οι συσκευές που χρησιμοποιούνται πρέπει να έχουν απαραίτητα τις προβλεπόμενες εγκρίσεις τύπου ή κυκλοφορίας από τη Διεύθυνση Τεχνικής και Ελέγχου Επικοινωνιών του Υπουργείου Μεταφορών και Επικοινωνιών[13]. Ομοίως, σύμφωνα με το άρθρο 444, παράγραφος 3 του ΚΠολΔ το μέσο το οποίο έχει χρησιμοποιηθεί για φωνοληψία αποτελεί ιδιωτικό έγγραφο. Ως τέτοιο λοιπόν μπορεί να αποτελεί αποδεικτικό μέσο αν αυτό συνοδεύεται από έγγραφο λόγο στον οποίον να αποτυπώνεται το περιεχόμενο του.

---

[12] Ελληνική Δημοκρατία, ΠΔ 287/2001, διαθέσιμο στο http://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.glavopoulos.gr%2Fnomoi%2FKOK-PD287-mesa-ilektronikis-astinomefsis.doc&ei=rABSVOatKdWvaa24gfAK&usg=AFQjCNEdbI1IChrA14w-7wN6UhmzQGvcZQ&sig2=NvAjpAb17W0AKGrE2FTM8g&bvm=bv.78597519,d.d2s&cad=rja

[13] ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ.. ΠΔ 287/2001 ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΧΡΗΣΗ ΕΙΔΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΚΕΥΩΝ ΓΙΑ ΤΗΝ ΚΑΤΑΓΡΑΦΗ ΚΑΙ ΒΕΒΑΙΩΣΗ ΠΑΡΑΒΑΣΕΩΝ ΤΟΥ ΚΟΚ. ΑΘΗΝΑ: ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

2.4 Συμπεράσματα

Στην σύγχρονη εποχή που οι νέες τεχνολογίες πληροφορικής και τηλεπικοινωνιών έχουν βρει εφαρμογές σε όλες τις πτυχές της καθημερινής ανθρώπινης δραστηριότητας, είναι επιτακτική ανάγκη η βασισμένη σε αυτές δράσεις να είναι δυνατό να χρησιμοποιούνται στην αποδεικτική διαδικασία που λαμβάνει χώρα στις αίθουσες των δικαστηρίων. Σε αυτήν την κατεύθυνση κινούνται και η εξομοίωση της προηγμένης ψηφιακής υπογραφής με την χειρόγραφή αλλά και η υπό προϋποθέσεις εξομοίωση κάθε είδους ηλεκτρονικής υπογραφής με αυτή. Αδυναμία τέτοιου είδους εξομοίωσης θα αφήσει εκτός της αποδεικτικής διαδικασίας μεγάλο πλήθος στοιχείων δυσχεραίνοντας σε πολύ μεγάλο βαθμό τις δικανικές διαδικασίες. Ενισχυτικό της άποψης αυτής είναι και το γεγονός ότι οι συνήθειες των ανθρώπων γίνονται ολοένα και σε μεγαλύτερο ποσοστό ψηφιακές εγκαταλείποντας παραδοσιακούς τρόπους δραστηριότητας. Ένα απλό παράδειγμα αποτελεί η επικοινωνία μέσω e-mail. Σήμερα όλο και περισσότεροι άνθρωποι επιλέγουν το ηλεκτρονικό ταχυδρομείο για να αποστείλουν μικρής ή μεγάλης σημασίας μηνύματα και πολύ σπάνια ανταλλάσσουν φυσικά υπογεγραμμένα μηνύματα σε χαρτί. Αδυναμία αποδοχής των μηνυμάτων ηλεκτρονικού ταχυδρομείου στις δικαστικές αίθουσες θα σήμαινε αυτόματα ότι ένας μεγάλο όγκος εν δύναμή αποδεικτικών στοιχείων θα παρέμενε ανεκμετάλλευτος. Αυτό που χρειάζεται πλέον να γίνει είναι συνεχής μελέτη για το πώς τα ηλεκτρονικά αρχεία μπορούν να αποκτούν τέτοια μορφή ώστε η αντικειμενική τους υπόσταση ως αποδεικτικά στοιχεία να είναι αδιαμφισβήτητη. Η μελέτη αυτή πρέπει να είναι συντονισμένη και πλήρως εναρμονισμένη με τις εξελίξεις που συμβαίνουν με ταχείς ρυθμούς στους τομείς της πληροφορικής και των τηλεπικοινωνιών. Παράλληλα θα πρέπει να θεσπιστούν αυστηρές προδιαγραφές στην επικοινωνία και τις δοσοληψίες που πραγματοποιούνται με ηλεκτρονικά μέσα και με την ανταλλαγή αρχείων ώστε η ύπαρξή τους και η γνησιότητα τους να μην είναι δυνατόν να αμφισβητηθεί.

ΚΕΦΑΛΑΙΟ 3 : ΔΙΑΤΗΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΓΡΑΦΩΝ ΕΤΑΙΡΙΩΝ ΚΑΤΩ ΑΠΟ ΤΙΣ ΑΠΟΦΑΣΕΙΣ ΤΗΣ Α.Δ.Α.Ε

3.1 Διατήρηση Τηλεπικοινωνιακών Δεδομένων

Τα ζητήματα που ανακύπτουν σχετικά με την διατήρηση των δεδομένων που σχετίζονται με την ηλεκτρονική επικοινωνία μέσω δημοσίων δικτύων τηλεπικοινωνιών ρυθμίζονται με τον νόμο Ν. 3917/2011 «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», που ψηφίστηκε από το Ελληνικό Κοινοβούλιο στις 21 Φεβρουαρίου 2011. Ο νόμος αυτός ενσωμάτωσε στο Ελληνικό Δίκαιο την Οδηγία 2006/24 του Ευρωπαϊκού Κοινοβουλίου, τροποποιώντας τον Ν.3471/2006.

Ο νόμος Ν.3471/2006 προέβλεπε ότι τα δεδομένα της επικοινωνίας των χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών, διατηρούνταν από τους παρόχους των υπηρεσιών αυτών. Αυτά επιτρεπόταν να υποστούν επεξεργασία για σκοπούς που σχετίζονται με την μετάδοση και την χρέωση των υπηρεσιών. Επιβάλλετο επίσης η καταστροφή τους όταν θα εξέπνεε η προθεσμία που θα είχαν οι χρήστες τους να αμφισβητήσουν τις χρεώσεις των υπηρεσιών που τους παρασχέθηκαν. Στον νόμο προσδιορίζονται αρχικά οι εξής όροι:

- Δεδομένα: τα δεδομένα κίνησης και θέσης και τα συναφή δεδομένα που είναι αναγκαία για την αναγνώριση του συνδρομητή ή χρήστη.
- Χρήστης: Κάθε φυσικό ή νομικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για ιδιωτικούς ή εμπορικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας·
- Τηλεφωνική υπηρεσία: Κλήσεις (στις οποίες συμπεριλαμβάνονται τα φωνητικά τηλεφωνήματα, το φωνητικό τηλεταχυδρομείο, οι τηλεδιασκέψεις και η τηλεφωνική μεταφορά δεδομένων), συμπληρωματικές υπηρεσίες (στις οποίες συμπεριλαμβάνονται η προώθηση και η εκτροπή κλήσεων), υπηρεσίες μηνυμάτων και πολυμέσων (στις οποίες συμπεριλαμβάνονται οι υπηρεσίες γραπτών μηνυμάτων, ενισχυμένων μέσων και πολυμέσων).
- Κωδικός ταυτότητας χρήστη: ο μοναδικός αναγνωριστικός κωδικός που αποδίδεται σε κάθε πρόσωπο, όταν καθίσταται συνδρομητής ή εγγράφεται σε κάποια υπηρεσία πρόσβασης στο διαδίκτυο ή επικοινωνίας μέσω του διαδικτύου·
- Κωδικός ταυτότητας κυψέλης: η ταυτότητα του κυψελωτού κυττάρου, από το οποίο ξεκινά ή στο οποίο καταλήγει συγκεκριμένη κλήση κινητής τηλεφωνίας·
- Ανεπιτυχής κλήση: Κλήση, κατά την οποία επιτυγχάνεται μεν σύνδεση με τον αριθμό προορισμού, η κλήση όμως παραμένει αναπάντητη ή σημειώνεται επέμβαση της διαχείρισης του δικτύου.

Οι διατάξεις του νόμου προβλέπουν την διατήρηση προσωπικών δεδομένων συνδρομητών και εγγεγραμμένων χρηστών που σχετίζονται με τις ηλεκτρονικές υπηρεσίες. Συνοπτικά τα στοιχεία που υποχρεούνται να διατηρούν οι πάροχοι συνοψίζονται στα εξής:

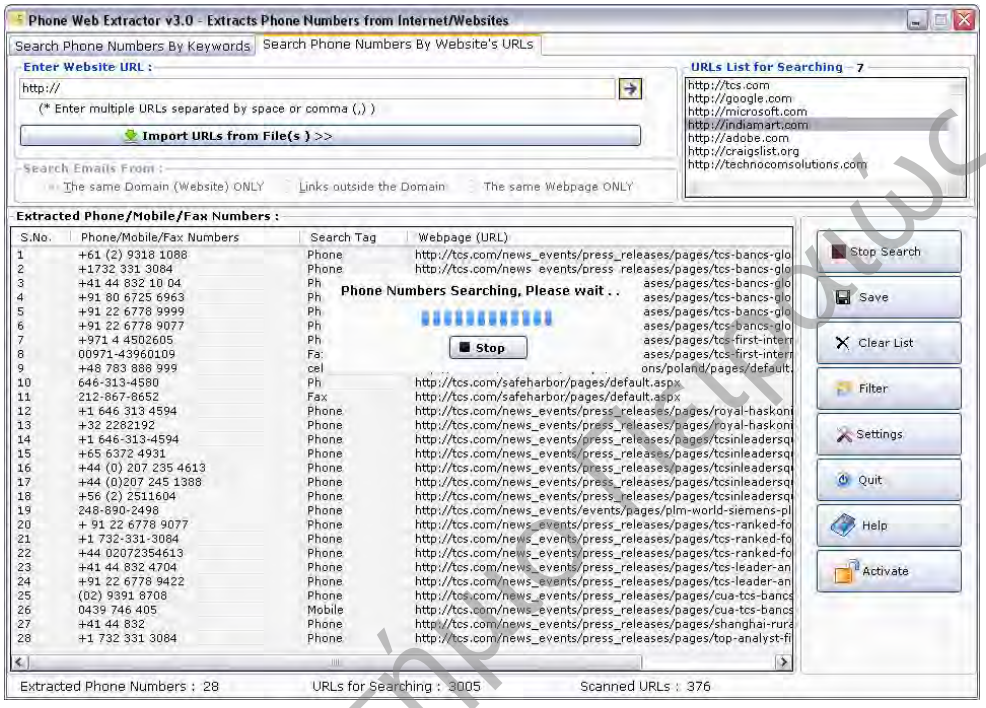
- Δεδομένα που σχετίζονται με την προέλευση της επικοινωνίας:
    - Σταθερή και κινητή τηλεφωνία: ο τηλεφωνικός αριθμός του καλούντος, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή του εγγεγραμμένου χρήστη·

- Πρόσβαση στο διαδίκτυο: ο αποδοθείς κωδικός ταυτότητας χρήστη, ο κωδικός ταυτότητας χρήστη και ο τηλεφωνικός αριθμός που δίνονται σε κάθε επικοινωνία που εισέρχεται στο δημόσιο τηλεφωνικό δίκτυο, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί κατά το χρόνο επικοινωνίας διεύθυνση IP (πρωτοκόλλου διαδικτύου), κωδικός ταυτότητας χρήστη ή αριθμός τηλεφώνου.

- Δεδομένα που σχετίζονται με τον προορισμό της επικοινωνίας:
  - Σταθερή και κινητή τηλεφωνία: ο καλούμενος αριθμός ή αριθμοί (ο αριθμός ή οι αριθμοί τηλεφώνου που κλήθηκαν), στις δε περιπτώσεις όπου υπεισέρχονται συμπληρωματικές υπηρεσίες όπως προώθηση/εκτροπή κλήσης, ο αριθμός ή οι αριθμοί τηλεφώνου προς τους οποίους προωθήθηκε η κλήση, τα ονοματεπώνυμα και οι διευθύνσεις των συνδρομητών ή εγγεγραμμένων χρηστών·
  - Ηλεκτρονικό ταχυδρομείο και διαδικτυακή τηλεφωνία: το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη και ο κωδικός ταυτότητας χρήστη του παραλήπτη της επικοινωνίας, ο κωδικός ταυτότητας χρήστη ή ο αριθμός τηλεφώνου του παραλήπτη διαδικτυακής τηλεφωνικής κλήσης·
- Δεδομένα σχετικά με τον χρόνο πραγματοποίησης της επικοινωνίας:
  - Σταθερή και κινητή τηλεφωνία: η ημερομηνία και η ώρα έναρξης και λήξης της επικοινωνίας·
  - Πρόσβαση στο διαδίκτυο: η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το διαδίκτυο με βάση συγκεκριμένη ωριαία ζώνη, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), είτε δυναμική είτε στατική, που απέδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη, η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου, με βάση συγκεκριμένη ωριαία ζώνη.
- Δεδομένα για τον προσδιορισμό του είδους της επικοινωνίας:
  - Σταθερή και κινητή τηλεφωνία: η χρησιμοποιηθείσα τηλεφωνική υπηρεσία.
  - Ηλεκτρονικό ταχυδρομείο και διαδικτυακή τηλεφωνία: η χρησιμοποιηθείσα διαδικτυακή υπηρεσία.
- Δεδομένα για τον χρησιμοποιούμενο τηλεπικοινωνιακό εξοπλισμό:
  - Σταθερή τηλεφωνία: οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου·
  - Κινητή τηλεφωνία: οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου, η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI) του καλούντος, η διεθνής ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI) του καλούντος, η IMSI του καλουμένου, η IMEI του καλουμένου, στην περίπτωση προπληρωμένων ανώνυμων υπηρεσιών, η ημερομηνία και ώρα της αρχικής ενεργοποίησης της υπηρεσίας και ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) από την οποία πραγματοποιήθηκε η ενεργοποίηση.
  - Πρόσβαση στο διαδίκτυο: ο τηλεφωνικός αριθμός καλούντος για την πρόσβαση μέσω τηλεφώνου, η ψηφιακή συνδρομητική γραμμή (DSL) ή άλλη απόληξη της πηγής της επικοινωνίας.

- Δεδομένα για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας: ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) κατά την έναρξη και λήξη της επικοινωνίας, δεδομένα με τα οποία προσδιορίζεται η γεωγραφική θέση των κυψελών βάσει των κωδικών θέσης (κωδικών ταυτότητας κυψέλης), κατά το χρονικό διάστημα για το οποίο διατηρούνται τα δεδομένα των επικοινωνιών.

Στην παρακάτω εικόνα φαίνεται ένα παράδειγμα τέτοιων εγγραφών.



Εικόνα 10: Τηλεπικοινωνιακά Δεδομένα

Στο πρώτο άρθρο του νόμου, καθορίζεται σαφώς ότι οι διατάξεις του αφορούν σε δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και στα δεδομένα που απαιτούνται για την αναγνώριση της ταυτότητας των συνδρομητών. Παράλληλα καθορίζεται ότι οι διατάξεις του δεν αφορούν το περιεχόμενο των κάθε είδους ηλεκτρονικών επικοινωνιών. Ο νόμος απαγορεύει την διατήρηση δεδομένων που μπορεί να αποκαλύπτουν το περιεχόμενο των επικοινωνιών ενώ ορίζεται ότι τα δεδομένα αποθηκεύονται σε αποθηκευτικές διατάξεις που βρίσκονται εντός της Ελληνικής επικράτειας. Η διάρκεια διατήρησης τους είναι δώδεκα μήνες από την πραγματοποίηση της επικοινωνίας και μετά την παρέλευσή τους καταστρέφονται με αυτοματοποιημένη διαδικασία από τον πάροχο, εκτός από εκείνα στα οποία έχει αποκτηθεί νομίμως πρόσβαση. Τα τελευταία, εφόσον παρήλθε η παραπάνω προθεσμία των 12 μηνών, καταστρέφονται από τον πάροχο μέσα σε δέκα ημέρες από την κοινοποίηση σε αυτόν σχετικής διάταξης που υποχρεώνεται να εκδώσει το κατά περίπτωση αρμόδιο όργανο. Ο πάροχος υποχρεούται να διατηρεί τα δεδομένα κατά τρόπο που να του επιτρέπει να τα επεξεργάζεται ηλεκτρονικά και να τα διαβιβάζει το αργότερο μέσα σε πέντε εργάσιμες ημέρες από τυχόν γνωστοποίηση διάταξης για πρόσβαση στα δεδομένα από την αρμόδια αρχή. Επίσης ο πάροχος δεσμεύεται να τηρεί τις παρακάτω αρχές όσον αφορά την διατήρηση των δεδομένων:

- τα διατηρούμενα δεδομένα είναι ίδιας ποιότητας και έχουν την ίδια προστασία και ασφάλεια με τα δεδομένα που περιέχει το δίκτυο.
- λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων κατά τυχαίας ή παράνομης καταστροφής τους ή τυχαίας απώλειας, αλλοίωσης, μη εξουσιοδοτημένης ή παράνομης αποθήκευσης, επεξεργασίας, πρόσβασης ή αποκάλυψης
- λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλισθεί ότι στα δεδομένα έχει πρόσβαση μόνον ειδικά εξουσιοδοτημένο προσωπικό.

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) επιφορτίζεται με την επίβλεψη της τήρησης των προβλεπόμενων από τον νόμο. Προβλέπονται αυστηρές ποινικές κυρώσεις στους παρόχους σε περιπτώσεις παρέκκλισης που προβλέπουν:

- σύσταση για συμμόρφωση μέσα στα χρονικά όρια της τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης
- πρόστιμο από 20.000 έως 5.000.000 ευρώ
- οριστική ανάκληση του δικαιώματος παροχής υπηρεσιών.

Η επεξεργασία των πληροφοριών που προκύπτουν από τα δεδομένα αυτά επιτρέπεται μόνον εφόσον διαταχθεί η διενέργεια της ανακριτικής πράξης της άρσης του απορρήτου σε βάρος συγκεκριμένου προσώπου για την τέλεση συγκεκριμένου εγκλήματος, ενώ σε καμία περίπτωση δεν επιτρέπεται προληπτική επεξεργασία των διατηρουμένων δεδομένων, ενόψει πάντοτε του άρθρου 19 του Συντάγματος και τηρουμένης της αρχής της αναλογικότητας[14] .

Η Ευρωπαϊκή οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, στην οποία βασίστηκε ο νόμος, κρίθηκε άκυρη από το Δικαστήριο της Ευρωπαϊκής Ένωσης, διότι θεωρήθηκε ότι από αυτή συνεπάγεται πολύ εκτεταμένη και ιδιαιτέρως σοβαρή επέμβαση στην άσκηση των θεμελιωδών δικαιωμάτων του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα χωρίς η επέμβαση αυτή να περιορίζεται στο απολύτως αναγκαίο. Σύμφωνα με το σκεπτικό της απόφασης του δικαστηρίου τα διατηρούμε εκ των παρόχων δεδομένα δίνει την δυνατότητα στον κτήτορά τους:

- να γνωρίζουν με ποιο πρόσωπο και με ποιο μέσο επικοινώνησε ένας συνδρομητής ή καταχωρισμένος χρήστης,
- να γνωρίζουν τον χρόνο της επικοινωνίας καθώς και ο τόπος από τον οποίο πραγματοποιήθηκε η επικοινωνία αυτή
- να γνωρίζουν την συχνότητα των επικοινωνιών του συνδρομητή ή καταχωρισμένου χρήστη με ορισμένα πρόσωπα κατά τη διάρκεια συγκεκριμένης περιόδου.

Τα δεδομένα αυτά, εκτιμάται ότι μπορεί να δώσουν ενδείξεις σχετικά με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα διατηρούνται, όπως είναι οι συνήθειες της καθημερινής ζωής, οι τόποι μόνιμης ή προσωρινής διαμονής, οι καθημερινές ή άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις και οι κοινωνικοί κύκλοι στους οποίους συχνάζει ο ενδιαφερόμενος. Με τον τρόπο αυτό συντελείται παράφορη παραβίαση των

[14] Ελληνική Δημοκρατία. (2006). Νόμος υπ'αρ.3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσίων. Αθήνα: Ελληνική Δημοκρατία

θεμελιωδών δικαιωμάτων του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Επιπλέον, το γεγονός ότι η διατήρηση και η μετέπειτα χρησιμοποίηση των δεδομένων πραγματοποιούνται χωρίς ο συνδρομητής ή ο καταχωρισμένος χρήστης να είναι ενήμεροι σχετικώς δύναται να προκαλέσει στα ενδιαφερόμενα πρόσωπα το αίσθημα ότι η ιδιωτική τους ζωή παρακολουθείται διαρκώς.

Το δικαστήριο αντιδρά κυρίως σε τέσσερα σημεία της οδηγίας:

- Καλύπτει δυνητικά το σύνολο του πληθυσμού χωρίς να γίνεται καμία διαφοροποίηση, περιορισμός ή εξαίρεση με βάση τον σκοπό της καταπολέμησης των σοβαρών αδικημάτων.
- Δεν διασφαλίζεται ότι οι αρμόδιες εθνικές αρχές δεν θα έχουν πρόσβαση στα δεδομένα και δε θα μπορούν να τα χρησιμοποιήσουν παρά μόνο για να προλάβουν, να διαπιστώσουν ή να διώξουν ποινικώς αδικήματα δυνάμενα να θεωρηθούν, υπό το πρίσμα της έκτασης και της σοβαρότητας της επέμβασης στην άσκηση των επίμαχων θεμελιωδών δικαιωμάτων, επαρκώς σοβαρά για να δικαιολογήσουν μια τέτοια επέμβαση και δεν προβλέπει τις ουσιαστικές και διαδικαστικές προϋποθέσεις υπό τις οποίες οι αρμόδιες εθνικές αρχές μπορούν να έχουν μετέπειτα πρόσβαση στα δεδομένα και να τα χρησιμοποιήσουν. Η πρόσβαση στα δεδομένα δεν εξαρτάται από τον προηγούμενο έλεγχο δικαστηρίου ή ανεξάρτητης διοικητικής αρχής.
- Επιβάλλεται μία περίοδος διατήρησης των δεδομένων χωρίς να γίνεται καμία διάκριση μεταξύ των κατηγοριών των δεδομένων σε συνάρτηση με τα ενδιαφερόμενα πρόσωπα ή με την ενδεχόμενη χρησιμότητα των δεδομένων σε σχέση με τον επιδιωκόμενο σκοπό. Επιπλέον, η διάρκεια αυτή ορίζεται μεταξύ των έξι μηνών κατ' ελάχιστο και των εικοσιτεσσάρων μηνών κατά μέγιστο όριο, χωρίς η οδηγία να διευκρινίζει τα αντικειμενικά κριτήρια βάσει των οποίων πρέπει να καθορίζεται η διάρκεια διατηρήσεως για να διασφαλίζεται ο περιορισμός της στο αυστηρώς αναγκαίο.
- Δεν προβλέπονται ασφαλιστικές δικλείδες για την διασφάλιση της αποτελεσματικής προστασίας των δεδομένων κατά των κινδύνων καταχρήσεως καθώς και κατά οποιασδήποτε αθέμιτης προσβάσεως ή χρησιμοποιήσεως των δεδομένων[15] .

3.2 Διατήρηση - Επεξεργασία Προσωπικών Δεδομένων

Οι προϋποθέσεις για την για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής ορίζονται από τον Νόμο 2472 "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Ο νόμος ορίζει την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως τον φορέα εκείνο ο οποίος είναι επιφορτισμένος με τον έλεγχο εφαρμογής του. Αναλυτικότερα τα βασικά καθήκοντα της Αρχής είναι:

[15] Δικαστήριο της Ευρωπαϊκής Ένωσης. (2014). Απόφαση στις συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12. Λουξεμβούργο: Δικαστήριο της Ευρωπαϊκής Ένωσης.

- Έκδοση οδηγιών για την εφαρμογή των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Επίβλεψη κωδίκων δεοντολογίας από φορείς που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής και των εν γένει δικαιωμάτων και θεμελιωδών ελευθεριών των φυσικών προσώπων στον τομέα της δραστηριότητάς τους.
- Συστάσεις προς φορείς που διατηρούν προσωπικά δεδομένα
- Χορήγηση αδειών επεξεργασίας προσωπικών δεδομένων
- Καταγγελία σχετικών παραβάσεων, επιβολή διοικητικών κυρώσεων, διενέργεια διοικητικών εξετάσεων, διενέργεια διοικητικών ελέγχων.
- Γνωμοδότηση για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.
- Έκδοση κανονιστικών πράξεων για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων.
- Ενημέρωση της Βουλής των Ελλήνων για παραβάσεις των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Σύνταξη ετήσιας έκθεση για την εκτέλεση της αποστολής .
- Εξέταση παραπόνων υποκειμένων δεδομένων προσωπικού χαρακτήρα.
- Συνεργασία με αντίστοιχες αρχές κρατών μελών της Ευρωπαϊκής Ένωσης
- Ασκεί ανεξάρτητο έλεγχο στο εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν.

Ο νόμος αφορά κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:

- Από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο.
- Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους- Μέλους της Ευρωπαϊκής Ένωσης ή κράτους του Ευρωπαϊκού Οικονομικού Χώρου, αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν.

Η επεξεργασία των προσωπικών δεδομένων είναι επιτρεπτή, σύμφωνα με τον νόμο αν:

- συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και υφίστανται θεμιτή και νόμιμη επεξεργασία για την εξυπηρέτηση και μόνο των σκοπών αυτών.
- είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.
- είναι ακριβή και ενημερωμένα.
- βρίσκονται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή

μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.

Ορίζεται ότι είναι θεμιτή η καταγραφή ήχου και εικόνας σε περιπτώσεις εξέτασης τέλεσης αξιόποινων πράξεων με εντολή εισαγγελικής αρχής ή όταν ο σκοπός της είναι διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημόσιας ασφάλειας, η διαχείριση της κυκλοφορίας. Στην περίπτωση αυτή το ληφθέν τηρείται για χρονικό διάστημα επτά ημερών, μετά το πέρας των οποίων καταστρέφεται με πράξη του αρμόδιου εισαγγελέα.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του ή όταν συντρέχουν ένας ή περισσότεροι από του εξής λόγους:

- Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.
- Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.
- Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
- Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.
- Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών [16] .

Ειδικότερα όσον αφορά τα θέματα λήψης ήχου και εικόνας η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εξέδωσε την Οδηγία 1/2011. Η οδηγία αυτή αφορά κυρίως την προστασία προσώπων και αγαθών καθώς και την παροχή υπηρεσιών υγείας. Η οδηγία ορίζει ως συστήματα βιντεοεπιτήρησης εκείνα που είναι μόνιμα εγκατεστημένα σε ένα χώρο, λειτουργούν συνεχώς ή σε τακτά χρονικά διαστήματα και έχουν τη δυνατότητα λήψης ή/και μετάδοσης σήματος εικόνας ή/και ήχου από τον χώρο αυτό προς έναν περιορισμένο αριθμό οθονών προβολής ή/και μηχανημάτων καταγραφής. Καθορίζονται επίσης οι προδιαγραφές ανά περίπτωση των ρυθμίσεων λήψης εικόνας και ήχου με γνώμονα την αποκλειστική εξυπηρέτηση

[16] Ελληνική Δημοκρατία. (1997). ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ. Ανάκτηση από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαθέσιμο στο http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#top

του σκοπού βιντεσκόπησης και μόνο. Για τον χρόνο διατήρησης του ληφθέντος υλικού καθορίζεται:

- Τα δεδομένα πρέπει να τηρούνται για συγκεκριμένο χρονικό διάστημα ενόψει του επιδιωκόμενου κάθε φορά σκοπού επεξεργασίας. Σε κάθε περίπτωση, εφόσον από τη λήψη εικόνων που αποθηκεύονται ή τη λήψη που γίνεται σε πραγματικό χρόνο δεν προκύπτει επέλευση συμβάντος που εμπίπτει στον επιδιωκόμενο σκοπό, τα δεδομένα πρέπει να καταστρέφονται το αργότερο μέσα σε δεκαπέντε εργάσιμες ημέρες.
- Σε περίπτωση συμβάντος σε βάρος του προσώπου ή των αγαθών του υπεύθυνου επεξεργασίας, αυτός επιτρέπεται να τηρεί τις εικόνες στις οποίες έχει καταγραφεί το συγκεκριμένο συμβάν σε χωριστό αρχείο για 30 ημέρες.
- Αν το συμβάν αφορά τρίτον, ο υπεύθυνος επεξεργασίας επιτρέπεται να τηρεί τις εικόνες για 3 μήνες.

Όσο αφορά την διαβίβαση του υλικού, αυτή μπορεί να γίνει με την συγκατάθεση του υποκειμένου ή με την παραγγελία εισαγγελικής ή αστυνομικές αρχές ή όταν αυτό αποτελεί αποδεικτικό στοιχείο για αξιόποινη πράξη [17].

3.3 Συμπεράσματα

Η συγκέντρωση και η διατήρηση κάθε είδους δεδομένων διευκολύνει σίγουρα την μεταγενέστερη έρευνα για την απόδοση ευθυνών σε αξιόποινες πράξεις. Ωστόσο αυτές ακριβώς οι ενέργειες μπορούν να οδηγήσουν στην απώλεια θεμελιωδών συνταγματικών δικαιωμάτων των πολιτών που σχετίζονται με τα ευαίσθητα προσωπικά τους δεδομένα. Οι Ευρωπαίοι νομοθέτες στην προσπάθεια τους κυρίως να διασφαλίσουν την προστασία της Ευρωπαϊκής Ένωσης από την διεθνή τρομοκρατία οδηγούνται στην πρόταση νόμων και οδηγιών που προσβάλλουν σε μεγάλο βαθμό τα δικαιώματα αυτά. Οι ρυθμοί ανάπτυξης της τεχνολογίας στους τομείς της πληροφορικής και των τηλεπικοινωνιών έχει βρει τους αντιπροσώπους της νομικής επιστήμης αρκούντος απροετοίμαστους. Έτσι ενώ οι τεχνολογικές προκλήσεις είναι εδώ και πολλά χρόνια παρούσες και με μεγάλη δυναμική οι νομικοί δεν είναι έτοιμοι να απαντήσουν.

Η χρήση των στοιχείων που με ευκολία και σε πλούσια ποσότητα μπορεί να παρέξει η τεχνολογία θα πρέπει να γίνουν αντικείμενα εκμετάλλευσης από τα δικαστήρια με τρόπο που να μην προσβάλει τα δικαιώματα των πολιτών. Σε κάθε περίπτωση μάλιστα η διαχείριση των στοιχείων αυτών θα πρέπει να γίνεται από φορείς του δημοσίου είτε σε Εθνικό είτε σε Ευρωπαϊκό (κοινοτικό) επίπεδο. Παράλληλα είναι ανάγκη να θεσπιστούν αυστηρές προδιαγραφές και ασφαλιστικές δικλίδες τόσο για την αποτροπή της διαρροής τους σε αναρμόδιους φορείς και πρόσωπα όσο και για την ακεραιότητα τους. Η ίδια η τεχνολογία της πληροφορικής και των τηλεπικοινωνιών είναι σε θέση να παρέχει μεθόδους για την επίτευξη των σκοπών αυτών

[17] Ελληνική Δημοκρατία. (1997). ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ. Ανάκτηση από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαθέσιμο στο http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#top

(κρυπτογραφία, εξουσιοδοτημένη πρόσβαση, ασφάλεια αποθήκευσης). Συνέπεια της μέριμνας αυτής μπορεί να είναι η διατήρηση μεγάλου όγκου αποδεικτικών στοιχείων με ασφάλεια, χωρίς να προσβάλλεται το υποκείμενο που αφορούν τα στοιχεία αυτά, για μεγάλα χρονικά διαστήματα και μάλιστα συμπεριλαμβάνοντας στον όγκο των στοιχείων αυτών περισσότερο ουσιώδη στοιχεία για την διερεύνηση αξιόποινων πράξεων.

ΚΕΦΑΛΑΙΟ 4 : ΧΡΗΣΗ ΑΝΑΛΥΣΗΣ ΙΣΤΟΡΙΚΟΥ ΚΙΝΗΤΩΝ ΩΣ ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ ΣΕ ΜΙΑ ΔΙΚΗ

4.1 Λειτουργία του Δικτύου Κινητής Τηλεφωνίας

Προκειμένου να γίνει αντιληπτή η δυνατότητα εκμετάλλευσης του ιστορικού των κινητών τηλεφώνων ως αποδεικτικά στοιχεία, θεωρείται σκόπιμη μία συνοπτική ανάλυση της αρχιτεκτονικής και της λειτουργίας ενός τυπικού δικτύου κινητής τηλεφωνίας. Ένα τυπικό δίκτυο αποτελείται από:

- Σταθμό βάσης ΣΒ (Base Transceiver station BTS): Εκπέμπει και δέχεται σήματα από συσκευές κινητής τηλεφωνίας και τα επεξεργάζεται με βάση συγκεκριμένα πρωτόκολλα. Στην συνέχεια συνδέεται έπειτα, με το BCS. Μετατρέπει επίσης τα δεδομένα φωνής από μορφή που εξυπηρετεί την ασύρματη διάδοση σε μορφή που εξυπηρετεί την ενσύρματη διάδοση.
- Ελεγκτή σταθμού βάσης (Base Station Controller BCS): Ελέγχει και συντονίζει την λειτουργία μίας ομάδας σταθμών βάσης για την πραγματοποίηση των επικοινωνιών. Συνδέεται με το κέντρο μεταγωγής.
- Κέντρο μεταγωγής (Mobile Switching Centre MSC): λειτουργεί ως κόμβος μεταγωγής στο ενσύρματο δημόσιο δίκτυο τηλεφωνίας. Συνδέεται με τις περιοχές καταγραφής και πιστοποίησης ώστε να μπορεί να γίνεται η ταυτοποίηση των συνδρομητών των υπηρεσιών κινητής τηλεφωνίας.
- Περιοχές καταγραφής και Πιστοποίηση: Περιλαμβάνει καταγραφείς των στοιχείων των συνδρομητών, των κλήσεων που πραγματοποίησαν και το κέντρο πιστοποίησής τους. Από εκεί γίνεται η δρομολόγηση των κλήσεων ανάλογα με την θέση του κάθε συνδρομητή.

Για τον προσδιορισμό καλουμένου και καλούντος υπάρχει ένα πλήθος ταυτοτήτων που αποθηκεύονται στην κάρτα SIM του κινητού τηλεφώνου:

- International mobile equipment identity (IMEI): Αποτελεί την μοναδική ταυτότητα της συσκευής (IMEI). Είναι ένας 15ψήφιος αριθμός που τοποθετείται στη συσκευή κατά τη διάρκεια κατασκευής της. Ο IMEI ελέγχεται κατά την εγκαθίδρυση των κλήσεων ώστε να διαπιστωθεί αν η συσκευή επιτρέπεται να συνδεθεί, πρέπει να παρακολουθηθεί ή αν έχει αναφερθεί ως κλεμμένη συσκευή.
- International mobile subscriber identity (IMSI): Αποτελεί μοναδική ταυτότητα του συνδρομητή και τον αντιστοιχεί στην συσκευή.
- Temporary mobile subscriber identity: Προσωρινή ταυτότητα συνδρομητή που παρέχεται ώστε να διευκολύνει την ταυτοποίηση κατά την διάρκεια της επικοινωνίας αφού είναι μικρότερη σε μήκος από την IMSI.
- Authentication key and cipher key: Χρησιμοποιείται για την πρόσβαση στα μηνύματα κινητής τηλεφωνίας.

Η διαδικασία κλήσεων σε δίκτυα κινητής τηλεφωνίας περιλαμβάνει τα παρακάτω στάδια:

- Ενεργοποίηση Συσκευής – Σύνδεση στο Δίκτυο: Το χρονικό διάστημα που μεσολαβεί από την ενεργοποίηση μίας συσκευής κινητής τηλεφωνίας μέχρι την

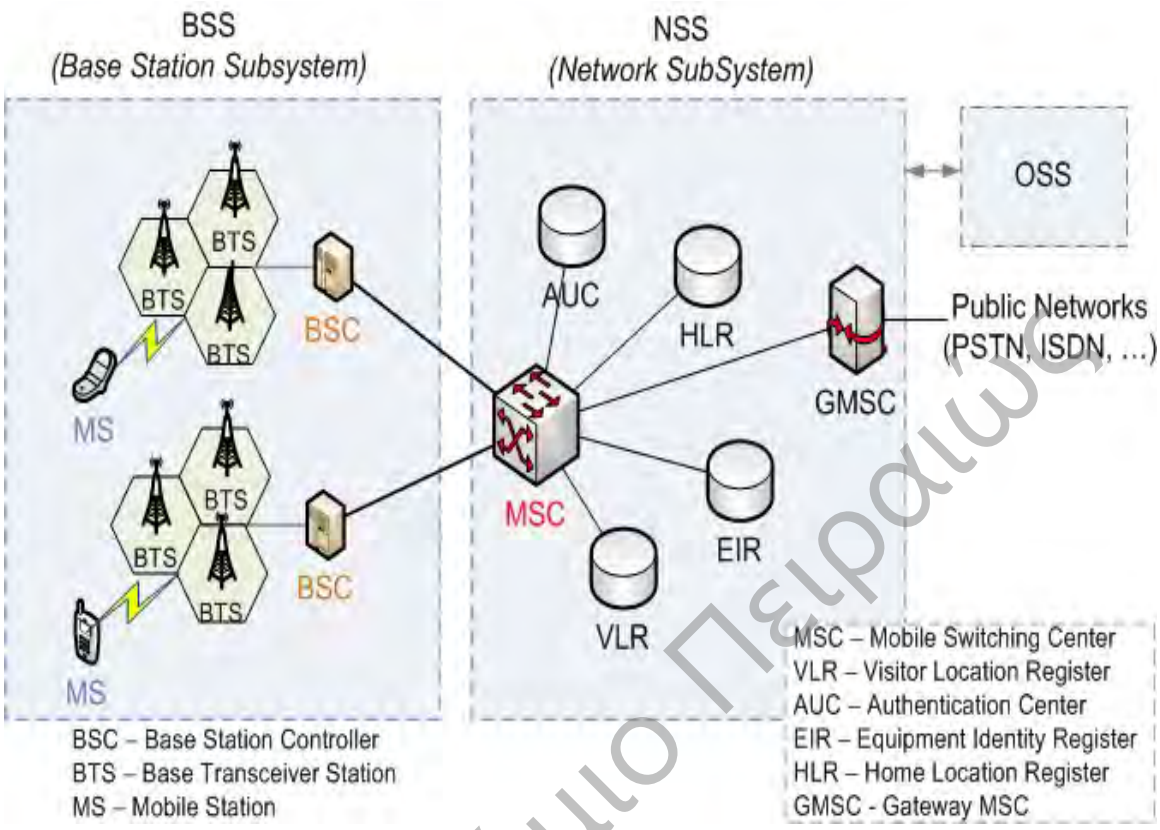
στιγμή που είναι συνδεδεμένη στο δίκτυο και έτοιμη να πραγματοποιήσει ή να δεχθεί κλήση, γίνεται η σύνδεσή της στο δίκτυο. Σε αυτό αναζητά τον σταθμό βάσης ανάμεσα στα σχετικά σήματα που αποστέλλοντας έναν μοναδικό αναγνωριστή για τον σταθμό βάσης μαζί με ένα αναγνωριστικό δικτύου. Συνδέεται τελικά με την ισχυρότερη συχνότητα διαστρωμάτωσης και μετά χρησιμοποιώντας το τυχαίας πρόσβασης κανάλι στέλνει το κανάλι καταχώρησης. Το δίκτυο απαντάει, ελέγχοντας την πιστοποίηση και αποθηκεύοντας τη θέση της συσκευής στο σύστημα πιστοποίησης.

- Έναρξη κλήσης: Η συσκευή επικοινωνεί με τον σταθμό βάσης προκειμένου να ξεκινήσει η κλήση. Στέλνει κατάλληλο σήμα ώστε να ξεκινήσει η διαδικασία εύρεσης ελεύθερου καναλιού για την επικοινωνία. Σε περίπτωση επιτυχίας ο σταθμός βάσης επιστρέφει έναν τυχαίο αριθμό και αποδίδει στη κινητή συσκευή ένα ραδιοκανάλι για την επικοινωνία.
- Λήψη κλήσης: Το δίκτυο ελέγχει για την τελευταία καταχωρημένη θέση της κινητής συσκευής και δρομολογεί την κλήση στην αντίστοιχη ομάδα σταθμών βάσης. Όταν η συσκευή λάβει την κλήση στέλνει απάντηση και πλέον το δίκτυο αναλαμβάνει την εγκαθίδρυση της επικοινωνίας και την ανταλλαγή των μηνυμάτων.
- Τερματισμός της κλήσης
- Μία κλήση τερματίζεται κι από τα δύο άκρα της σύνδεσης. Με την διακοπή της κλήσης ελέγχεται από το δίκτυο αν έχει τερματιστεί ομαλά ή αν διακόπηκε χωρίς την θέληση των συμμετεχόντων. Με την ολοκλήρωση της κλήσης απελευθερώνεται και το κανάλι επικοινωνίας που χρησιμοποιήθηκε.
- Μεταγωγή: Οι κινητές συσκευές έχουν την δυνατότητα να ελέγχουν κάθε φορά αν μετακινούνται σε νέα κυψέλη και αν θα πρέπει να εξυπηρετηθούν από άλλο σταθμό βάσης ακόμα και να βρίσκονται σε κατάσταση επικοινωνίας στα πλαίσια μίας κλήσης. Από τα χαρακτηριστικά των γειτονικών σταθμών βάσης και των αποκρίσεων της κινητής συσκευής στην αναζήτηση του καλύτερου σήματος, το δίκτυο αποφασίζει αν θα χρειαστεί η μετάβαση της συσκευής σε άλλον σταθμό βάσης.
- Υπηρεσία μικρών μηνυμάτων (Short Message Service SMS): Με την υπηρεσία αυτή παρέχεται η δυνατότητα εκπομπής και λήψης μηνυμάτων κειμένου προς και από τις κινητές συσκευές. Τα μηνύματα από τον αποστολέα δρομολογούνται σε ένα κέντρο μηνυμάτων και μετά στον παραλήπτη. Η παραλαβή από τον παραλήπτη δημιουργεί μία αναφορά παράδοσης προς το κέντρο μηνυμάτων.

Από την παραπάνω περιγραφή φαίνεται ότι η χρήση της κινητής τηλεφωνίας μπορεί να προσφέρει πολλά, πλούσια και ουσιαστικά αποδεικτικά στοιχεία στην αποδεικτική διαδικασία[18].

Στην επόμενη εικόνα φαίνεται σχηματικά η λειτουργία του δικτύου κινητής τηλεφωνίας.

[18] ΕΑΠ, Global System for Mobile Communication (GSM), διαθέσιμο στο http://edu.eap.gr/pli/pli23/documents/Parallila_Keimena/GSM.pdf



Εικόνα 11: Λειτουργία Δικτύου κινητής τηλεφωνίας

4.2 Ανάλυση Ιστορικού

Η ανάλυσης του ιστορικού κινητού τηλεφώνου (CSA) είναι μια διαδικασία που εκτελείται από ένα εξειδικευμένο μηχανικό ή αναλυτή, χρησιμοποιώντας τα στοιχεία κλήσεων που αποθηκεύονται από έναν φορέα εκμετάλλευσης δικτύου κινητής τηλεφωνίας. Οι σχετικές με τις κλήσεις πληροφορίες, που είναι γνωστές ως το Call Data Records (CDR) και τα δεδομένα ρύθμισης της συσκευής κινητής τηλεφωνίας (Cell Configuration Data), μπορούν να αναλυθούν συνδυασμένα προκειμένου να ερευνηθεί αν μια συσκευή κινητού τηλεφώνου ή κάρτα SIM μπορεί να σχετίζονται με μία παρελθούσα κλήση ή ένα συμβάν. Η ανάλυση των δεδομένων αυτών μπορεί να γίνει είτε για τηλεφωνικές συνδέσεις συμβολαίου ή καρτοκινητής.

Η χρήση κάρτας SIM για τηλεφώνημα, δεν μπορεί να αποτελέσει απόδειξη ότι την κλήση την έκανε ο ιδιοκτήτης της. Λεπτομερής ανάλυση των αρχείων δεδομένων κλήσεων για παρατεταμένο χρονικό διάστημα μπορεί να βοηθήσει να καθορίσει ποιος θα μπορούσε να έχει ο χρήστης της συσκευής ή της κάρτας SIM σε μια συγκεκριμένη χρονική στιγμή.

Η ανάλυση των αρχείων του κινητού τηλεφώνου είναι συνήθως γίνεται σε δύο στάδια:

- Ανάλυση της γενικής συμπεριφοράς του συνδρομητή ώστε να προσδιοριστούν τα πρότυπα της επικοινωνίας του με την χρήση κινητού τηλεφώνου
- Αναζήτηση χρονικών και τοπικών λεπτομερειών εκτέλεσης ή λήψης κλήσεων ή αποστολής και λήψης γραπτών μηνυμάτων.

Σε μια ποινική δίκη, η θέσπιση θέσης του κατηγορουμένου κατά τη διάρκεια της διάπραξη των εγκλημάτων που του χρεώνονται στο κατηγορητήριο είναι σημαντική για τον προσδιορισμό της κριτικής επιτροπής του εάν ο εναγόμενος είναι ένοχος για τα εγκλήματα που του προσάπτονται.

Η μαρτυρία ενός αυτόπτη μάρτυρα και τα φυσικά στοιχεία που παραδοσιακά υπήρξαν και συνεχίζουν να είναι η πρωτογενής μέθοδος απόδειξης της θέσης του κατηγορουμένου σε χρόνους και τόπους που σχετίζονται με τα αδικήματα για τα οποία κατηγορείται. Αυτό το είδος μαρτυρίας ονομάζεται "απόδειξη τοποθεσίας κατηγορουμένου." Πολλάκις, περιπτώσεις που έχουν πάει σε δίκη περιλαμβάνουν ελάχιστα ή και καθόλου φυσικά στοιχεία, όπως δακτυλικά αποτυπώματα ή DNA, και η μαρτυρία των μαρτύρων συνήθως αμφισβητείται από την υπεράσπιση για λόγους αξιοπιστίας. Οι δικηγόροι συνήθως ανακρίνουν θύματα και ορίζουν μάρτυρες που καταθέτουν για την «απόδειξη τοποθεσίας κατηγορουμένου» με βάση ποικίλες ικανότητες τους να αντιλαμβάνονται με ακρίβεια, και να ανακαλέσουν τις εν λόγω αποδείξεις βασισμένοι σε στοιχεία. Από την άλλη οι εμπιστευτικοί πληροφοριοδότες και οι «βαλτοί» μάρτυρες δεν θεωρούνται στοιχεία αναφορές και οι πληροφορίες τους είναι αβάσιμες.

Οι μάρτυρες επιβολής είναι συχνά αντιμέτωποι με μία ή και τις δύο αυτές τακτικές άμυνας που έχουν σχεδιαστεί για να εγείρουν αμφιβολίες ενόρκων για την απόδειξη κατηγορούμενος θέση.

Σήμερα, οι παραδοσιακές «αποδείξεις τοποθεσίας κατηγορουμένου» μπορεί να συμπληρωθούν με την χρήση αποδεικτικών στοιχείων που προκύπτουν από την ανάλυση Historical Cell Site (CSA) σε περιπτώσεις όπου ένα ή περισσότερα κινητά τηλέφωνα μπορούν να συνδεθούν με κατηγορούμενους, συνεργούς, τα θύματα, ή μάρτυρες σε χρόνους και τόπους που σχετίζονται με τα αδικήματα που βρίσκονται υπό έρευνα. Τα αποδεικτικά στοιχεία που προσκομίζονται μέσω της CSA θεωρούνται "ιστορική" στη φύση επειδή τα αρχεία που χρησιμοποιούνται στην ανάλυση είναι ιστορικά αρχεία ολοκληρωμένων κλήσεων μέσω κινητού τηλεφώνου σταλμένα μηνύματα κειμένου. Τα ιστορικά αποδεικτικά στοιχεία μέσω CSA περιλαμβάνουν τη χρήση αναλυτικών εγγραφών των κλήσεων που πραγματοποιήθηκαν (CDR) για να προσδιορισθεί η τοποθεσία και η σειρά των δραστηριοτήτων με βάση πάντα τις κλήσεις που πραγματοποιήθηκαν ή τα μηνύματα κειμένου που στάλθηκαν μέσω του κινητού τηλεφώνου. Η μείωση της γεωγραφικής θέσης των κινητών τηλεφώνων σε συγκεκριμένες χρονικές στιγμές είναι χρήσιμο για τον καθορισμό της εγγύτητας των στοιχείων που βρέθηκαν όσον αφορά την τοποθεσία και τις κινήσεις των χρηστών των κινητών τηλεφώνων[19].

4.3 Συμπεράσματα

Τα κινητά τηλέφωνα και η κάθε είδους έξυπνες συσκευές που χρησιμοποιούν τα δίκτυα κινητής τηλεφωνίας έχουν εδώ και δύο δεκαετίες περίπου, γίνει απαραίτητα για την καθημερινότητα κάθε ανθρώπου. Δεν θα ήταν υπερβολικό να υποστηρίξει κάποιος ότι δεν υπάρχει ενήλικος άνθρωπος στην Ευρώπη ο οποίος δεν χρησιμοποιεί έστω μία συσκευή κινητής τηλεφωνίας. Όπως παρουσιάστηκε στο παρόν κεφάλαιο η ίδια η φύση των δικτύων κινητής τηλεφωνίας και η λειτουργίες των συσκευών είναι ικανά να προσφέρουν ουσιαστικά και αδιάσειστα αποδεικτικά στοιχεία για τους χρήστες τους. Κατά συνέπεια η ύπαρξη κατάλληλου θεσμικού πλαισίου είναι δυνατόν να ενισχύσει την αποδεικτική διαδικασία στις δικαστικές αίθουσες με ισχυρά αποδεικτικά

[19] T. O'Shea, J.Darnell, Admissibility of forensic cell phone evidence, σελ. 42-51

στοιχεία. Προς αυτήν την κατεύθυνσης ήταν και η πρόσφατη ρύθμιση που αφορούσε τα καρτοκινητά και την υποχρέωση των ιδιοκτητών τους να πιστοποιηθούν. Χρειάζεται ωστόσο μία εκστρατεία ενημέρωσης των πολιτών ώστε να ξέρουν το πώς μπορούν να διασφαλίσουν ότι κάποιος τρίτος δεν μπορεί να συμμετέχει σε επικοινωνία μέσω δικτύου κινητής τηλεφωνίας προσποιούμενος τον ίδιους. Αυτός είναι άλλωστε και ο μόνος παράγοντας ο οποίος μπορεί να ακυρώσει τέτοιου είδους αποδεικτικά στοιχεία.

ΕΠΙΛΟΓΟΣ

Οι νέες τεχνολογίες πληροφορικής και τηλεπικοινωνιών γνώρισαν ραγδαία ανάπτυξη τα τελευταία χρόνια. Ειδικότερα η ανάπτυξη του διαδικτύου τις τελευταίες δύο δεκαετίες έφερε τον άνθρωπο πολύ κοντά με τα τεχνολογικά επιτεύγματα. Η νομική επιστήμη δεν έδειξε έγκαιρα ανεπτυγμένα αντανακλαστικά στις εξελίξεις αυτές με αποτέλεσμα σήμερα να έχει μείνει αρκετά «πίσω» και να πασχίζει να τις προλάβει. Οι Ευρωπαίοι νομοθέτες πλέον εκ των πραγμάτων οφείλουν και μεριμνούν στα νομοθετήματα τους να λαμβάνουν υπ' όψη το διαμορφωμένο τεχνολογικό περιβάλλον. Η αργοπορία της αντίδρασης των νομικών οδηγεί ακόμα και σήμερα σε διατάξεις και οδηγίες οι οποίες συγκρούονται με βασικά δικαιώματα των Ευρωπαίων πολιτών. Το γεγονός αυτό καταδεικνύει ότι είναι ανάγκη να υπάρχει σύμπραξη των νομικών με επιστήμονες της πληροφορικής και των τηλεπικοινωνιών ώστε να παράγεται αποτέλεσμα το οποίο θα διασφαλίζει στον μέγιστο βαθμό τις συνταγματικές ελευθερίες και που θα συνδράμει αποφασιστικά στην επιβολή του δικαίου.

Εκτός όμως από την παθητική προσαρμογή του Δικαίου στις τεχνολογικές εξελίξεις, χρειάζεται και η ενσωμάτωση των εξελίξεων αυτών στην νομική. Πρέπει δηλαδή τα κάθε είδους επιτεύγματα της πληροφορικής και των τηλεπικοινωνιών να τύχουν εκμετάλλευσης από την δικαστική και την νομοθετική εξουσία ώστε να γίνεται αποδοτικότερη εφαρμογή του Δικαίου. Ένας κλασικό παράδειγμα είναι η θεσμική κατοχύρωση της προηγμένης ψηφιακής υπογραφής το οποίο όμως είναι μόνο ένα βήμα. Η τεχνολογία έχει διαθέσιμα πολλά εργαλεία τα οποία με κατάλληλες προσαρμογές μπορούν να γίνουν καταλύτες στην προσπάθεια απόδοσης Δικαιοσύνης. Αυτός είναι και ο σκοπός του κλάδου της Νομικής Πληροφορικής, ενός κλάδου του οποίου πρέπει να διαμορφωθεί κατάλληλος προσανατολισμός και να του τεθούν σαφείς στρατηγικοί και επιχειρησιακοί στόχοι.

Αναφορές

Ιγγλεζακης Ι., Νομική Πληροφορική,2012

Jan Valdman, Log file analysis, σελ 4-7, διαθέσιμο στο http://www.kiv.zcu.cz/site/documents/verejne/vyzkum/publikace/technicke-zpravy/2001/tr-2001-04.pdf

M. Krotoski, J. Passwaters, Using log record analysis to show internet and computer activity in criminal classes, σελ 16 - 34, διαθέσιμο στο http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf

Καράκωστας, Δίκαιο και ίντερνετ. Νομικά ζητήματα του διαδικτύου, 2003

Σινανιώτη-Μαρούδη Ηλεκτρονική τραπεζική, σελ 367

Σ. Κουσούλης, Σύγχρονες μορφές έγγραφης συναλλαγής, 1992

Δ. Πουλάκης, Κρυπτογραφία, 2004

Δ. Μανιώτης, Η ψηφιακή υπογραφή ως μέσο διαπίστωσης της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο, 1998

Ε. Παπακωνσταντίνου, Νομικά θέματα πληροφορικής, 2006

Κ. Χριστοδούλου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία, 2001

Δικαστήριο της Ευρωπαϊκής Ένωσης. (2014). Απόφαση στις συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12. Λουξεμβούργο: Δικαστήριο της Ευρωπαϊκής Ένωσης.

M. Krotoski, Effectively Using Electronic Edidence before and at trial, σελ 52-71, διαθέσιμο στο http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf

Ελληνική Δημοκρατία. (1997). ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ. Ανάκτηση από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#top

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ. (2001). ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ' ΑΡΙΘ. 150/2001 (ΦΕΚ 125 Α΄/25-6-2001) . ΑΘΗΝΑ: ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ.

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ. (2004). ΠΔ 287/2001 ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΧΡΗΣΗ ΕΙΔΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΚΕΥΩΝ ΓΙΑ ΤΗΝ ΚΑΤΑΓΡΑΦΗ ΚΑΙ ΒΕΒΑΙΩΣΗ ΠΑΡΑΒΑΣΕΩΝ ΤΟΥ ΚΟΚ. ΑΘΗΝΑ: ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ.

Ελληνική Δημοκρατία. (2006). Νόμος υπ'αρ.3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσίων. Αθήνα: Ελληνική Δημοκρατία.

Κουσούλης, Σ. . Σύγχρονες μορφές έγγραφης συναλλαγής.

Παπαδημητρίου, Γ. (2010). Network Forensics. Ανάκτηση από https://www.cs.ucy.ac.cy/courses/EPL674/lectures/Forensics-GR.pdf

ΠΡΩΤΟΔΙΚΕΙΟ ΑΘΗΝΩΝ. (2004). Αριθμός απόφασης 1963/2004. Ανάκτηση από Δικηγορικός Σύλλογος Αθηνών: ΠΡΩΤΟΔΙΚΕΙΟ ΑΘΗΝΩΝ

Χριστοδούλου, Κ.. Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία.

T. O'Shea, J.Darnell, Admissibility of forensic cell phone evidence, σελ. 42-51