ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΡΟΣΟΜΟΙΩΣΗ ΣΕΝΑΡΙΩΝ ΨΗΦΙΑΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΜΕ ΤΟΝ ΠΡΟΣΟΜΟΙΩΤΗ CUPCARBON

Διπλωματική Εργασία

του

Κασούμη Νικολάου (ΜΑΙ 17044)

Θεσσαλονίκη, 10/2018

ΠΡΟΣΟΜΟΙΩΣΗ ΣΕΝΑΡΙΩΝ ΨΗΦΙΑΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΜΕ ΤΟΝ ΠΡΟΣΟΜΟΙΩΤΗ CUPCARBON

Κασούμης Νικόλαος

Πτυχίο Μηχανικών Πληροφορικής, ΑΤΕΙ Καστοριάς, 2014

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Φουληράς Παναγιώτης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29/10/2018

Φουληράς Παναγιώτης	Μαυρίδης Ιωάννης	Βεργίδης Κωνσταντίνος
.....	.....	.....

Κασούμης Νικόλαος

.....

Περίληψη

Η καθημερινότητα μας είτε πρόκειται για την ιδιωτική ζωή μαζί με οικογένειά ή φίλους, είτε στο χώρο της εργασίας, τα τελευταία χρόνια έχει άμεση σχέση με το Διαδίκτυο, τα έξυπνα κινητά και με μια πληθώρα ηλεκτρονικών συσκευών που είναι συνδεδεμένα μεταξύ τους και με το Διαδίκτυο. Εξαιρώντας όλες τις τρομερές διευκολύνσεις που μας προσφέρει η χρήση τους, υπάρχει η αντίθετη πλευρά και συγκεκριμένα, τα προβλήματα ασφαλείας και τα τρωτά σημεία που οι κακόβουλοι χρήστες μπορούν να παραβιάσουν, ώστε να αποσπάσουν χρήσιμες για αυτούς πληροφορίες.

Η παρούσα διπλωματική εργασία λοιπόν, μελετά την ανάγκη για ασφάλεια και αναλύει την επιστήμη της Ψηφιακής Εγκληματολογίας, καθώς και τις μεθόδους που χρησιμοποιούν οι ερευνητές, κατά την διάρκεια μιας έρευνας. Στη συνέχεια γίνεται επισκόπηση του Internet of Things (αρχιτεκτονική, χαρακτηριστικά), καθώς και οι προκλήσεις ασφαλείας που υπάρχουν. Περιγράφεται πώς μπορεί το IoT να συμβάλλει στην Ψηφιακή Εγκληματολογία, αλλά και ποιες προκλήσεις δημιουργεί. Επίσης, εξετάζονται οι μέθοδοι εγκληματολογίας που υπάρχουν στην βιβλιογραφία.

Στο πρακτικό μέρος της διπλωματικής προβάλλονται τρία σενάρια επίθεσης σε συσκευές του IoT που τυγχάνουν ευρείας χρήσης στην καθημερινότητα με την χρήση του προσομοιωτή CupCarbon. Σκοπός είναι να παρουσιαστούν τα μοντέλα εγκληματολογίας στην πράξη, οι δυνατότητες του προσομοιωτή CupCarbon και η συλλογή αποδεικτικών στοιχείων τα οποία αποκομίζονται από τα αντικείμενα που συμμετέχουν στις προσομοιώσεις.

Λέξεις Κλειδιά:Ψηφιακή Εγκληματολογία, Διαδίκτυο των Πραγμάτων, Internet of Things (IoT), Εγκληματολογία στο Διαδίκτυο των Πραγμάτων, IoT Forensics, προσομοίωση, CupCarbon

Abstract

Our daily routine, whether it is private home life with family or friends, or in the workplace, has in recent years been directly related to the Internet, smartphones and plenty electronic devices that are connected to each other and with Internet. Excluding all the tremendous facilities offered by their use, there is and the opposite side and specifically, the security issues and vulnerabilities that malicious users may violate in order to obtain useful information for them.

Therefore this dissertation examines the need for security and analyzes the science of Digital Forensics, as well as the methods used by Digital Forensics scientists during an investigation. Afterwards the architecture of the Internet of Things is presented,features and security challenges that exist. It is described the way that IoT can contribute in Digital Forensics, but also what challenges isintroduced. Also, we examine the models of IoT Forensics that exist in bibliography.

In the applied part of the dissertation, three attack scenarios are presented on IoT devices that are widely used in everyday life using the CupCarbon simulator. The aim is to present the IoT Forensic models in practice, the capabilities of the CupCarbon simulator and the collection of evidence obtained from the objects involved in the simulations.

Keywords: Digital forensics, Internet of Things (IoT), IoT Forensics, simulation, CupCarbon

Ευχαριστίες

Με το πέρας αυτής της διπλωματικής εργασίας θα πρέπει να ευχαριστήσω την οικογένειά μου που στάθηκε δίπλα μου, κατά την διάρκεια των σπουδών μου και με στήριξε με κάθε τρόπο. Ακόμα, θα ήθελα να ευχαριστήσω την Ελένη που ήταν η συνοδοιπόρος μου και σε αυτό το ταξίδι.

Θα ήταν μεγάλη παράβλεψή μου, αν δεν ευχαριστούσα τον κύριο Φουληρά Παναγιώτη, ο οποίος με εμπιστεύτηκε, ώστε να αναλάβω αυτήν την εργασία και ήταν πάντα διατεθειμένος να μου λύσει όποια απορία προέκυπτε. Επίσης, ένα μεγαλό ευχαριστώ και στον κύριο Αποστολίδη-Αφεντούλη Βασίλειο για την βοήθεια που μου παρείχε.

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

1. Εισαγωγή

Στην σημερινή εποχή στους κύκλους της πληροφορικής και της τεχνολογίας ένα θέμα που έχει ήδη ξεκινήσει να έχει τρομερή απήχηση και να συζητιέται όλο και παραπάνω είναι το Διαδίκτυο των Πραγμάτων ή αλλιώς Internet of Things (IoT). Το Διαδίκτυο των Πραγμάτων έχει να κάνει με την διασύνδεση των διαφόρων αντικειμένων μεταξύ τους, που είναι εξοπλισμένα με λογισμικό, αισθητήρες και την προϋπόθεση πρόσβασης στο διαδίκτυο είτε άμεσα, είτε εκ των υστέρων. Αυτά τα αντικείμενα, που μπορεί να είναι οικιακές συσκευές, οχήματα, ακόμα και σπίτια παρέχουν την δυνατότητα στον χρήστη να τα ελέγξει απομακρυσμένα και στοχεύουν να κάνουν την καθημερινότητα του πιο εύκολη.

Επόμενο είναι να διεξάγονται συνεχώς έρευνες από ακαδημαϊκούς φορείς, βιομηχανίες, γύρω από αυτό το θέμα για να ανακαλυφθούν όλες οι δυνατότητες αυτής της έννοιας και να αφομοιωθούν από την ανθρωπότητα ώστε να αυξήσουν την ποιότητα ζωής. Ωστόσο, ένα σημαντικό ζήτημα που γεννιέται είναι η ασφάλεια των δεδομένων που διακινούνται ανάμεσα στις συσκευές και στους ανθρώπους και κατ' επέκταση στο διαδίκτυο. Όπως κάθε τεχνολογία υπόκειται σε κατάχρηση και εκμετάλλευση για την διεξαγωγή παράνομων δραστηριοτήτων έτσι και το Διαδίκτυο των Πραγμάτων δεν αποτελεί εξαίρεση. Ιδιαίτερα αφού η ταχύτητα εξάπλωσης του είναι μεγάλη με αποτέλεσμα σε κάποιες περιπτώσεις να μη δίδεται προσοχή στην ασφάλεια και να δημιουργούνται κενά που μπορούν να αποτελούν κίνδυνο με τις συσκευές μπορούν να δεχτούν επίθεση και τα αποτελέσματα να είναι δυσάρεστα για τους χρήστες. Από την στιγμή όμως που οι τεχνολογίες του IoT ήρθαν για να μείνουν θα είναι καλό να υπάρχει η δέουσα εμπιστοσύνη από τους χρήστες όταν τις χρησιμοποιούν.

Σε αυτό το σημείο εμπλέκεται η ασφάλεια και ειδικότερα ο κλάδος της ψηφιακής εγκληματολογίας (DigitalForensics) που ασχολείται και η συγκεκριμένη εργασία. Η ψηφιακή εγκληματολογία κατά τον McKemmish (Mckemmish, 1999) περιγράφεται ως "Η διαδικασία της ταυτοποίησης, διατήρησης, ανάλυσης και παρουσίασης ψηφιακών αποδείξεων με τρόπο που είναι νομικά αποδεκτός". Πρακτικά δηλαδή, τα πειστήρια που ανακάλυψε ο ερευνητής μετά από μία ψηφιακή επίθεση να μπορούν να παρουσιαστούν σε δικαστική αίθουσα και να είναι νομικά βάσιμα ώστε να χρησιμοποιηθούν αναλόγως.

1.1 Καθορισμός και Σπουδαιότητα του Προβλήματος

Μεγάλο μέρος της κοινωνίας έχει εξοικειωθεί ήδη με την τεχνολογία του Διαδικτύου των Πραγμάτων και αναμένεται οι χρήστες να φτάσουν σε μεγαλύτερο βαθμό. Για αυτό και η ασφάλεια πρέπει να λαμβάνεται σοβαρά υπόψη από τους κατασκευαστές και τους χρήστες. Κάποιες φορές

όσα μέτρα προστασίας και όσες προφυλάξεις έχουν ληφθεί, μπορεί να μην είναι αρκετά και ένας κακόβουλος χρήσης να καταφέρει να επιτύχει να ξεπεράσει την ασφάλεια και να επιδοθεί σε παράνομες ενέργειες που έχουν ως σκοπό να μας βλάψουν. Έτσι δημιουργήθηκε η ψηφιακή εγκληματολογία, που ανήκει στο κλάδο της ασφάλειας. Η ψηφιακή εγκληματολογία χρησιμοποιείται για να αναλύσει τα ίχνη και να αποκαλύψει τα γεγονότα που προηγήθηκαν μιας επίθεσης.

Όπως έχει ήδη αναφερθεί ανάμεσα στα αντικείμενα του Διαδικτύου των Πραγμάτων ανταλλάσσονται πολλά δεδομένα που είναι πλούσια σε πληροφορίες. Συνεπώς, κατανοούμε πως αυτές οι συσκευές αποτελούν πηγή άντλησης και διευκολύνουν τις διεργασίες της ψηφιακής εγκληματολογίας, μέσα από την ανάλυση των δεδομένων. Εντούτοις, η περιορισμένη μνήμη τους αποτελεί πρόβλημα και οι πιθανότητες τα δεδομένα αυτά να διαγραφούν ή να χαθούν είναι πολύ μεγάλες (Lillis, Becker, O'Sullivan, & Scanlon, 2016)

Η πρόκληση είναι να εφαρμοστούν οι αρχές της Ψηφιακής Εγκληματολογίας (οι οποίες θα αναλυθούν σε παρακάτω κεφάλαιο) στο IoT που πιθανότατα θα εμπλέκονται smartphone, αισθητήρες και πλειάδα άλλων πληροφοριών που απαιτούν ανάλυση για να κρατηθούν μόνο αυτές που χρειάζονται.

1.2 Διάρθρωση της Διπλωματικής

Η παρούσα εργασία έχει την παρακάτω δομή:

Πρώτα, γίνεται μια αναφορά στο Διαδίκτυο των Πραγμάτων, τα χαρακτηριστικά που εξυπηρετεί ήδη και πού αναμένεται να βοηθήσει. Ποιες τεχνολογίες το διέπουν, πού βρίσκει εφαρμογή και ποία προβλήματα ασφαλείας αντιμετωπίζει.

Ακολούθως, θα αναλυθεί η Ψηφιακή Εγκληματολογία και θα παρουσιαστεί η μέχρι τώρα αντίστοιχη βιβλιογραφία που αφορά τα μοντέλα διαδικασιών που υπάρχουν και βάση με αυτά πραγματοποιούνται οι έρευνες. Στη συνέχεια θα εστιάσουμε στα ψηφιακά πειστήρια και στον τρόπο με τον οποίο θα ήταν καλό να τα χειριστεί κάποιος ώστε να αντλήσει όλες τις πληροφορίες και τα δεδομένα που θα χρειαστεί για να φτάσει στον επιθυμητό στόχο. Αναφέρονται επίσης οι προκλήσεις που μπορεί να συναντήσει ένας ερευνητής κατά την έρευνά του και χρήσιμα εργαλεία τα οποία χρησιμοποιούν οι επιστήμονες της Ψηφιακής Εγκληματολογίας ώστε να συνδράμουν στο έργο τους.

Αμέσως μετά θα προχωρήσουμε στο Διαδίκτυο των Πραγμάτων και θα αναλύσουμε την αρχιτεκτονική τους, τα χαρακτηριστικά τους, τα προβλήματα ασφαλείας που ενδεχομένως αντιμετωπίζουν, τις εφαρμογές τους και ποια οφέλη μπορούν να έχουν.

Ακολούθως, το πέμπτο κεφάλαιο πραγματεύεται την χρήση που βρίσκει η επιστήμη του IoT στην Ψηφιακής Εγκληματολογία και τις καινούργιες προκλήσεις που συστήνει το Διαδίκτυο των Πραγμάτων. Ακόμα, περιγράφονται οι διαφορές της Ψηφιακή Εγκληματολογίας και της Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων

Στο επόμενο κεφάλαιο θα διερευνηθεί ο προσομοιωτής CupCarbon και οι δυνατότητες του, θα δημιουργηθούν σενάρια επίθεσης με σκοπό την συλλογή ψηφιακών στοιχείων από αντικείμενα του Διαδικτύου των Πραγμάτων με χρήσητων μοντέλων διαδικασιών για να δούμε με ποίο τρόπο θα συγκεντρωθούν τα πειστήρια και πως θα χρησιμοποιηθούν.

Στο τελευταίο κεφάλαιο θα παρουσιαστούν τα αποτελέσματα αυτής της διπλωματικής εργασίας σχετικά με την εφαρμογή της Ψηφιακής Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων, αλλά θα γίνουν και προτάσεις για μελλοντική επέκταση.

1.3 Στόχοι της Διπλωματικής

Οι στόχοι της διπλωματικής είναι να κατανοήσουμε την τεχνολογία του IoT και στην συνέχεια την έννοια της ψηφιακής εγκληματολογίας. Επιπλέον, τον τρόπο με τον οποίο αυτές οι δύο τεχνολογίες μπορούν να συνδυαστούν και πώς όταν εμπλέκονται συσκευές συνδεμένες στο IoT αποτελούν πηγή άντλησης των χρήσιμων πληροφοριών για την ανακατασκευή του συμβάντος για την καλύτερη ανάλυσή του. Επίσης, μετά από την ανάλυση των προτεινόμενων από την βιβλιογραφία μοντέλων ο αναγνώστης θα έχει μια ολοκληρωμένη άποψη γύρω από αυτά.

Ακόμα, θα επιχειρηθεί μέσα από τιςδιάφορες προσομοιώσεις με το CupCarbon να δούμε τον τρόπο συλλογής των πειστηρίων από τα αντικείμενα του IoT και πώς αυτά θα μπορούσαν να χρησιμοποιηθούν σε μια δικαστική αίθουσα.

1.4 Συνεισφορά

Η συνεισφορά της διπλωματικής ορίζεται ως εξής:

1. Αναλύσαμε την επιστήμη της Ψηφιακής Εγκληματολογίας
2. Μελετήσαμε την τεχνολογία του IoT
3. Προβάλλαμε τα μοντέλα που υπάρχουν στην βιβλιογραφία γύρω από την Εγκληματολογία στο Διαδίκτυο των Πραγμάτων
4. Παρουσιάσαμε πως συνδυάζεται η τεχνολογία του IoT με την Ψηφιακή Εγκληματολογία και πως αυτό ωφελεί σε μια έρευνα τους ειδικούς
5. Εξετάσαμε το μοντέλα Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων που υπάρχουν στην βιβλιογραφία

6. Υλοποιήσαμε τρεις προσομοιώσεις, από τις οποίες είδαμε, τα μοντέλα εγκληματολογίας στην πράξη, τον τρόπο συλλογής των πειστηρίων από τις συσκευές του IoT, πώς αυτά επικουρούν στην εξαγωγή συμπερασμάτων και τη χρήση του CupCarbon σε προσομοιώσεις που αφορούν εγκληματολογικούς σκοπούς

2. Γενικές Έννοιες Ασφάλειας

2.1 Ασφάλεια Υπολογιστών

Το σημαντικότερο κομμάτι της καλής λειτουργίας ενός υπολογιστή, μίας έξυπνης συσκευής, και των δικτύων υπολογιστών είναι η ασφάλεια. Το Διαδίκτυο κρύβει κινδύνους τόσο για τους απλούς χρήστες όσο και για τους πιο έμπειρους, αλλά και για οργανισμούς/επιχειρήσεις. Μολονότι υπάρχουν δισεκατομμύρια κάτοχοι υπολογιστών και πλέον έξυπνων συσκευών, λίγοι είναι αυτοί που γνωρίζουν αυτούς τους κινδύνους. Η ασφάλεια, λοιπόν, αναλαμβάνει αυτή την εργασία της προστασίας του υπολογιστή από τα διάφορα κακόβουλα προγράμματα και τους κακόβουλους χρήστες. Για αυτό αποτελεί μια αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με άλλες βασικές λειτουργίες όπως η ποιότητα και η απόδοση των υπηρεσιών, για την σωστή και ολοκληρωμένη λειτουργία μιας επιχείρησης ή ακόμα και της απλής χρήσης του προσωπικού υπολογιστή, του έξυπνου κινητού και του Διαδικτύου από έναν χρήστη.

Η έννοια της ασφάλειας σχετίζεται με την προστασία των πληροφοριών που έχουμε στην κατοχή μας από περιπτώσεις αλλοιώσεων και καταστροφών, καθώς και από παράνομη χρήσης τους. Άρα, η ασφάλεια στηρίζεται στην λήψη μέτρων όπου διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των πληροφοριών και των δεδομένων,όπως και η συνεχής λειτουργία του δικτύου και του υπολογιστή μας.

Ποιο συγκεκριμένα λοιπόν, η ασφάλεια συνδέεται με:

- Πρόληψη (Prevention):Την λήψη μέτρων για να προληφθούν καταστροφές και φθορές σε δεδομένα ακόμα και στους υπολογιστές.
- Ανίχνευση (Detection):Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε καταστροφή και φθορά.
- Αντίδραση (Reaction):Την λήψη μέτρων για την αποκατάσταση ή ανάκτηση των δεδομένων και των πληροφοριών που πιθανώς έχουν επηρεαστεί.

Η προστασία ενός δικτύου υπολογιστών ή ενός δικτύου αισθητήρων και των προσωπικών μας υπολογιστών που συνδέονται με το Διαδίκτυο είναι ένα θέμα που πρέπει να αντιμετωπίσουν οι

χρήστες και οι οργανισμοί. Έχουν ωστόσο κατοχυρωθεί στις μέρες μας οι έννοιες Διαθεσιμότητα, Εμπιστευτικότητα και Ακεραιότητα οι οποίες σχετίζονται πολύ στενά με την έννοια της ασφάλειας.

Διαθεσιμότητα είναι η διασφάλιση ότι όλες οι πληροφορίες, δεδομένα, και προγράμματα θα είναι προσβάσιμα στους χρήστες ενός δικτύου. Έτσι, όλες οι υπηρεσίες θα είναι λειτουργικές χωρίς να έχει σημασία εάν υπάρχει κάποια τυχαία διακοπή ρεύματος, ατυχήματα, κτλ. Αυτό βέβαια σημαίνει ότι οι χρήστες δε θα αντιμετωπίζουν την άρνηση εξυπηρέτησης (Denial of Service) όταν θέλουν να χρησιμοποιήσουν το δίκτυο.

Οι επιθέσεις άρνησης εξυπηρέτησης είναι οι επιθέσεις εναντίον ενός υπολογιστή ή δικτύου οι οποίες αποσκοπούν να καταστήσουν τον υπολογιστή ή το δίκτυο ανίκανο να δεχτεί άλλες συνδέσεις με αποτέλεσμα να μην μπορεί να εξυπηρετήσει άλλους πελάτες. Επίσης, δεν επιτρέπει κάποιον νόμιμο χρήστη να προσπελάσει και να εκμεταλλευτεί δεδομένα και πληροφορίες.

Η **Εμπιστευτικότητα** ασχολείται με την πρόληψη της μη εξουσιοδοτημένης πρόσβασης στα δεδομένα και στις πληροφορίες. Οι επιθέσεις θεωρούνται παθητικές, αφού ο εισβολέας δεν τροποποιεί το σύστημα, αλλά απλά «κλέβει» τα αντίγραφα των πληροφοριών που διέρχονται και μεταδίδονται μέσω του δικτύου ή που είναι αποθηκευμένα στον υπολογιστή.

Η **Ακεραιότητα** αποτελεί την διαβεβαίωση ότι τα δεδομένα και οι πληροφορίες που έχουν ληφθεί, αποθηκευτεί και σταλεί δεν έχουν υποστεί κάποια μετατροπή από κάποιο τρίτο, μη εξουσιοδοτημένο πρόσωπο. Αυτό σημαίνει ότι μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να αλλάξουν οτιδήποτε και κανένας άλλος.

2.2 Αναγκαιότητα της Ασφάλειας

Τα τελευταία χρόνια λόγω της άνθησης και της εξάπλωσης των διαφόρων τεχνολογιών, του Internet of Things, των ηλεκτρονικών συσκευών και των υπηρεσιών του Διαδικτύου, αναπτύσσονται παράλληλα και πολυάριθμοι κίνδυνοι. Η χρήση ασφάλειας κρίνεται απαραίτητη, τόσο σε προσωπικό επίπεδο, όσο και σε επίπεδο επιχειρήσεων/οργανισμών γιατί έτσι προστατεύονται οι πληροφορίες, τα προσωπικά δεδομένα, τα οικονομικά μιας επιχείρησης και τα σχέδια της. Ωστόσο, είναι επόμενο με την υιοθέτηση διαφόρων μέτρων ασφάλειας να δημιουργούνται κάποια άλλα προβλήματα στη λειτουργία των δικτύων, των έξυπνων συσκευών και των υπολογιστών, όπως το να επιβαρύνεται η απόδοση, το κόστος εγκατάστασης και λειτουργίας ενός δικτύου ή μιας συσκευής.

Η τεχνολογία, ο ανταγωνισμός και οι διάφοροι εισβολείς με συνεχώς βελτιωμένους τρόπους επιθέσεων καθιστούν πολύ σημαντικούς τους συχνούς ελέγχους του συστήματος. Αν, λοιπόν, ακολουθείται αυτή η πολιτική στις επιχειρήσεις (και όχι μόνο), μειώνονται οι κίνδυνοι αφού το σύστημα ασφαλείας διορθώνεται, βελτιώνεται και εμφανίζεται πιο έτοιμο σε κάθε πιθανή επίθεση από τον οπουδήποτε.

Βέβαια, οι περιπτώσεις όπου τελικά η ασφάλεια δεν κατάφερε να αποτρέψει κάποια επίθεση ή κάποιο άλλο γεγονός που είχε ως στόχο να βλάψει είναι πολλές. Η διερεύνηση μιας επίθεσης και η ανάλυση των δεδομένων είναι διαδικασίες που σχετίζονται με την Ψηφιακή Εγκληματολογία που θα εξεταστεί παρακάτω και είναι ένας κλάδος που είναι στενά συνδεδεμένος με την Ασφάλεια.

3. Ψηφιακή Εγκληματολογία (Digital Forensics)

3.1 Η επιστήμη των Forensics

Η επιστήμη των Forensics(που στην ελληνική βιβλιογραφία αναφέρεται ως εγκληματολογία) χρησιμοποιείται από το ποινικό σύστημα και είναι η εφαρμογή της επιστήμης στους νόμους. Ο σκοπός της είναι τελικά να χρησιμοποιηθεί στον χώρο του δικαστηρίου. Οι ειδικοί που ασχολούνται με τον κλάδο των Forensics ποικίλουν, αφού μπορούν να προέρχονται από τους κλάδους της ιατρικής, της πληροφορικής και της βιολογίας, και να συνδράμουν στο δικαστικό σύστημα με τις γνώσεις τους προσφέροντας επιστημονικά αποδεδειγμένες πληροφορίες. Οι ερευνητές χρησιμοποιούν τις εξειδικευμένες γνώσεις τους και τα κατάλληλα εργαλεία για την συλλογή, ανάλυση και παρουσίαση των αποδεικτικών στοιχείων προκειμένου να διαλευκάνουν ένα έγκλημα. Τα παραπάνω στάδια είναι τα τρία βασικά βήματα που ακολουθούνται στον τομέα των Forensic κατά την διάρκεια της έρευνας.

Κάποιοι από τους τομείς που ανήκουν στην επιστήμη των Forensics θεωρούνται η Δικανική Ανθρωπολογία, η Δικανική Οδοντιατρική, η Τοξικολογία, η Γενετική, η Βαλλιστική και βεβαίως η Ψηφιακή Εγκληματολογία, την οποία και πραγματεύεται αυτή η εργασία.

3.2 Πώς ορίζεται η ψηφιακή εγκληματολογία

Όπως και στα εγκλήματα που διαπράττονται στον φυσικό κόσμο, τις περισσότερες φορές οι δράστες μετά το πέρασμά τους αφήνουν, είτε γενετικό υλικό, είτε διάφορα άλλα ίχνη και στοιχεία, που είναι ικανά να οδηγήσουν τους ερευνητές στην λύση του εγκλήματος. Έτσι και στα ψηφιακά εγκλήματα οι διαφορές δεν είναι μεγάλες εκτός του ότι τα ίχνη είναι ηλεκτρονικά. Σε αυτό το σημείο ξεκινάει ο ρόλος της Ψηφιακής Εγκληματολογίας (Digital Forensics) που ασχολείται - εκτός των άλλων - και με την ανάκτηση χαμένων πληροφοριών, ανάλυση ψηφιακών αποδείξεων - ακόμα και αναπαράσταση του ψηφιακού εγκλήματος.

Ως Ψηφιακή Εγκληματολογία ορίζεται η χρήση επιστημονικά προερχόμενων και αποδεδειγμένων μεθόδων για την διατήρηση, συλλογή, επικύρωση, αναγνώριση, ανάλυση, ερμηνεία, καταγραφή και παρουσίαση των ψηφιακών αποδείξεων που προέρχονται από ψηφιακές πηγές και έχουν ως σκοπό την διευκόλυνση, ανακατασκευή και αναπαράσταση εγκληματικών ενεργειών ή συμβάλλουν στην πρόληψη μη εξουσιοδοτημένων ενεργειών που δείχνουν να αποτελούν κίνδυνο για σχεδιαζόμενες λειτουργίες (Palmer, 2001). Ο όρος αυτός χρησιμοποιήθηκε στο πρώτο Digital Forensic Research Workshop (DRFWS) που διεξήχθη το 2001 στην Νέα Υόρκη θέλοντας να καλύψει όλα τα ψηφιακά μέσα που έχουν την δυνατότητα να αποθηκεύσουν δεδομένα. Κάποια που εκείνη την εποχή είχαν αυτήν την ικανότητα ήταν τα κινητά τηλέφωνα, τα δίκτυα και

οι ασύρματες συσκευές. Σήμερα έχουμε wearables, έξυπνα κινητά, έξυπνα ρολόγια, έξυπνα σπίτια, έξυπνα αυτοκίνητα. Βεβαίως, όλα αυτά ανήκουν στο Διαδίκτυο των Πραγμάτων (Internet of Things), για το οποίο θα αναφερθούμε παρακάτω.

Με την κατακόρυφη εξέλιξη της τεχνολογίας και την όλο αυξανόμενη χρήση υπολογιστών, ψηφιακών συσκευών και δικτύων, η Ψηφιακή Εγκληματολογία έχει αναδειχθεί ως σημαντική επιστήμη για την ανάκτηση χρήσιμων ψηφιακών δεδομένων που θα οδηγήσουν τελικά στον εντοπισμό κακόβουλων ενεργειών. Για την διασφάλιση ότι τα αποτελέσματα είναι αποδεκτά στο δικαστήριο, οι επιστήμες αυτού του είδους είναι υποχρεωμένες να ακολουθούν τις βασικές αρχές της τεχνολογίας μαζί με επικυρωμένες και παγιωμένες διαδικασίες.

3.3 Η Ιστορία της Ψηφιακής Εγκληματολογίας

Το 1984 το FBI δημιούργησε την πρώτη ομάδα που ασχολείτο με τα ψηφιακά πειστήρια. Η ομάδα αυτή ονομαζόταν Computer Analysis and Response Team (CART). Τα λειτουργικά συστήματα εκείνη την περίοδο ήταν αρκετά, αλλά η διαδικασία της ψηφιακής εγκληματολογίας δεν ήταν τόσο απαιτητική. Ένα από τα εργαλεία εκείνης της περιόδου ήταν το NortonDiskEdit (Zareen, Waqar, & Aslam, 2013). Το 1990 ήταν η αρχή των λειτουργικών συστημάτων με γραφικό περιβάλλον (GUI) και ακολούθησαν, ως προς την υιοθέτηση του γραφικού περιβάλλοντος, και τα εργαλεία της ψηφιακής εγκληματολογίας, όπως το Encase (το οποίο θα δούμε παρακάτω). Στην δεκαετία του 2000-2010 το λειτουργικό σύστημα των Windows γνώρισε τεράστια άνθηση και κατάφερε να γίνει το κύριο λειτουργικό σύστημα, τόσο σε προσωπικούς υπολογιστές, όσο και σε εταιρικούς. Λόγω αυτής της εξέλιξης η ψηφιακή εγκληματολογία έγινε σχετικά ευκολότερη σαν διαδικασία, διότι οι περισσότεροι υπολογιστές χρησιμοποιούσαν κοινό λειτουργικό σύστημα.

Σύμφωνα με τον M.Pollit (Pollitt, 2010),ο οποίος έχει καταγράψει την εξέλιξη της ψηφιακής εγκληματολογίας ξεκινώντας από την προϊστορική εποχή που είναι πριν το 1985, δεν υπήρχε ακόμα ο όρος ψηφιακή εγκληματολογία και οι υπολογιστές δεν χρησιμοποιούνταν παρά μόνο σε μεγάλες επιχειρήσεις. Άρα δεν είναι παράξενο που δεν υπάρχουν και πολλές αναφορές για εκείνη την περίοδο. Ακολούθησε η βρεφική περίοδος η οποία είναι ανάμεσα στο 1985-1995 που άρχισαν δειλά-δειλά οι υπολογιστές να μπαίνουν και στα σπίτια των ανθρώπων εκτός των επιχειρήσεων και να αντιλαμβάνονται οι χρήστες πως οι υπολογιστές θα παίξουν μεγάλο ρόλο στο μέλλον αφού κανείς θα μπορεί να συγκεντρώσει πολλές πληροφορίες. Η παιδική περίοδος από το 1995 έως το 2005 σηματοδότησε μια έκρηξη στην επιστήμη. Οι λόγοι ήταν πολλοί. Ωστόσο, η έκρηξη της τεχνολογίας, οι παράνομες δραστηριότητες, η διακίνηση ύποπτου υλικού μέσω των υπολογιστών και των δικτύων, ακόμα και τα γεγονότα της 11ης Σεπτεμβρίου 2001, ήταν οι σημαντικότεροι. Από το 2005 έως σήμερα η ψηφιακή εγκληματολογία διανύει την εφηβική περίοδο που έχει γνωρίσει

και την πιο μεγάλη απήχηση σε ότι αφορά τους επαγγελματίες που ασχολούνται με την επιστήμη. Οι πηγές όπου μπορεί κανείς να αποσπάσει στοιχεία αυξάνονται και προσφέρουν παραπάνω όγκο δεδομένων στον κάθε ερευνητή.

3.4 Ψηφιακή Πειστήρια (Digital Evidence)

Τα ψηφιακά πειστήρια ή ψηφιακά αποδεικτικά στοιχεία παίζουν τον πιο σημαντικό ρόλο στην διαμόρφωση αποτελέσματος για μια έρευνα. Οι Carrier και Spafford (Carrier&Spafford, Anevent-baseddigitalforensicinvestigationframework, 2004) όρισαν τα ψηφιακά αποδεικτικά στοιχεία σαν τις πληροφορίες που μπορούν να στηρίξουν ή να διαψεύσουν μια υπόθεση για ψηφιακά γεγονότα ή την κατάσταση των ψηφιακών πληροφοριών.

Τέτοιου είδους πειστήρια μπορούν να συλλεχθούν από περιπτώσεις όπου εμπλέκονται ψηφιακές συσκευές που παρέχουν τα αντίστοιχα δεδομένα. Ο Perumal (Perumal S. , 2009) υποστήριξε πως τα ψηφιακά πειστήρια είναι οποιαδήποτε πληροφορία που παρέχει διασύνδεση ανάμεσα στον λόγο του εγκλήματος και το θύμα. Τα στοιχεία αυτά παρέχουν μια ψηφιακή διάσταση σε μια έρευνα και ο ερευνητής (συλλέγοντάς τα) μπορεί να δημιουργήσει το προφίλ ενός ατόμου σε αρκετά μεγάλο βαθμό.

Τα ψηφιακά αποδεικτικά στοιχεία είναι ιδιαίτερα ευπαθή και μπορούν να μορφοποιηθούν ή ακόμα και να καταστραφούν από απρόσεκτο χειρισμό. Για αυτό και πρέπει να λαμβάνονται μέτρα ασφαλείας για να διατηρούν την αρχική τους κατάσταση.

Οι τύποι πειστηρίων που ενδέχεται να εμφανιστούν ποικίλουν. Οι υπολογιστές, τα κινητά, οι έξυπνες συσκευές βρίσκονται πλέον παντού σε κάθε πτυχή σχεδόν της καθημερινότητάς μας. Ο Henseler (Henseler, 2000)κατηγοριοποίησε τα υπολογιστικά συστήματα που περιέχουν τέτοιου είδους δεδομένα, ως εξής:

- **Ανοιχτά υπολογιστικά συστήματα (Open computer systems)**: Είναι οι κοινοί υπολογιστές που πλέον χρησιμοποιούν πάρα πολλοί άνθρωποι λόγω της δουλειάς τους ή για την διασκέδασή τους. Όσο περνούν τα χρόνια και η τεχνολογία εξελίσσεται ο χώρος αποθήκευσης των σκληρών δίσκων φτάνει όλο και σε μεγαλύτερα νούμερα και αυτό συνεπάγεται ακόμα παραπάνω πληροφορία που μπορεί να χρησιμοποιηθεί ως ψηφιακό πειστήριο.
- **Συστήματα Επικοινωνίας (Communication Systems)**: Τηλεφωνικά συστήματα όπως τα γνωρίζουμε, ασύρματα δίκτυα επικοινωνίας, το Διαδίκτυο, είναι όλα συστήματα που έχουν την δυνατότητα της παροχής στοιχείων που θα φανούν χρήσιμα στον ερευνητή. Ποιος ήταν ο αποστολέας, ποιος ήταν ο παραλήπτης, ο χρόνος που στάλθηκε ένα μήνυμα μέσω κινητού

ή μέσω ηλεκτρονικού ταχυδρομείου, είναι μερικές από τις πληροφορίες που θα μπορούσε να εκμεταλλευτεί ο ερευνητής.

- **Ενσωματωμένα Υπολογιστικά Συστήματα (Embedded Computer Systems)**: Κινητά τηλέφωνα, έξυπνες κάρτες, συσκευές με δυνατότητα στιγματοθέτησης (GPS) και ό,τι γενικότερα περιέχει υπολογιστικό σύστημα και μπορεί να προσφέρει πληροφορίες. Πλέον έχουμε τα έξυπνα κινητά τηλέφωνα, wearables, έξυπνα αυτοκίνητα, έξυπνες κάρτες, συστήματα "νέφους" (clouds) που όλα αυτά αποτελούν το Διαδίκτυο των Πραγμάτων και μπορούν να επικοινωνούν μεταξύ τους.

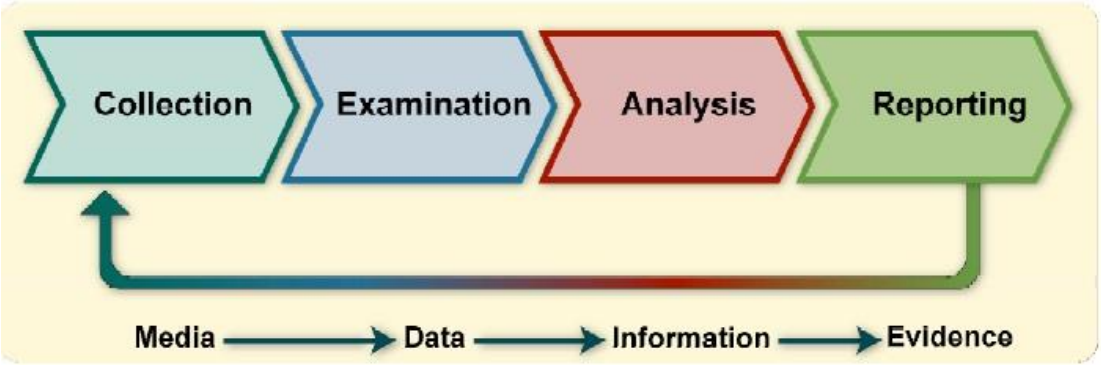
3.5 Μεθοδολογία Ψηφιακής Εγκληματολογίας

3.5.1 Μοντέλο του National Institute of Standards and Technology

Οι μεθοδολογίες που χρησιμοποιούνται από τους ερευνητές της Ψηφιακής Εγκληματολογίας ποικίλουν. Τα μοντέλα που έχουν προταθεί κατά καιρούς στην βιβλιογραφία είναι διάφορα, διότι όλες οι περιπτώσεις δεν είναι ίδιες και ο ερευνητής οφείλει να προσαρμόσει την έρευνά του ανάλογα. Ωστόσο, αν κάποιος τα μελετήσει προσεκτικά, θα παρατηρήσει πως όλα ακολουθούν τα ίδια περίπου βήματα και διαδικασίες με κάποιες, είτε μικρές, είτε μεγάλες παραλλαγές.

Τα πιο συνήθη βήματα σύμφωνα με το National Institute of Standards and Technology (NIST) που εφαρμόζονται σε κάθε έρευνα εγκληματικής ενέργειας είναι τα εξής:

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



Εικόνα 1: Μοντέλο NIST

I. Συλλογή Δεδομένων (Data Collection): Οι πρώτες κινήσεις που γίνονται από τον ερευνητή που ακολουθεί το μοντέλο του ινστιτούτου NIST είναι να αναγνωρίσει τις πηγές από τις οποίες μπορεί να αποκτήσει πληροφορίες και δεδομένα. Οι πηγές αυτές μπορεί να είναι εκατοντάδες. Οι πιο κοινές που ο καθένας μπορεί να φανταστεί είναι επιτραπέζιοι υπολογιστές, φορητοί υπολογιστές, εξυπηρετητές, δίκτυα. Μέσω αυτών των ψηφιακών συσκευών και δεδομένων ο ερευνητής θα φτάσει στο σκληρό δίσκο του συστήματος και σε θύρες USB που μπορεί να τις χρησιμοποιήσει για να εξάγει τις πληροφορίες που χρειάζεται να συλλέξει. Επίσης, οι οπτικοί δίσκοι, τα USB sticks, οι κάρτες μνήμης θεωρούνται μέσα εξωτερικής αποθήκευσης που περιέχουν σημαντικά δεδομένα. Εκτός από αυτά, δεδομένα υπάρχουν ακόμα και σε κινητά τηλέφωνα, mp3 players, iPods, ψηφιακές κάμερες και πλέον και στα έξυπνα ψυγεία, στα αυτοκίνητα τελευταίας τεχνολογίας, και γενικότερα σε συσκευές που αποτελούν το Διαδίκτυο των Πραγμάτων. Ο ερευνητής κατά την διάρκεια της έρευνάς του οφείλει μέσα από την εμπειρία του να ξεχωρίσει οποιαδήποτε συσκευή μπορεί να του προσφέρει πληροφορία.

Δεν πρέπει να παραβλέπεται πως χρήσιμα δεδομένα μπορούν να αποθηκευθούν ακόμα και στην μνήμη RAM του υπολογιστή ή στο δίκτυο, που σημαίνει πως στην επόμενη επανεκκίνηση ή στο κλείσιμο υπολογιστή αυτά θα χαθούν, άρα χρήζουν ιδιαίτερης προσοχής.

Κάποια άλλα σημεία που θα πρέπει να έχει στο νου ο ερευνητής είναι και σημεία που βρίσκονται εκτός του οργανισμού που ερευνάει. Τέτοια, σημεία μπορεί να είναι ο πάροχος Διαδικτύου που χρησιμοποιεί ο οργανισμός και από εκεί μπορεί να αποκτήσει τα logs, ούτως ώστε να μελετήσει την δραστηριότητα στο Διαδίκτυο. Για να αποκτήσει, ωστόσο κάποιος τα logs θα πρέπει προηγηθεί δικαστική εντολή. Δεν είναι δυνατόν πάντα να συλλεχθούν πληροφορίες από τα μέσα που επιθυμεί ο ερευνητής για πρακτικούς λόγους. Για αυτό και πρέπει να είναι ικανός να βρει άλλους τρόπους να αποκτήσει τα δεδομένα που χρειάζεται.

Από την στιγμή που η πρόληψη είναι η καλύτερη θεραπεία, οι εταιρείες και οι ειδικοί που δουλεύουν σε αυτές μπορούν να λάβουν κάποια μέτρα πρόληψης για να συλλέγουν χρήσιμα δεδομένα που θα χρειαστούν σε μια ψηφιακή εγκληματολογική έρευνα και θα διευκολύνουν τον ερευνητή σε περίπτωση που χρειαστεί. Τα πιο γνωστά λειτουργικά συστήματα, έχουν την δυνατότητα να ρυθμιστούν για να καταγράφουν τις αλλαγές που μπορεί να προκύψουν στις ρυθμίσεις ασφαλείας του συστήματος. Αυτά τα logs μπορούν να αποδειχτούν ιδιαίτερα σημαντικά στο μέλλον για έναν οργανισμό. Όλα αυτά τα μέτρα βέβαια, θα πρέπει να σχεδιαστούν έχοντας ως βάση τον σεβασμό στην ιδιωτικότητα του εργαζόμενου ή γενικότερα του χρήστη.

Αφού ο ερευνητής εντοπίσει τις πιθανές πηγές, επόμενο βήμα είναι να αποκτήσει τα δεδομένα που χρειάζεται ώστε να τα μελετήσει. Το NIST διαχωρίζει αυτήν την διεργασία σε τρεις μικρότερες διεργασίες, τις οποίες θα δούμε παρακάτω:

- **Σχεδιασμός:** Ο Σχεδιασμός σύμφωνα με τις πιθανές πηγές είναι ένα σημαντικό βήμα, διότι ο ερευνητής σε αυτό το σημείο βασισμένος στα ψηφιακά μέσα που έχει εντοπίσει θα τα κατηγοριοποιήσει και θα τα διαχωρίσει. Οι παράγοντες που θα λάβει υπόψη του για να θέσει τις προτεραιότητες έχουν να κάνουν με την πιθανή αξία μιας πηγής και για το πόσο χρήσιμα θα είναι τα δεδομένα που μπορεί να προσφέρει. Ο ερευνητής σύμφωνα με την εμπειρία του και την φύση του συμβάντος θα μπορέσει να υπολογίσει πόσο σημαντική είναι η κάθε πηγή. Ακολουθεί, η ρευστότητα των δεδομένων. Στην ρευστότητα έχουμε αναφερθεί ήδη μιλώντας για την μνήμη RAM, η οποία μπορεί να έχει αποθηκευμένα δεδομένα τα οποία όμως μετά από τον τερματισμό του υπολογιστή θα χαθούν. Άρα καλό θα ήταν η συλλογή των δεδομένων αυτών να βρίσκεται πολύ ψηλά στην λίστα του ερευνητή και να προτιμώνται από τα υπόλοιπα δεδομένα. Ο τρίτος παράγοντας είναι η προσπάθεια που απαιτείται για την συλλογή αφού οι πηγές θα είναι πολλές και πιθανόν να πρέπει να εμπλακούν και άλλοι ειδικοί. Επίσης, η προσπάθεια που χρειάζεται για να αποκτήσει κάποιος πρόσβαση σε στοιχεία που μόνο ο πάροχος Διαδικτύου κατέχει, θα είναι σίγουρα πολύ μεγάλη και χρονοβόρα.
- **Ανάκτηση Δεδομένων:** Η ανάκτηση των δεδομένων προτείνεται να γίνει με εργαλεία της ψηφιακής εγκληματολογίας και να διατηρούνται στην αρχική μορφή τους. Η διαδικασία μπορεί να γίνει είτε τοπικά, είτε μέσω του δικτύου. Ο καλύτερος τρόπος ανάμεσα στους δύο είναι ο τοπικός επειδή οι πληροφορίες και το σύστημα ελέγχονται καλύτερα.
- **Επαλήθευση των Δεδομένων:** Μετά την ανάκτηση των δεδομένων, κρίνεται απαραίτητο να επαληθευτεί η ακεραιότητά τους. Αυτό γίνεται για νομικούς λόγους και έτσι ο ερευνητής επιβεβαιώνει πως δεν έχει τροποποιήσει ότι έχει συλλέξει. Και σε αυτό το βήμα η επαλήθευση θα γίνει με εργαλεία της ψηφιακής εγκληματολογίας, όπου μέσω της συνάρτησης κατακερματισμού θα συγκριθούν τα αρχικά στοιχεία με αυτά που απέκτησε ο ερευνητής κατά την διάρκεια της έρευνας.

II. Εξέταση (Examination): Μετά την φάση της συλλογής των δεδομένων περνάμε στην δεύτερη φάση που είναι η εξέταση. Από αυτήν την διαδικασία περιμένει κάποιος να αξιολογηθούν τα στοιχεία και να εξαχθούν πληροφορίες για αυτά. Ο όγκος των δεδομένων συνήθως είναι τεράστιος και θεωρείται δύσκολο να βρεθούν αποτελέσματα χειροκίνητα. Τα εργαλεία της ψηφιακής εγκληματολογίας προσφέρουν λύση και σε αυτό το κομμάτι σύμφωνα με τους Zareen et al.(Zareen, Waqar, & Aslam, 2013) ως εξής:

- Μέσω αναζήτησης με λέξεις κλειδιά που μπορούν να βρουν κείμενο ή κάποιο μοτίβο

- Με διαχωρισμό/φιλτράρισμα σε δεδομένα που βασίζονται σε διαφορετικούς τύπους δεδομένων όπως π.χ., κείμενο, ήχος, βίντεο, γραφικά, κτλ.

III. Ανάλυση (Analysis): Ύστερα και από την εξέταση είναι σειρά της ανάλυσης όπου ο ερευνητής θα προσπαθήσει να εξαγάγει κάποια συμπεράσματα σύμφωνα με τις πληροφορίες που εξέτασε στην προηγούμενη φάση. Είναι καίριο να γνωρίζει πότε ένα γεγονός έχει συμβεί ή πότε ένας φάκελος δημιουργήθηκε ή τροποποιήθηκε. Έτσι θα μπορέσει να αναπαραστήσει από την αρχή κάποια γεγονότα με στόχο την ακόμα καλύτερη ανάλυση των γεγονότων.

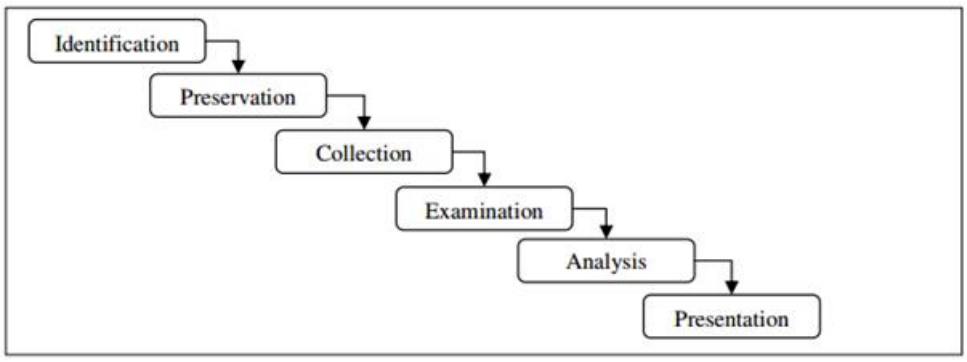
IV. Αναφορά (Reporting): Η τελευταία φάση αποτελείται από την αναφορά των αποτελεσμάτων. Η αναφορά εμπεριέχει πληροφορίες για τα δεδομένα που έχει αποκτήσει ο ερευνητής συνοδευόμενα από την ημερομηνία, την ώρα, το μέρος που τα σύλλεξε, με ποια μέθοδο και εργαλεία έχει χρησιμοποιήσει. Τις περισσότερες φορές η αναφορά γίνεται γραπτά και όταν ο ερευνητής κληθεί από το δικαστήριο προφορικά. Σε περίπτωση που ένα γεγονός έχει παραπάνω από μία εξηγήσεις ο ερευνητής οφείλει να τις αναφέρει όλες και πάντα θα πρέπει να είναι ακριβής και λεπτομερής στην αναφορά των ευρημάτων του (Kent, Chevalier, Grance, & Dang, 2006).

3.5.2 Επιπρόσθετα μοντέλα Ψηφιακής Εγκληματολογίας

Εκτός από το μοντέλο του ινστιτούτου NIST, στην βιβλιογραφία όπως προαναφέρθηκε συναντάμε πολλά μοντέλα, έτσι αξίζει να αναφερθούν κάποια από αυτά.

- DFRWS Investigative Model

Το συγκεκριμένο μοντέλο χρησιμοποιείται συχνά από τους ερευνητές και είναι απόρροια του πρώτου συνεδρίου του DFRWS. Αποτελείται από τα εξής βήματα: Ταυτοποίηση (Identification), Διαφύλαξη (Preservation), Συλλογή (Collection), Εξέταση (Examination), Ανάλυση (Analysis) και Παρουσίαση (Presentation).



Εικόνα 2: Μοντέλο DRFWS

Στην πρώτη φάση διακρίνουμε την ταυτοποίηση (identification) την εντόπιση του γεγονότος, την αναγνώριση κάποιας ανωμαλίας στο σύστημα, την ανάλυση ελέγχου και την παρακολούθηση του συστήματος. Ακολουθεί, η διαφύλαξη (preservation) στην οποία έχουμε την διατήρηση της ακεραιότητας των στοιχείων που έχουν συλλεχθεί κατά την διάρκεια της έρευνας. Στο στάδιο αυτό υπάρχει και η διαδικασία της ιεραρχίας των αποδεικτικών στοιχείων (chain of custody), κατά την οποία καταγράφεται από ποιο σημείο συλλέχθηκε ένα στοιχείο, σε ποιο χρονικό σημείο, σε ποια κατάσταση, που θα μεταφερθεί αργότερα κτλ. Η διαφύλαξη είναι ένα σημαντικό βήμα για τις υπόλοιπες φάσεις. Στη συνέχεια είναι η συλλογή (collection) που τα δεδομένα και οι πληροφορίες συλλέγονται με την βοήθεια εγκεκριμένων εργαλείων. Η εξέταση (examination) έρχεται αμέσως μετά και έχει να κάνει με την ιχνηλασιμότητα των πειστηρίων, τις τεχνικές επικύρωσης και φιλτραρίσματος και την εξαγωγή και ανακάλυψη των κρυμμένων στοιχείων. Με την ανάλυση (analysis) όπου έχουμε εξόρυξη δεδομένων (datamining) και πραγματοποίηση του χρονοδιαγράμματος, περνάμε και στο τελευταίο βήμα, που είναι η παρουσίαση (presentation) και κατά την οποία ο ερευνητής τεκμηριώνει και καταθέτει για τα ευρήματά του (Palmer, 2001).

- Digital Forensics Investigation Model (DFIM)

Το DFIM, που προτάθηκε από τους Ademu et al. (Ademu, Imafidon, & Preston, 2011), είναι ένα μοντέλο που χωρίζεται σε 4 επίπεδα με επαναλαμβανόμενες διαδικασίες σε κάθε επίπεδο. Το πρώτο επίπεδο είναι η προετοιμασία το οποίο συμβαίνει καθ’ όλη την διάρκεια της έρευνας ως την παρουσίαση. Σέ αυτό το επίπεδο περικλείονται η προετοιμασία, η αναγνώριση, η εξουσιοδότηση και η επικοινωνία. Στο δεύτερο επίπεδο (η φάση της αλληλεπίδρασης) υπάρχουν οι κανόνες της συλλογής, διατήρησης και τεκμηρίωσης. Η φάση της ανοικοδόμησης περιλαμβάνει τους κανόνες της εξέτασης, διερευνητικές δοκιμές και ανάλυση. Όλα αυτά μας οδηγούν στο τέταρτο επίπεδο που είναι η παρουσίαση με κανόνες, όπως το αποτέλεσμα και η αναφορά.

- Abstract Digital Forensic Model (ADFM)

Οι Reith et al. (Reith, Carr, & Gunsch, 2002), μετά από εξέταση διαφόρων μοντέλων της ψηφιακής εγκληματολογίας, χρησιμοποίησαν το μοντέλο DFRWS ως πηγή έμπνευσης για να παρουσιάσουν το δικό τους μοντέλο το Abstract Digital Forensic Model. Οι δημιουργοί του ισχυρίζονται πως το μοντέλο τους μπορεί να βελτιώσει το μοντέλο DFRWS Investigative Model, αφού εμπνέεται από αυτό. Αποτελείται από:

i. Ταυτοποίηση (Identification): Είναι η αναγνώριση ενός περιστατικού και ο καθορισμός του συμβάντος. Είναι μια σημαντική φάση γιατί επηρεάζει και άλλα βήματα.
ii. Προετοιμασία (Preparation): Περιλαμβάνει την προετοιμασία εργαλείων, τεχνικές εξουσιοδοτήσεις και διαχείριση.

iii. Στρατηγική Προσέγγισης (Strategy Approach): Αναπτύσσεται μια προσέγγιση για την μεγιστοποίηση της συλλογής ατελών πειστηρίων από την σκηνή του εγκλήματος.

iv. Διατήρηση (Preservation): Εμπλέκει την απομόνωση, ασφάλιση και διατήρηση της κατάστασης των φυσικών και ψηφιακών αποδείξεων.

v. Συλλογή (Collection): Είναι το βήμα για την καταγραφή της φυσικής σκηνής και αντιγραφής των ψηφιακών στοιχείων χρησιμοποιώντας τυποποιημένες και αποδεκτές διαδικασίες.

vi. Εξέταση (Examination): Μια αναζήτηση εις βάθος για αποδείξεις που σχετίζονται με το έγκλημα. Η εστίαση βρίσκεται στο να ταυτοποιηθούν και να εντοπιστούν τα πιθανά πειστήρια.

vii. Ανάλυση (Analysis): Εδώ αποφασίζεται το πόσο σημαντικό και ποία είναι η αποδεικτική αξία του εξεταζόμενου στοιχείου.

viii. Παρουσίαση (Presentation): Σύνοψη και επεξήγηση.

ix. Επιστροφή Αποδεικτικών Στοιχείων (Returning Evidence): Επιστροφή της φυσικής και ψηφιακής περιουσίας στον ιδιοκτήτη.

- The Integrated Digital Investigation Process Model (IDIP)

Οι Carrier and Spafford (Carrier&Spafford, 2003) πρότειναν ένα μοντέλο ψηφιακής έρευνας που περιέχει φυσικά και ψηφιακά πειστήρια σε μια ενοποιημένη διαδικασία. Τα βασικά χαρακτηριστικά του μοντέλου αυτού είναι ο διαχωρισμός της έρευνας στο φυσικό και ψηφιακό τόπο του εγκλήματος. Τα αντικείμενα που βρίσκονται στην σκηνή τα χειρίζεται ο ερευνητής ως φυσικές αποδείξεις χρησιμοποιώντας παραδοσιακά μοντέλα έρευνας. Αν αυτά τα αντικείμενα είναι πηγές ψηφιακών αποδείξεων εξετάζονται σύμφωνα με την ψηφιακή σκηνή του εγκλήματος. Το μοντέλο αυτό είναι χωρισμένο σε 17 φάσεις και 5 ομάδες.

- A Model for Hybrid Evidence Investigation

Οι Vlachopoulos et al. το 2013(Vlachopoulos, Magkos, & Chrissikopoulos, 2013) πρότειναν ένα μοντέλο που μπορεί να εφαρμοστεί σε περιπτώσεις όπου τα πειστήρια είναι και φυσικά και ψηφιακά. Για αυτό και ονομάστηκε υβριδικό. Βέβαια, μπορεί να χρησιμοποιηθεί και σε περιπτώσεις που υπάρχουν είτε ψηφιακές, είτε φυσικές αποδείξεις. Το μοντέλο αποτελείται από 4 φάσεις και 12 μικρότερες.

i. Φάση πρώτη: Προετοιμασία (Preparation)
   - Ειδοποίηση (Notification): Ειδοποίηση ότι διαπράχθηκε ένα έγκλημα.
   - Εξουσιοδότηση (Authorization): Παρέχεται από τον οργανισμό που έχει οριστεί να διεξάγει την έρευνα.

- Προετοιμασία (Preparation): Περιλαμβάνει την διαθεσιμότητα των εξοπλισμού και του προσωπικού που θα διεξάγει την έρευνα.

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

- Διατήρηση (Preservation): Ο πρώτος που φτάνει στον τόπο του εγκλήματος είναι υπεύθυνος για να οργανώσει, για παράδειγμα την ασφάλεια της σκηνής, ποιος μπορεί να πλησιάζει και ποιος όχι.
- Ταυτοποίηση (Identification): Σε αυτό το σημείο αναγνωρίζονται τα πιθανά πειστήρια από τους ειδικούς.
- Συλλογή – Εξέταση (Collection-Examination): Ο ερευνητής συλλέγει στοιχεία που έχουν σχέση με το έγκλημα. Αυτά μπορεί να είναι φυσικά (π.χ., δακτυλικά αποτυπώματα), αλλά μπορεί να είναι και ψηφιακά. Ακόμα, μπορεί να διεξαχθεί εξέταση αλλά όχι όπως σε εργαστηριακό επίπεδο. Δεν πρόκειται δηλαδή για την κανονική εξέταση των στοιχείων.
- Μεταφορά (Transportation): Αν και η μεταφορά θεωρείται ως δευτερεύουσα διαδικασία ο Βλαχόπουλος et al. την θεωρούν σημαντική για τα μέτρα προστασίας των αποδεικτικών που πρέπει να λάβει κάποιος κατά την μεταφορά.

iii. Φάση τρίτη: Εργαστηριακή εξέταση (Laboratory examination)

- Εξέταση (Examination): Πρόκειται για την εξέταση των αποκτηθέντων στοιχείων στο εργαστήριο που μπορεί να δώσει απαντήσεις για στοιχεία.
- Αποθήκευση (Storage): Μετά την εξέταση τα στοιχεία θα πρέπει να αποθηκευτούν σε ασφαλή χώρο.
- Αναφορά (Report): Η αναφορά περιέχει το αποτέλεσμα της εργαστηριακής εξέτασης και αποτελεί μια σημαντική διεργασία.

iv. Φάση τέταρτη: Συμπέρασμα (Conclusion)

- Ανακατασκευή (Reconstruction): Η ανακατασκευή της σκηνής είναι ευθύνη του ερευνητή που αξιολογεί τα στοιχεία και παρουσιάζει τα γεγονότα.
- Διάχυση (Dissemination): Είναι η τελευταία διαδικασία του μοντέλου. Γίνεται μια λεπτομερής ανασκόπηση της έρευνας για να διαχυθούν οι γνώσεις που αποκτήθηκαν και να χρησιμοποιηθούν σε επόμενες παρόμοιες περιπτώσεις.

Μοντέλο	Ερευνητές	Χρονιά	Φάσεις/Στάδια
NIST	Ινστιτούτο NIST	2006	4
DFRWS	Ερευνητές DFRWS	2001	6
Digital Forensics Investigation Model (DFIM)	Ademu, I.O., Imafidon, C.O. Preston, D.S.,	2011	4
Abstract Digital Forensic Model (ADFM)	Reith, M., Carr, C. and Gunsch, G.	2002	9
The Integrated Digital Investigation Model (IDIP)	Carrier, B. and Spafford	2003	17
A Model for Hybrid Evidence Investigation	Vlachopoulos, K., Magkos, E. and Chrissikopoulos, V.	2013	4

Πίνακας 1: Λίστα με τα μοντέλα έρευνας

3.6 Προκλήσεις στην Ψηφιακή Εγκληματολογία

Με την όλο και μεγαλύτερη εξέλιξη της τεχνολογίας η επιστήμη της ψηφιακής εγκληματολογίας θα θεωρείται όλο και πιο χρήσιμη για επιλύσεις τέτοιων υποθέσεων. Η ποικιλομορφία των πηγών θα απαιτεί την ανάλυσή τους από ερευνητές. Οι προκλήσεις και οι δυσκολίες βέβαια είναι πολλές, υπήρχαν από πάντα και θα συνεχίσουν να υπάρχουν. Σε αυτήν την ενότητα θα παρουσιαστούν οι πιο σημαντικές σύμφωνα με τους Karie και Venter (Karie & Venter, 2015).

Κρυπτογράφηση: Η πρόοδος των τεχνολογιών επικοινωνίας, όπως λόγου χάρη το Διαδίκτυο συμπαρασύρει και τα λογισμικά κρυπτογράφησης ώστε να εξελίσσονται και να γίνονται ακόμα πιο περίπλοκα από ό,τι ήταν. Έτσι η καθημερινότητα ενός ερευνητή γίνεται πιο δύσκολη όταν πρέπει να πραγματοποιήσει μια αποκρυπτογράφηση.

Μεγάλος όγκος δεδομένων: Έχει σημειωθεί πολύ μεγάλη αύξηση στα μέσα αποθήκευσης των δεδομένων τόσο στα προσωπικά, όσο και στα εταιρικά συστήματα. Άρα ο κάθε χρήστης έχει τη δυνατότητα να αποθηκεύει τεράστιο όγκο. Οι συνέπειες αυτής της εξέλιξης είναι ο χρόνος που χρειάζεται για να αποκτηθούν και να αναλυθούν τα στοιχεία.

Ασυμβατότητα μεταξύ των εργαλείων: Πολλά εργαλεία συχνά δεν μπορούν να συνεργαστούν μεταξύ τους, γιατί ενδέχεται να έχουν διαφορετική λειτουργία, κόστος ή και πολυπλοκότητα. Αυτό συμβαίνει διότι δεν φτιάχνονται όλα τα εργαλεία για τον ίδιο σκοπό: κάποια προσφέρουν λιγότερες λειτουργίες και κάποια άλλα μία γκάμα λειτουργιών.

Αστάθεια των ψηφιακών πειστηρίων: Σε αυτήν την ιδιαιτερότητα των πειστηρίων αναφερθήκαμε και σε προηγούμενη ενότητα σε αυτό το κεφαλαίο. Κάποια στοιχεία έχουν το ιδιαίτερο χαρακτηριστικό να είναι εύθραυστα. Μπορεί κάποια λειτουργία όπως η ενεργοποίηση, η επανεκκίνηση, η απώλεια της μπαταρίας να τα καταστρέψουν. Αντιλαμβάνεται κανείς πως ο κάθε ερευνητής έχει να αντιμετωπίσει μια πολύ σοβαρή πρόκληση όταν ξεκινάει την έρευνα ενός περιστατικού.

Περιορισμοί Bandwidth: Υπάρχουν περιπτώσεις όπου η αναμετάδοση των στοιχείων μπορεί να είναι αργή λόγου του δικτύου, επειδή η υπολογιστική μηχανή που καλείται ο ερευνητής να αντιγράψει τα στοιχεία προς το δικό του μηχάνημα για ανάλυση είναι ήδη σε λειτουργία και ενδεχόμενη απενεργοποίηση θα προκαλέσει ανεπανόρθωτα προβλήματα και απώλειες.

Περιορισμένη διάρκεια ζωής ψηφιακών μέσων: Η ικανότητα πλέον των ψηφιακών μέσων να αποθηκεύουν έχει φτάσει σε πολύ μεγάλο βαθμό, όπως αναφέρθηκε προηγουμένως. Ωστόσο, η μακροχρόνια αποθήκευση δεν πρέπει να θεωρείται δεδομένη. Η απώλεια έστω και ενός bit είναι ικανή να προκαλέσει την καταστροφή των δεδομένων.

Επιτήδευση των ψηφιακών εγκλημάτων: Σύμφωνα με την ACPO οι ερευνητές συχνά βρίσκονται αντιμέτωποι με καινούργια εργαλεία που χρησιμοποιούν οι hackers και καινούργια λογισμικά. Λόγω αυτού οι έρευνες γίνονται ακόμα πιο χρονοβόρες.

Αναπτυσσόμενες Τεχνολογίες και Συσκευές: Νέες και εξελισσόμενες τεχνολογίες ξεπροβάλλουν πλέον όλο και με μεγαλύτερη ταχύτητα. Αντιμετωπίζοντας ένα καινούργιο σύστημα, είτε σε επίπεδο λογισμικού, είτε σε επίπεδο συσκευής που ο ερευνητής δεν έχει ξανασυναντήσει θα πρέπει να προσαρμόσει τα εργαλεία του και το τρόπο προσέγγισης σύμφωνα με αυτά.

Περιορισμένο παράθυρο για συλλογή ψηφιακών πειστηρίων: Κατά την συλλογή των πειστηρίων είναι σημαντικό για τους ερευνητές να αντιλαμβάνονται ποια στοιχεία θα αποκτήσουν πρώτα. Ειδικότερα όταν πιέζει ο χρόνος οι αποφάσεις παίρνονται πιο γρήγορα.

Τα Antiforensics: Η συγκεκριμένη συλλογή εργαλείων έχει δημιουργηθεί με σκοπό να εμποδίζει το έργο των εργαλείων της ψηφιακής εγκληματολογίας. Αυτό πρακτικά έχεις ως αποτέλεσμα να δυσκολεύει τον ερευνητή, αφού τα εργαλεία αυτά μπορούν να διαταράσσουν τις πληροφορίες.

Απόκτηση πληροφοριών από συσκευές διαφορετικές των ηλεκτρονικών υπολογιστών: Η απόκτηση στοιχείων από υπολογιστές ίσως είναι πιο εύκολη διαδικασία σε σχέση με την απόκτηση

από κινητά τηλέφωνα, wearables, έξυπνες συσκευές και γενικότερα από αντικείμενα του Διαδικτύου των Πραγμάτων. Ωστόσο, θα ασχοληθούμε εκτενέστερα παρακάτω.

Προκλήσεις σχετιζόμενες με την τεχνολογία του "νέφους" (cloud): Οι τεχνολογίες "νέφους" έχουν βοηθήσει στο έπακρο τις επιχειρήσεις, διότι τους εξοικονομούν χρήματα για εξοπλισμό. Ο ερευνητής θα πρέπει να υπολογίσει την δικαιοδοσία και την ετερογένεια του νέφους όταν χρησιμοποιεί τέτοιες υπηρεσίες, διότι μπορεί να αποτελέσουν τροχοπέδη στην έρευνα.

3.7 Εργαλεία Ψηφιακής Εγκληματολογίας

Ένα σημαντικό κεφάλαιο στην ψηφιακή εγκληματολογία είναι τα εργαλεία. Αυτά αποτελούν σημαντική μέριμνα για τον ερευνητή κατά την διάρκεια της έρευνας. Κάποιος μπορεί να βρει εργαλεία που μπορεί να είναι είτε εμπορικά, είτε ανοιχτού κώδικα και δωρεάν.

Η επιλογή του εργαλείου καλό είναι να γίνεται σύμφωνα με την περίπτωση που εργάζεται ο ειδικός. Το ινστιτούτο NIST (NIST, n.d.) έχει δημιουργήσει μια βάση με όλα σχεδόν τα εργαλεία που κυκλοφορούν στην αγορά. Τα εργαλεία έχουν διαχωριστεί με βάση τις λειτουργίες τους. Καλό θα ήταν να αναφερθούν επιγραμματικά οι κατηγορίες που εμφανίζονται στην ιστοσελίδα:

- Cloud services
- Database forensics
- Deleted file recovery
- Disk imaging
- Drone forensics
- Email parsing
- File Carving
- Forensics Boot Environment
- Forensics tool suite
- GPS forensics
- Hardware write block
- Hash analysis
- Image analysis
- Infotainment & vehicle forensics
- Instant Messenger
- Media sensitization/ drive re-use
- Memory capture and analysis
- Mobile device acquisition, analysis & triage
- P2P analysis
- Password recovery
- Remote capabilities/ Remote forensics
- Social media
- Software write block
- Steganalysis
- String search
- Video analytics
- VoIP forensics
- Web browser forensics
- WiFi forensics
- Windows registry analysis

Η πληθώρα των εργαλείων είναι μεγάλη. Με αυτά ο ερευνητής είναι σε θέση να ανακαλύψει τα ψηφιακά πειστήρια που θα τον οδηγήσουν σε ασφαλή συμπεράσματα. Παρακάτω

θα ακολουθήσει μια βιβλιογραφική ανασκόπηση μερικών τέτοιων εργαλείων. Πρόκειται για τα πιο διαδεδομένα.

Forensic Toolkit (FTK): Το FTK είναι ένα εργαλείο που έχει δημιουργηθεί από την εταιρεία AccessData. Είναι γρήγορο, σταθερό και εύκολο στην λειτουργία του χάρη στο περιβάλλον του. Χρησιμοποιεί κατανεμημένη επεξεργασία και με αυτόν τρόπο αξιοποιεί πλήρως τους πολλούς πυρήνες των υπολογιστών. Έτσι, εκμεταλλεύεται πλήρως τις δυνατότητες του συστήματος για καλύτερο αποτέλεσμα. Το FTK παρέχει ολοκληρωμένη επεξεργασία και indexing, με επακόλουθο το φιλτράρισμα και η αναζήτηση να γίνονται γρηγορότερα. Είναι βασισμένο σε βάση δεδομένων και χρησιμοποιεί μια βάση που είναι προσβάσιμη από τις ομάδες που δουλεύουν. Όλα τα δεδομένα αποθηκεύονται στην ίδια βάση, ασφαλή και έτσι όλοι έχουν πρόσβαση στα ίδια σημεία. Κατά αυτόν τον τρόπο υπάρχει μείωση του κόστους και της πολυπλοκότητας για την δημιουργία πολλών συνόλων με δεδομένα. Το FTK είναι εμπορικής χρήσης και η αξία αγοράς του ανέρχεται στα $3.995 για την τελευταία έκδοση που είναι η Forensics Toolkit 6.2. (Accessdata, n.d.)

Digital Forensics Framework (DFF): Είναι ένα λογισμικό ανοιχτού κώδικα γραμμένο σε C++, Python. Το DFF προσφέρει γραφικό περιβάλλον που έχει αναπτυχθεί στο PyQt4[1]. Χρησιμοποιείται για την συλλογή, διατήρηση και αποκάλυψη ψηφιακών πειστηρίων χωρίς να διακινδυνεύουν υπολογιστικά συστήματα και πληροφορίες. Επιπρόσθετα, ο χρήστης μπορεί να ανακτήσει κρυφά στοιχεία ή ακόμα και διαγραμμένα. Παρέχεται σε τρεις εκδόσεις: την DFF που είναι δωρεάν, την DFF Pro και την DFF Live. Οι δύο τελευταίες είναι εμπορικής χρήσης. Μπορούν να χρησιμοποιηθούν σε λειτουργικά συστήματα Windows και Linux.(Digital Forensics Framework, n.d.)

The Sleuth Kit: Είναι ένα λογισμικού ανοιχτού κώδικα γραμμένο σε C και Perl. Το Sleuth Kit είναι μια βιβλιοθήκη και μια συλλογή από εντολές που δίνουν την δυνατότητα στον χρήστη να ερευνήσει τον δίσκο. Η βασική λειτουργία του προγράμματος επιτρέπει την ανάλυση μεγάλου όγκου δεδομένων και στοιχείων του συστήματος. Συν τοις άλλοις, μπορεί να ενσωματωθεί σε μεγαλύτερα εργαλεία ψηφιακής εγκληματολογίας και να οδηγήσει κατ' ευθείαν στην εύρεση πειστηρίων. Το **Autopsy** που είναι μια πλατφόρμα προσφέρει γραφικό περιβάλλον για το Sleuth Kit και παρέχει διαχείριση περιπτώσεων, αναζήτηση λέξεων-κλειδιά και πολλές άλλες αυτόματες λειτουργίες. Χρησιμοποιείται στα λειτουργικά συστήματα Windows και Linux. (Sleuthkit)

[1]Το PyQt προσφέρει στον χρήση widgets. Είναι μια διεπαφή Python για Qt, μια από τις πιο ισχυρές και διαδεδομένες βιβλιοθήκες γραφικού περιβάλλοντος και έχει την δυνατότητα να λειτουργήσει και σε πολλαπλά λειτουργικά συστήματα (Windows, OSX, Linux, Android).

Blacklight: Το Blacklight είναι ένα εργαλείο ανάλυσης που επιτρέπει τον ερευνητή γρήγορα να εκτελέσει μια ψηφιακή έρευνα. Μπορεί να χρησιμοποιηθεί σε συσκευές που έχουν εγκαταστημένο λειτουργικό σύστημα MacOS, iOS συσκευές αλλά και σε συστήματα με Windows. Οι δυνατότητές του επεκτείνονται ακόμα και στα μέσα κοινωνικής δικτύωσης και σε υπηρεσίες ανταλλαγής μηνυμάτων. Το κόστος του για έναν χρήστη ανέρχεται στα $3400. (BlackbagtechTechnologies, n.d.)

XRY: Το XRY είναι ένα λογισμικό φτιαγμένο από την εταιρεία MSAB. Δίνει στον χρήστη την δυνατότητα να εξάγει δεδομένα και πληροφορίες που μπορεί να του χρησιμεύσουν ως αποδείξεις από συσκευές που μπορεί να είναι έξυπνα κινητά τηλέφωνα, GPS, μόντεμ, tablets. Η τιμή για την αγορά του είναι στα $7990 και χρησιμοποιείται για λειτουργικά συστήματα Windows.(MSAB, n.d.)

Digital Evidence & Forensic Toolkit (DEFT): Το DEFT είναι μια διανομή Linux. Σύμφωνα με τον κατασκευαστή του προγράμματος αποτελείται από GNU/Linux και την σουίτα Digital Advanced Response Toolkit (DART). Το συγκεκριμένο πρόγραμμα είναι μια λύση που βρίσκει εφαρμογή ακόμα και σε νομικές υπηρεσίες και η διανομή του είναι δωρεάν. (deft, n.d.)

Internet Evidence Finder (IEF): Το συγκεκριμένο εργαλείο είναι της εταιρείας magnetforensics. Είναι φιλικό προς τον χρήστη λόγω του γραφικού του περιβάλλοντος. Η ικανότητα του IEF έχει να κάνει με την εύρεση, ανάλυση και παρουσίαση των πειστηρίων από υπολογιστές, έξυπνα κινητά τηλέφωνα ακόμα και tablets. Αυτά μπορεί να είναι είτε στοιχεία από μηνύματα ή μέσα κοινωνικής δικτύωσης και ακόμα από πολλές πηγές. Το κόστος του ανέρχεται στα $1700 για ένα χρήστη και υποστηρίζει τα λειτουργικά συστήματα Windows, Linux, MacOSX. (Magnetforensics, n.d.)

Sans Investigative Forensics Toolkit (SIFT): Το SIFT φτιάχτηκε βασισμένο στο Ubuntu. Είναι κυρίως δωρεάν ωστόσο κάποια plug-in κοστίζουν. Το λογισμικό είναι πολλαπλών χρήσεων και συνοδεύεται απ’ όλα τα εργαλεία που μπορεί να χρειαστεί κάποιος. (Digital Forensics, n.d.)

EnCase: Το EnCase είναι από τα πιο διαδεδομένα λογισμικά αυτού του είδους. Με το εργαλείο αυτό ο ερευνητής έχει την δυνατότητα να συλλέξει πληροφορίες από διάφορες ηλεκτρονικές συσκευές. Έχει ένα φιλικό προς τον χρήστη περιβάλλον και την ικανότητα να παράγει αυτόματα αναφορά. Εκτός από αυτά μπορεί να αποκρυπτογραφήσει στοιχεία που θα φανούν χρήσιμα κατά την διάρκεια της έρευνας. Το κόστος για μία άδεια κοστίζει $3594. (EncaseForensic, n.d.)

Computer Aided Investigative Environment (CAINE): Είναι ένα λογισμικό ανοιχτού κώδικα Linux διανομή με φιλικό προς τον χρήστη περιβάλλον και αντίστοιχα εργαλεία. Διανέμεται δωρεάν. (CAINE, n.d.)

X-Ways forensics: Υποστηρίζει μόνο τα λειτουργικά συστήματα Windows. Μπορεί να βρει διαγραμμένους φακέλους. Οι απαιτήσεις του όσον αφορά την εγκατάσταση είναι φυσιολογικές χωρίς να χρειάζεται κάτι ιδιαίτερο από άποψη υλικού. Δεν απαιτεί εγκατάσταση και εκτελείται απλά από μια USB συσκευή σε περίπτωση που ο χρήστης δεν επιθυμεί την εγκατάστασή του. Η τιμή για μια άδεια χρήσης κοστίζει περίπου $1065. (X-Ways, n.d.)

3.8 Κλάδοι Ψηφιακής Εγκληματολογίας

Η Ψηφιακή Εγκληματολογία είναι μια πολυδιάστατη επιστήμη η οποία έχει αρκετούς κλάδους. Διαχωρίζεται στην εγκληματολογία δικτύων, εγκληματολογία υπολογιστών, εγκληματολογία βάσεων δεδομένων και στον πιο πρόσφατο κλάδο ο οποίος είναι η εγκληματολογία στο Διαδίκτυο των Πραγμάτων.

Η *Εγκληματολογία δικτύων (NetworkForensics)* περιστρέφεται γύρω από τα δίκτυα υπολογιστών και έχει ως στόχο να αποδείξει με ποιον τρόπο έγινε μια παραβίαση. Αναλύοντας και ανακτώντας τα πακέτα που κινούνται σε ένα δίκτυο ο ερευνητής προσπαθεί να εξηγήσει και να παρέχει εκείνα τα αποδεικτικά στοιχεία που θα καταφέρουν να συνδράμουν σε μια έρευνα. Μελετώντας τα logs, τις κινήσεις που κατέγραψε το firewall του χρήστη και με τα διάφορα εργαλεία του ο ερευνητής μπορεί να φτάσει σε κάποια πρώτα συμπεράσματα.

Η πρόκληση στην εύρεση των αποδεικτικών στοιχείων και στην ανίχνευση των συμβάντων έγκειται στο γεγονός πως λόγω της τεχνολογίας οι κακόβουλες ενέργειες μπορούν να αποκρύβουν εύκολα ή ακόμα και να φαίνονται σαν φυσιολογικές ενέργειες. Εκτός αυτής της πρόκλησης, υπάρχει και το μειονέκτημα για τους ερευνητές πως τα δεδομένα στα δίκτυα είναι πιο ρευστά και πιο ευμετάβλητα σε σχέση με τα στοιχεία που υπάρχουν σε κάποιον σκληρό δίσκο. Επίσης, λόγω του τρόπου λειτουργίας τους τα δεδομένα μπορούν να ταξιδέψουν οπουδήποτε και να βρίσκονται σε οποιοδήποτε σημείο, κάνοντας δύσκολο για τον ερευνητή να τα εντοπίσει. Η ίδια κατάσταση ισχύει όμως και για τους κακόβουλους χρήστες που θα τους είναι αδύνατο να καταστρέψουν.

Η *Εγκληματολογία Υπολογιστών (ComputerForensics)* είναι λίγο-πολύ αυτό που έχει αναλυθεί στις προηγούμενες ενότητες. Σχετίζεται με την έρευνα για αποδεικτικά στοιχεία από σκληρούς δίσκους, USB συσκευές, CD, DVD, εκτυπωτές. Σκοπός είναι η παρουσίαση αυτών των στοιχείων εμπεριστατωμένα κατά την διάρκεια ενός δικαστηρίου. Ο ερευνητής με συγκεκριμένες τεχνικές και εργαλεία εργάζεται για το επιθυμητό αποτέλεσμα.

Σύμφωνα με τον Eoghan Casey (Casey, 2011) η ορολογία Εγκληματολογία Υπολογιστών (Computer Forensics) δεν είναι τόσο διαδεδομένη πια, διότι μετά το πρώτο DFRWS συμφωνήθηκε να αναθεωρηθεί, όπως και έγινε, και η κατάληξη ήταν η Ψηφιακή Εγκληματολογία (Digital Forensics) που είναι μία γενικότερη έννοια.

Η *Εγκληματολογία Βάσεων Δεδομένων (Database Forensics)* ανήκει και αυτή στην επιστήμη της Ψηφιακής Εγκληματολογίας. Ο σκοπός της δε διαφέρει από τους παραπάνω κλάδους. Εφαρμόζονται τεχνικές για τη συλλογή αποδεικτικών στοιχείων, αλλά σε βάσεις δεδομένων. Ο ερευνητής επικεντρώνεται στο timestamp που διαμορφώνεται ανάλογα με τις αλλαγές που πιθανότατα να έγιναν σε πίνακες στην βάση δεδομένων.

Η *Εγκληματολογία στο Διαδίκτυο των Πραγμάτων (Internet of Things Forensics)* είναι ο σχετικά νεότερος κλάδος στην ψηφιακή εγκληματολογία σε σχέση με τους προαναφερθέντες. Οι τεχνολογίες και οι συσκευές του Διαδικτύου των Πραγμάτων είναι πλέον ιδιαίτερα διαδομένες και αναμένεται να εξελιχθούν ακόμα παραπάνω. Οι συσκευές που συμμετέχουν στο IoT δεν είναι μόνο κινητά τηλέφωνα, αλλά και GPS, έξυπνες οικιακές συσκευές, έξυπνα τηλέφωνα, έξυπνες πόλεις.

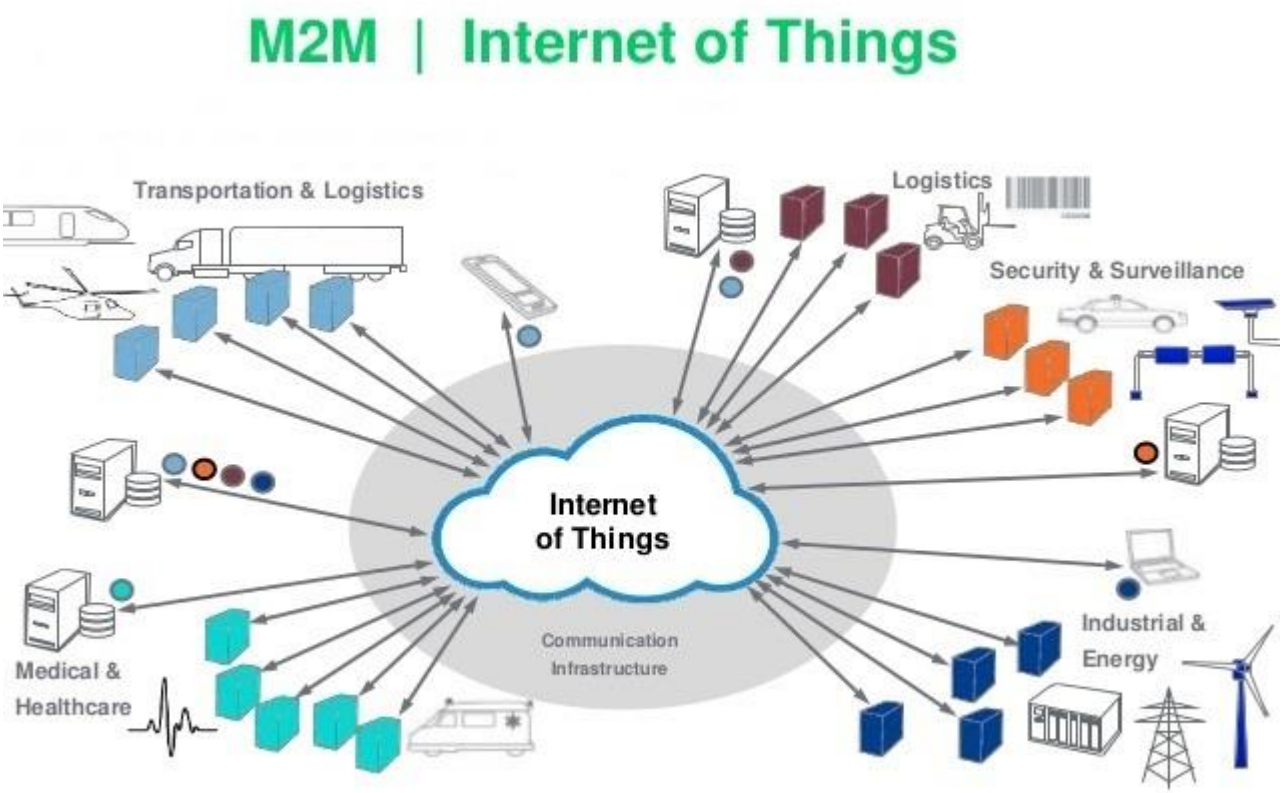
Όπως και οι υπολογιστές έτσι και οι συσκευές διαθέτουν μνήμη RAM, επεξεργαστή, αποθηκευτικούς χώρους και βέβαια δυνατότητα σύνδεσης στο δίκτυο και ανταλλαγής δεδομένων σε αυτό αλλά και αναμεταξύ τους. Μία σημαντική διαφορά όμως είναι η ποικιλία των συσκευών και των λειτουργικών συστημάτων που κυκλοφορούν στην αγορά και καθιστούν το έργο του ερευνητή πολύ δύσκολο. Οι ιδιαιτερότητες που μπορεί κανείς να συναντήσει είναι πολλές και θα αναφερθούν στο παρακάτω κεφάλαιο.

4. Διαδίκτυο των Πραγμάτων (Internet of Things)

4.1 Διαδίκτυο των Πραγμάτων (Internet of Things)

Η βασική ιδέα γύρω από το Διαδίκτυο των Πραγμάτων (Internet of Things-IoT), είναι η εξής: Οι διάφορες ηλεκτρονικές συσκευές οι οποίες έχουν την δυνατότητα να συνδέονται μεταξύ τους όπως και στο Διαδίκτυο και να μπορούν να ανταλλάσουν πληροφορίες, ακόμα και να αλληλεπιδρούν. Ο όρος προτάθηκε για πρώτη φορά από τον Kevin Ashton το 1999 (Ashton, 2009). Το IoT αποτελεί μια επανάσταση στο χώρο της τεχνολογίας. Βέβαια, ακόμα μεγαλύτερη επανάσταση αποτελεί το γεγονός πως πολλές φορές η ανθρώπινη συμμετοχή στην εύρυθμη λειτουργία των συσκευών δεν κρίνεται απαραίτητη. Τα αντικείμενα αυτά είναι ικανά να λειτουργούν αυτόνομα και ανάλογα με τις πληροφορίες που συλλέγουν από το περιβάλλον.

Απαρτίζεται από ηλεκτρονικές συσκευές, κινητά, κάμερες, επιστημονικά όργανα ακόμα και κτίρια, αρκεί όλα αυτά να έχουν ενσωματωμένα κυκλώματα, αισθητήρες, λογισμικό, Radio-Frequency IDentification (RFID) και την δυνατότητα της σύνδεσης με το Διαδίκτυο, ώστε να συλλέγουν και να μοιράζουν δεδομένα και πληροφορίες. Το αποτέλεσμα αυτών των δυνατοτήτων θα είναι η αυτοματοποίηση πολλών πτυχών της καθημερινότητάς μας.



Εικόνα 3: Το Διαδίκτυο των Πραγμάτων σε διάφορους τομείς.

Αξίζει να σημειωθεί πως σύμφωνα με έρευνα της Gartner μέχρι το 2020 θα υπάρχουν 20,8 δισεκατομμύρια συσκευές συνδεμένες στο Διαδίκτυο, οι οποίες θα παράγουν πάνω από 20 zettabytes δεδομένων (Gartner, 2013). Η Ericsson για την ίδια περίοδο εκτιμά πως περισσότερες από 16 δισεκατομμύρια ηλεκτρονικές συσκευές θα είναι διασυνδεμένες (Ericsson, 2016). Η ServiceMax υποστηρίζει πως το 2020 το 40% των δεδομένων που θα παράγονται θα είναι από συσκευές του IoT (ΣΕΠΕ, 2015). Επίσης, υπολογίζεται πως στα επόμενα 20 χρόνια θα επενδυθούν $41 τρισεκατομμύρια σε αναβαθμίσεις υποδομών ώστε να συνάδουν με το IoT. Από αυτούς τους αριθμούς αντιλαμβανόμαστε πόσο μεγάλο ρόλο θα παίζουν οι συσκευές αυτές στην ζωή μας τα επόμενα χρόνια.

4.2 Αρχιτεκτονική των IoT

Ο αριθμός των πληροφοριών που ανταλλάσσονται και κυκλοφορούν μεταξύ των συσκευών του Διαδικτύου των Πραγμάτων είναι ήδη πολλές και όπως είδαμε παραπάνω αναμένεται να αυξηθεί δραματικά τα προσεχή χρόνια. Μία βελτίωση που απαιτείται στο IoT είναι περισσότερος χώρος αποθήκευσης των δεδομένων αυτών. Εκτός από αυτό, η τεχνολογία του IoT θα βρεθεί αντιμέτωπη με προκλήσεις που αφορούν την ιδιωτικότητα και την ασφάλεια. Παρακάτω θα παρουσιαστεί η αρχιτεκτονική των IoT, η οποία χωρίζεται σε πέντε στρώματα (Wu, Lu, Ling, Sun, &Du, 2010):

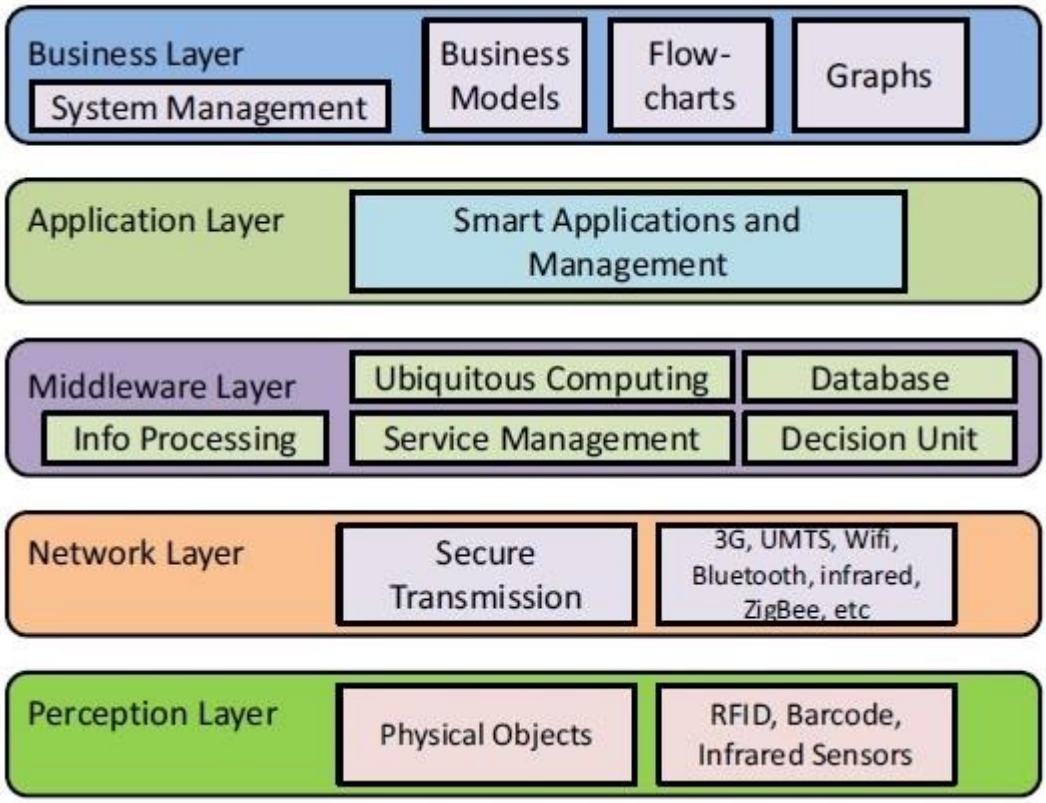
i. Στρώμα Αντίληψης: Το στρώμα αυτό λέγεται διαφορετικά και στρώμα συσκευής. Εδώ συγκαταλέγονται οι φυσικές συσκευές και όλα αυτά που περιέχουν όπως αισθητήρες, RFID. Ο στόχος είναι η ταυτοποίηση και συλλογή συγκεκριμένων πληροφοριών από τους αισθητήρες για περαιτέρω χρήση. Αυτά τα δεδομένα αφορούν αλλαγές στην θερμοκρασία, στην τοποθεσία, στην υγρασία, στον αέρα, κτλ. Όλα αυτά θα χρησιμοποιηθούν στο επόμενο στρώμα που είναι του Δικτύου.
ii. Στρώμα Δικτύου: Το στρώμα ονομάζεται και Μετάδοσης. Οι πληροφορίες των αισθητήρων από αυτό το στρώμα μεταδίδονται με ασφάλεια στο σύστημα της επεξεργασίας. Το μέσο που γίνεται η μετάδοση είναι είτε ασύρματο είτε μέσω καλωδίου με τις τεχνολογίες του 4G, WiFi, Bluetooth,κτλ. Έτσι, το στρώμα Δικτύου είναι ο μεσάζων ο οποίος μεταφέρει τις πληροφορίες από το στρώμα Αντίληψης στο επόμενο στρώμα που είναι το στρώμα Ενδιάμεσου Λογισμικού.
iii. Στρώμα Ενδιάμεσου Λογισμικού: Οι συσκευές του IoT υλοποιούν υπηρεσίες διαφορετικού τύπου. Κάθε συσκευή συνδέεται και επικοινωνεί με εκείνες τις συσκευές που υλοποιούν την ίδια υπηρεσία. Το στρώμα αυτό είναι υπεύθυνο για την διαχείριση και την σύνδεση με την

βάση δεδομένων. Δέχεται τις πληροφορίες από το προηγούμενο στρώμα που είναι του Δικτύου και τις αποθηκεύει στην βάση δεδομένων.

iv. Στρώμα Εφαρμογής: Αυτό το σημείο του στρώματος παρέχει την διαχείριση της εφαρμογής σύμφωνα με τις πληροφορίες, που η επεξεργασία τους έλαβε χώρα στο προηγούμενο στρώμα. Οι εφαρμογές που υλοποιούνται από τα IoT μπορεί να είναι γύρω από το έξυπνο σπίτι, τις έξυπνες πόλεις, έξυπνη γεωργία, κτλ.

v. Στρώμα Επιχείρησης: Το Στρώμα Επιχείρησης είναι υπεύθυνο για την διαχείριση του συνολικού συστήματος του IoT. Από τις πληροφορίες που λαμβάνει από το στρώμα της Εφαρμογής, ο χρήστης μπορεί να φτιάξει επιχειρησιακά μοντέλα και γραφήματα, τα οποία (αφού τα αναλύσει) θα λάβει αποφάσεις για ενέργειες και στρατηγικές που θα ακολουθήσει στο μέλλον.

Το Διαδίκτυο των Πραγμάτων είναι μια τεχνολογία που συνεχώς εξελίσσεται και δεν έχει υιοθετηθεί καμία σταθερή αρχιτεκτονική. Πολλοί ερευνητές έχουν προτείνει διάφορες, ώστε να εξηγήσουν πιθανούς τρόπους υλοποίησης του.



Εικόνα 4: Αρχιτεκτονική του Διαδικτύου των Πραγμάτων

4.3 Χαρακτηριστικά των IoT

Στην ενότητα αυτά θα παρατεθούν τα βασικά χαρακτηριστικά που έχουν οι συσκευές που συμμετέχουν στο Διαδίκτυο των Πραγμάτων. Αυτά είναι τα γνωρίσματα τέτοιων ηλεκτρονικών συσκευών που τις κάνουν να ξεχωρίζουν σύμφωνα με τον Patel (Patel & Patel, 2016).

- Διασυνδεσιμότητα.

Ότι αφορά το IoT, είναι συνδεδεμένο με την παγκόσμια υποδομή πληροφοριών. Δηλαδή οι συσκευές είναι συνδεμένες με το Διαδίκτυο και μεταξύ τους και πάντα ενημερώνονται και ανταλλάσσουν πληροφορίες.

- Υπηρεσίες σχετικά με τα αντικείμενα.

Το IoT είναι ικανό να παρέχει υπηρεσίες σχετικά με τα αντικείμενα μέσα από περιορισμούς, όπως είναι η προστασία της ιδιωτικότητας και η σημασιολογική συνοχή μεταξύ των φυσικών και των εικονικών αντικειμένων. Προκειμένου να παρέχονται υπηρεσίες σχετικά με τα αντικείμενα και οι δύο οι τεχνολογίες (στον φυσικό κόσμο και στον κόσμο της πληροφορίας) θα αλλάξουν.

- Ανομοιογένεια.

Οι συσκευές που συμμετέχουν στο IoT είναι διαφορετικές, αφού μπορεί να χρησιμοποιούν διαφορετικά υλικά και δίκτυα. Ωστόσο, έχουν την ικανότητα να αλληλεπιδρούν μεταξύ τους, αν και είναι διαφορετικά δομημένα.

- Δυναμικές αλλαγές.

Η κατάσταση λειτουργίας των συσκευών μπορεί να αλλάξει ανά πάσα στιγμή. Από την μια στιγμή στην άλλη, μία συσκευή μπορεί να είναι σε κατάσταση αναστολής λειτουργίας και ξαφνικά να συνδέεται με το δίκτυο ή με κάποια άλλη συσκευή. Επίσης, υπάρχει η περίπτωση της αλλαγής της τοποθεσίας και θα πρέπει η συσκευή να ενσωματωθεί με το καινούργιο περιβάλλον σε πολύ μικρό χρονικό διάστημα.

- Τεράστια Κλίμακα.

Ο αριθμός των συσκευών που πρέπει να αλληλεπιδράσουν μεταξύ τους για ανταλλαγή πληροφοριών είναι τεράστιος.

- Ασφάλεια.

Σημαντικό χαρακτηριστικό –στο οποίο θα αναφερθούμε και παρακάτω- είναι η ασφάλεια. Η ασφάλεια των συσκευών αυτών εξασφαλίζει στον χρήστη πως τα δεδομένα που διακινούνται στο Διαδίκτυο και μεταξύ των συσκευών είναι ασφαλή.

- Συνδεσιμότητα.

Η συνδεσιμότητα επιτρέπει την προσβασιμότητα και τη συμβατότητα σε ένα δίκτυο. Η προσβασιμότητα γίνεται σε ένα δίκτυο, ενώ η συμβατότητα παρέχει την δυνατότητα κατανάλωσης και παραγωγής δεδομένων.

4.4 Προκλήσεις Ασφάλειας στο IoT

Μπορούμε να φανταστούμε πόσο σημαντικό είναι οι συσκευές και οι τεχνολογίες που συμμετέχουν στο Διαδίκτυο των Πραγμάτων να είναι ασφαλείς από κακόβουλους χρήστες. Αν σκεφτούμε ότι το ίδιο το Διαδίκτυο είναι εκτεθειμένο σε κινδύνους σχεδόν από τη δημιουργία του έως σήμερα, καταλαβαίνουμε πως δε θα ισχύει κάτι διαφορετικό και στον κόσμο του IoT.

Η εκπληκτική εξέλιξη που γνωρίζει το Διαδίκτυο των Πραγμάτων και η θέληση των κατασκευαστών να δημιουργήσουν λόγω του ανταγωνισμού ολοένα και πιο γρήγορα, καινούργιες συσκευές και τεχνολογίες οδηγεί συχνά σε προβλήματα ασφάλειας, διότι δεν υπάρχει η κατάλληλη μερίμνα για ασφάλεια ή κάποιες φορές περνάει σε δεύτερη μοίρα. Σε συνδυασμό βέβαια με την συνεχή εξέλιξη των κακόβουλων χρηστών τα αποτελέσματα μπορεί να αποβούν μοιραία για τους χρήστες οι οποίοι μπορεί να είναι κυβερνήσεις, στρατός και μεγάλες επιχειρήσεις. Αρκεί να σκεφτούμε πόσες πληροφορίες και δεδομένα κυκλοφορούν ανάμεσα στις συσκευές.

Ποιες όμως είναι οι κυριότερες προκλήσεις ασφάλειας στο Διαδίκτυο των Πραγμάτων; Παρακάτω θα τις αναλύσουμε σύμφωνα με τους Conti et al. (Conti, Dehghantanha, Franke, & Watson, 2018).:

- Ταυτοποίηση

Η ταυτοποίηση επιτρέπει σε όλες τις διαφορετικές συσκευές που συμμετέχουν στο IoT να ενταχθούν και να αναγνωριστούν ενώ προέρχονται από διαφορετικά πλαίσια. Η ταυτοποίηση περιλαμβάνει την επαλήθευση των διαφορετικών διαδρομών αλλά και των σημείων από τα οποία περνάει η πληροφορία για να φτάσει στον προορισμό της. Η πραγματική πρόκληση σε αυτό το σημείο είναι η αποτελεσματική δημιουργία κλειδιών και η διαχείρισή τους. Μία γεννήτρια κρυπτογραφημένων κλειδιών και ανταλλαγής τους θα μπορούσε να δημιουργήσει υπερφόρτωση σε κόμβους του IoT.

- Εξουσιοδότηση και Έλεγχος Πρόσβασης

Η εξουσιοδότηση περιλαμβάνει προσδιορισμό των δικαιωμάτων πρόσβασης σε διαφορετικούς πόρους ενώ ο έλεγχος πρόσβασης εγγυάται πως πρόσβαση θα έχουν μόνον όσοι έχουν την κατάλληλη εξουσιοδότηση. Κάθε κόμβος στο IoT μπορεί να υποστηρίξει περιορισμένο αριθμό προσβάσεων, ο οποίος μπορεί να διαφέρει σε κάθε συσκευή στον ίδιο κόμβο. Επομένως, η ανάπτυξη και η διαχείριση εξουσιοδοτήσεων και ελέγχων πρόσβασης που προσαρμόζονται σε διαφορετικούς κόμβους είναι μια πρόκληση για ετερογενή δίκτυα.

- Ιδιωτικότητα

Η ανάπτυξη αυτόνομων αντικειμένων στο IoT που αντιλαμβάνεται και αποθηκεύει ευαίσθητα προσωπικά δεδομένα (όπως ιατρικά) θέτει ένα καινούργιο επίπεδο απειλής στην ιδιωτικότητα των ατόμων. Τις πιο πολλές φορές τα αντικείμενα καταφέρνουν να συλλέγουν δεδομένα για έναν χρήση χωρίς αυτός να το γνωρίζει και να το αντιλαμβάνεται. Άρα μπορούμε να πούμε πως παραβιάζεται ένα από τα πιο σημαντικά δικαιώματα του ανθρώπου. Υπάρχουν μηχανισμοί οι οποίοι παρέχουν ιδιωτικότητα προσανατολισμένοι προς τον χρήστη, προς το περιεχόμενο και προς το πλαίσιο[2]του χρήστη. Ωστόσο, είναι και αυτοί που περιέχουν κόμβους που λειτουργούν αυτόνομα και συλλέγουν πληροφορίες προσανατολισμένα προς τα αντικείμενα. Πέρα από αυτά, το γεγονός πως πολλές φορές τα προσωπικά δεδομένα των χρηστών παραμένουν στις ηλεκτρονικές συσκευές ακόμα και όταν δεν θεωρούνται πλέον χρήσιμα, μπορεί να γνωστοποιηθούν με μοιραία για τον χρήση αποτελέσματα. Για αυτό και ο εντοπισμός τέτοιων κόμβων θεωρείται αναγκαίος. Αυτό σημαίνει παραπάνω διεργασίες για την ηλεκτρονική συσκευή η οποία έχει περιορισμένη ισχύ λόγω της φύσης της.

- Αρχιτεκτονική Ασφαλείας

Η δημιουργία μιας αρχιτεκτονικής η οποία θα ξεπερνά τα προηγούμενα προβλήματα είναι πολύ σημαντική. Αυτή η αρχιτεκτονική θα πρέπει εκτός από τα παραπάνω να αντιμετωπίζει τις προκλήσεις που παρουσιάζονται - όχι εξαιτίας των συσκευών του IoT- στα Software Defined Networks (SDN) και στις τεχνολογίες ‘νέφους’ (cloud). Τα ζητήματα ασφαλείας αυτών των τεχνολογιών κληροδοτούνται από το IoT.

4.5 Εφαρμογές του IoT

Το Διαδίκτυο των Πραγμάτων έχει αρχίσει να γίνεται μέρος της ζωή μας χωρίς ίσως να το αντιλαμβανόμαστε. Σε αυτήν την ενότητα θα παρουσιαστούν κάποιες τέτοιες περιπτώσεις σύμφωνα με τους Atamli et al.(Atamli, 2014).

I. Διαχείριση ενέργειας:

Μία από τις πιο σημαντικές χρήσεις του IoT είναι αυτή της διαχείρισης ενέργειας, είτε πρόκειται για κατοικίες, είτε για μεγάλες βιομηχανίες. Από την στιγμή που τα αποθέματα ενέργειας στην Γη όλο και λιγοστεύουν κρίνεται επιτακτική η ανάγκη για την δημιουργία ενός συστήματος που θα μεριμνεί για την καλύτερη διαχείριση αυτών των αποθεμάτων.

[2]Το πλαίσιο σύμφωνα με τον Abowd είναι οποιαδήποτε πληροφορία που μπορεί να χρησιμοποιηθεί για να περιγράψει την κατάσταση μιας οντότητας. Η οντότητα μπορεί να είναι, είτε πρόσωπο, είτε χώρος που θεωρείται ότι σχετίζεται με την αλληλεπίδραση μεταξύ ενός χρήστη και μιας εφαρμογής.

Μία ηλεκτρονική συσκευή που έχει αισθητήρες και ενεργοποιητή μπορεί να διαχειριστεί σωστά την κατανάλωση ενέργειας, αφού αναλύσει τα δεδομένα του περιβάλλοντος με τον αισθητήρα που έχει και ανταποκρινόμενο σύμφωνα με ένα προκαθορισμένο πρόγραμμα εξοικονόμησης ενέργειας μέσω της λειτουργίας του ενεργοποιητή. Για παράδειγμα, σε ένα έξυπνο σπίτι ένας οικιακός θερμοστάτης είναι ένα απαραίτητο μέσο για τον έλεγχο της λειτουργίας της θερμοκρασίας του χώρου. Με τον αισθητήρα μπορεί ο θερμοστάτης να ελέγξει την θερμοκρασία του σπιτιού και σύμφωνα με τις ρυθμίσεις του χρήστη στέλνει πληροφορίες στον ενεργοποιητή για την στιγμή που θα πρέπει αυτός να δρομολογήσει αλλαγές. Ο θερμοστάτης προσαρμόζει την λειτουργία του ώστε να διατηρήσει την θερμοκρασία του σπιτιού στα επιθυμητά σύμφωνα με τον χρήστη επίπεδα. Έτσι, μπορεί να κλείσει όταν η θερμοκρασία φτάσει μία συγκεκριμένη τιμή ή μπορεί να λειτουργήσει όταν η θερμοκρασία είναι σε χαμηλά επίπεδα.

Στο IoT αυτός ο θερμοστάτης προσφέρει στον χρήστη πρόσθετες δυνατότητες. Για παράδειγμα ο χρήστης μπορεί να τον διαχειρίζεται απομακρυσμένα και έτσι μπορεί να προετοιμάζει τον χώρο για την επιστροφή του. Το λογισμικό του θερμοστάτη (αφού συμβουλευτεί την τοποθεσία του χρήστη από το κινητό του μέσω του GPS, μπορεί να ενεργοποιήσει ή να απενεργοποιήσει τη συσκευή. Έτσι, για παράδειγμα μπορεί ο θερμοστάτης να ενεργοποιήσει την θέρμανση του σπιτιού, όταν ο χρήστης επιστρέφει στην οικεία του. Επίσης, παρόμοιες δυνατότητες παρέχει και ο αισθητήρας κίνησης, ο οποίος αναγνωρίζει την κίνηση μέσα στον χώρο και ξεκινά την λειτουργία του σύμφωνα με αυτήν. Όταν ο χρήστης δεν είναι παρών (άρα δεν υπάρχει κίνηση), ο θερμοστάτης δεν λειτουργεί. Μέσα σε μικρό χρονικό διάστημα ο θερμοστάτης μαθαίνει τις συνήθειες του χρήστη και λειτουργεί σύμφωνα με αυτές.

II. Έξυπνα αυτοκίνητα:

Η Google μέχρι το 2020 (Bussiness Insider, 2016) επιθυμεί να έχει έτοιμα για το κοινό αυτόνομα αυτοκίνητα. Αυτή της την επιθυμία την συμμερίζονται και μεγάλες αυτοκινητοβιομηχανίες. Τα έξυπνα κινητά θα πάρουν την θέση των σημερινών κλειδιών και θα προσφέρουν στον χρήστη την δυνατότητα ελέγχου τους. Το Near Field Communication(NFC, n.d.) θεωρείται μια από τις τεχνολογίες κλειδί για την ανάπτυξη αυτών των δυνατοτήτων, διότι το κοντινό εύρος επικοινωνίας χαρίζει την ασφάλεια της φυσικής ύπαρξης του χρήστη.

Πλέον βέβαια ο χρήστης μπορεί να ξεκλειδώσει το αυτοκίνητό του και μέσω αυτού να περιηγηθεί στο Διαδίκτυο για να κατεβάσει κάποιον χάρτη ή να ενημερωθεί για την κίνηση που υπάρχει στους δρόμους. Το αυτοκίνητο έχοντας αυτά τα στοιχεί μπορεί μετά από την επεξεργασία τους να επιλέξει την καταλληλότερη διαδρομή, που θα είναι η γρηγορότερη και πιο οικονομική.

Εικόνα 5: Τα αυτοκίνητα στο IoT

Τα έξυπνα αυτοκίνητα μπορούν να συμβάλλουν στην μείωση των ατυχημάτων που συμβαίνουν στους δρόμους, με την δυνατότητα της μεταξύ τους επικοινωνίας και της επεξεργασίας δεδομένων που το καθένα στέλνει και δέχεται. Μεταξύ των άλλων, μπορούν να συμβάλλουν και σε ένα πιο ασφαλή κόσμο, στον όποιο μόνον όσοι βρίσκονται στην λίστα οδηγών του αυτοκινήτου θα έχουν την ευκαιρία να το οδηγήσουν. Με αυτόν τον τρόπο μειώνονται οι κλοπές .

Κάποιες από αυτές τις δυνατότητες έχουν ήδη υιοθετηθεί από διάφορες αυτοκινητοβιομηχανίες και βρίσκονται στην μαζική παραγωγή. Ωστόσο, ο δρόμος προς την τελειοποίηση των έξυπνων αυτοκινήτων είναι μακρύς και οι βελτιώσεις συνεχείς.

III. Έξυπνο σύστημα υγείας:

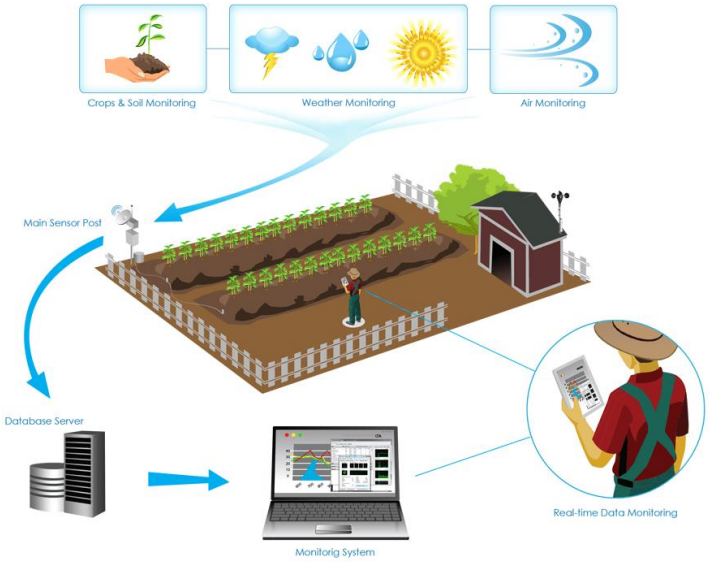
Όσο η διάρκεια ζωής αυξάνεται και νέες αρρώστιες εμφανίζονται, δημιουργείται και η ανάγκη για μεγαλύτερη και συνεχή παρακολούθηση των ασθενών, ιδιαίτερα των μεγαλύτερων σε ηλικία ή αυτών με χρόνιες παθήσεις. Ωστόσο, οι τωρινές εγκαταστάσεις στα νοσοκομεία είναι περιορισμένες. Είναι απαραίτητο να αναπτυχθούν δυνατότητες οι οποίες θα παρακολουθούν την κατάσταση του χρήστη όπου και αν βρίσκεται. Η χρήση IoT μπορεί να σταθεί αρωγός και να στέλνει τα δεδομένα στο κατάλληλο προσωπικό ή ακόμα να τα αναλύει για να προλαμβάνει ασθένειες που θα παρουσιαστούν στο μέλλον.

Προς το παρόν υπάρχουν συσκευές όπως οι βηματοδότες ή οι αντλίες ινσουλίνης που παρέχουν από μόνες τους άμεση βοήθεια στον χρήστη όταν αυτός την χρειαστεί.

4.6 Οφέλη του IoT στο μέλλον

Η ραγδαία εξέλιξη των εφαρμογών και συσκευών του Διαδικτύου των Πραγμάτων δείχνει πως με το πέρασμα του χρόνου εκτός από τις παραπάνω περιπτώσεις, θα βρει εφαρμογή σε κάθε πτυχή της καθημερινότητας του ανθρώπου χωρίς καμία εξαίρεση. Το 2012 οι Khan et al.(Khan, Khan, Zaheer, & Khan, 2012) παρουσίασαν μερικά τέτοια σημεία:

1. Πρόβλεψη φυσικών καταστροφών: Ο συνδυασμός των αισθητήρων, του αυτόνομου συντονισμό τους και η δυνατότητα προσομοίωσης που έχουνε μπορεί να βοηθήσει στην πρόβλεψη επικείμενων περιστατικών φυσικών καταστροφών ώστε να γίνουν οι κατάλληλες ενέργειες εκ των προτέρων.
2. Εφαρμογές στην βιομηχανία: Το IoT μπορεί στο μέλλον να βρει εφαρμογή στην βιομηχανία, όπως για παράδειγμα η διαχείριση του στόλου μιας εταιρείας. Οι συσκευές θα μπορούσαν μετά από την παρακολούθηση των ρύπων των αυτοκινήτων να αποφασίσουν ποια μολύνουν την ατμόσφαιρα και να στείλουνε προς συντήρηση.
3. Παρακολούθηση λειψυδρίας: Το IoT μπορεί να βοηθήσει να εντοπιστούν σημεία στα οποία υπάρχει λειψυδρία. Τα δίκτυα αισθητήρων μπορούν να παρακολουθούν τις μακροχρόνιες παρεμβάσεις στο νερό, αλλά μπορούν να ειδοποιούν και τους χρήστες αν πρόκειται να υπάρξει αύξηση της στάθμης ή αν απελευθερωθούν λύματα στο νερό με επικίνδυνες συνέπειες.
4. Σχεδίαση έξυπνων σπιτιών: Το Διαδίκτυο των Πραγμάτων θα ικανό μελλοντικά να βοηθήσει τους αρχιτέκτονες στην σχεδίαση έξυπνων σπιτιών με σκοπό την σωστή διαχείριση της ενέργειας, την γρήγορη ειδοποίηση για επείγοντα περιστατικά όπως φωτιά και την ασφάλεια της κατοικίας.
5. Ιατρικές εφαρμογές: Μια από τις σημαντικότερες εφαρμογές θα είναι στον ιατρικό τομέα, όπου οι συσκευές και το λογισμικό του IoT θα είναι σε θέση να σώζει ζωές ή να βελτιώνει την υγεία, με την παρακολούθηση ιατρικών παραμέτρων, παρακολούθηση και ειδοποίηση λήψης φαρμάκων.
6. Εφαρμογή στην γεωργία: Ένα δίκτυο αισθητήρων το όποιο θα μπορεί να επεξεργάζεται κα να αναλύει πληροφορίες ώστε να ειδοποιείται ο αγρότης για την κατάλληλη περίοδο που θα μπορεί να φυτεύει νέα σοδειά, να συλλέγει τους καρπούς, κτλ. Ακόμα με τέτοιου είδους πληροφορίες θα μπορεί ο γεωπόνος να συμβουλεύεις τους αγρότες για καταλληλότερες τεχνικές ώστε να παράγουν μεγαλύτερο και ποιο ποιοτικό προϊόν.



Εικόνα 5: Εφαρμογή στη γεωργία

7. Έξυπνο σύστημα μετακινήσεων: Με το σύστημα αυτό θα μπορεί η μετακίνηση του επιβατικού κοινού να είναι πιο αποτελεσματική, πιο γρήγορη και με λιγότερες καθυστερήσεις. Οι αισθητήρες θα ειδοποιούν για μποτιλιαρίσματα, για ατυχήματα ή ακόμα και για καλύτερη διαδρομή.
8. Σχεδίαση έξυπνων πόλεων: Το IoT εκτός της σχεδίασης έξυπνων σπιτιών όπως προαναφέρθηκε θα συμβάλλει και στην παρακολούθηση της ποιότητας του αέρα, στο παρκάρισμα, στην ασφάλεια των πολιτών ή της αποτελεσματικότερης λειτουργίας του δημόσιου φωτισμού, όπου μπορεί να εξοικονομηθεί πολύ ενέργεια.

Εικόνα 6: Έξυπνη πόλη και οφέλη

9. Έξυπνη καταμέτρηση και παρακολούθηση: Οι αισθητήρες και η τεχνολογία του IoT μπορούν να βρουν εφαρμογή και στην μέτρηση της ενέργειας που έχει ξοδέψει ένας χρήστης (π.χ., του ρεύματος) και να του στέλνουν ηλεκτρονικά τον λογαριασμό.
10. Έξυπνη Ασφάλεια: Στο τομέα της ασφάλειας και της παρακολούθησης η εφαρμογή αυτής της τεχνολογίας θα βοηθήσει στην παρακολούθηση ανθρώπων, υποδομών, πολύτιμων αντικειμένων, κτλ.

4.7 Ηλεκτρονικές συσκευές του IoT

Υπάρχουν πολλές εταιρείες που αντιλαμβάνονται πόσο σημαντική τεχνολογία είναι αυτή του IoT και πόσο επηρεάζει τις ζωές των ανθρώπων. Σε αυτήν την ενότητα θα αναφερθούμε σε κάποιες συσκευές που θεωρούνται συσκευές του IoT.

- Garmin Forerunner

Οι συσκευές αυτής της σειράς απευθύνεται σε ανθρώπους που ασχολούνται με τον αθλητισμό. Καταγράφουν τον καρδιακό παλμό, τα χιλιόμετρα που διανύει ο χρήστης και του δίνουν πληροφορίες γύρω από την προπόνησή του ώστε να βελτιώνεται. Οι τιμές κυμαίνονται από τα 81 € έως 575 €(Garmin, n.d.).

- AmazonEcho

Η συσκευή αυτή ουσιαστικά είναι ένα ηχείο το οποίο μπορεί να ακούσει τον χρήστη και να απαντήσει στις ερωτήσεις του και στις εντολές του, μπορεί να παίξει μουσική, να ενημερώσει τον χρήστη για τις ειδήσεις, την κίνηση τους δρόμους πριν αυτός ξεκινήσει για την εργασία του και κοστίζει περίπου 80 €(Amazon, n.d.).

- Arduino

Το Arduinoπροσφέρει ηλεκτρονικές πλακέτες ανοιχτού κώδικα οι οποίες έχουν ενσωματωμένους μικροελεγκτές και μπορούν να προγραμματιστούν. Τα μοντέλα είναι πολλά με τιμές έως τα 120 €(Arduino, n.d.).

- August Doorbell Cam

Η συσκευή αυτή είναι κάτι παραπάνω από ένα απλά κουδούνι πόρτας. Συνδέεται με το κινητό του χρήστη και η με την κάμερα του μπορεί να ο χρήστης να μιλήσει με τους ανθρώπους που βρίσκονται στην εξώπορτα, είτε αυτός βρίσκεται στο σπίτι, είτε όχι. Το κόστος της είναι 65 €(August, n.d.).

- Honeywell Smart House Products

Η εταιρεία αυτή προσφέρει συσκευές απαραίτητες για ένα έξυπνο σπίτι, όπως έξυπνες λάμπες, θερμοστάτες, συστήματα καταγραφής μέσω καμερών και πολλά άλλα(Honeywell, n.d.).

- Samsung SmarterThings

Η σειρά αυτή προσφέρει έξυπνες πρίζες, αισθητήρες κίνησης, αισθητήρες διαρροής νερού, κ.α. Η Samsungεπίσης προσφέρει ένα πλήρη εξοπλισμό οικιακής παρακολούθησης(Samsung, n.d.).

- Awair

Η Awairμε αξία 188 € βοηθάει τους ανθρώπους που υποφέρουν από αλλεργίες και άσθμα. Είναι μια συσκευή που αναλύει την ποιότητα αέρα και στέλνει πληροφορίες στο έξυπνο κινητό του χρήστη για συμβουλές βελτίωσής του (AWAIR, n.d.).

- Roost

Το Roost είναι μια έξυπνη μπαταρία που χρησιμοποιείται σε ανιχνευτές καπνού.Η μπαταρία αυτή ειδοποιεί τον χρήστη για την στιγμή που πρέπει να την αλλάξει και η τιμή της είναι περίπου 20€(Roost, n.d.).

- CargoSense

Το CargoSense αποτελεί μια λύση για μεγάλες μεταφορικές εταιρίες. Δίνει την δυνατότητα του ελέγχου του κάθε φορτίου, που σημαίνει πως στέλνει πληροφορίες για την θερμοκρασία, την υγρασία, το φως και την πίεση που δέχεται το κάθε φορτίο. Με αυτά τα δεδομένα οι κατασκευαστές και οι μεταφορικές εταιρείες έχουν την δυνατότητα να γνωρίζουν τι συμβαίνει ανά πάσα στιγμή στο κάθε φορτίο(CargoSense, n.d.).

5. Ψηφιακή Εγκληματολογία στο Διαδίκτυο των Πραγμάτων

5.1 Ορισμός της Ψηφιακής Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων

Η συνεχής ανάπτυξη του IoT συστήνει νέες προκλήσεις στην ασφάλεια. Το γεγονός πως δισεκατομμύρια συσκευές είναι συνδεμένες μεταξύ τους, παράγοντας και ανταλλάσοντας προσωπικές πληροφορίες των χρηστών ή ακόμα και πληροφορίες επιχειρήσεων, το αναδεικνύουν ως ένα αρκετά ελκυστικό στόχο για επιθέσεις. Η ασφάλεια στον κόσμο του IoT δεν είναι τουλάχιστον μέχρι σήμερα όσο επαρκής θα όφειλε. Στην πραγματικότητα έχουν υιοθετηθεί πολλές τεχνικές ασφαλείας που όμως δεν είναι τόσο ικανές ώστε να αποτρέψουν από επιθέσεις που προκαλούνται από λάθη των ίδιων των χρηστών ή από λανθασμένες ρυθμίσεις. Από την άλλη πλευρά, οι εγκληματίες βρίσκονται συχνά είναι ένα βήμα μπροστά από τους ειδικούς της ασφάλειας. Απόρροια όλων αυτών αποτελούν οι παραβιάσεις ασφαλείας που γίνονται στον ψηφιακό κόσμο και στο IoT. Οι ειδικοί πρέπει να είναι θέση να τις επιλύουν.

Σύμφωνα λοιπόν με τα παραπάνω το Διαδίκτυο των Πραγμάτων παρουσιάζει καινούργιες διαστάσεις στην Ψηφιακή Εγκληματολογία, καθώς το περιβάλλον αυτό παρέχει μια τεράστια γκάμα δεδομένων και στοιχείων που, σε συνδυασμό μεταξύ τους, μπορούν να δώσουν πληροφορίες για ένα γεγονός που συνέβη. Αυτές οι διαστάσεις απαιτούν μια διαφορετική προσέγγιση. Η Εγκληματολογία στο Διαδίκτυο των Πραγμάτων (Internet of Things Forensics) είναι μια επιστήμη η οποία σύμφωνα με τους Shams Zawoad και Ragib Hanson (Zawoad & Hasan, 2015) θεωρείται παράρτημα της Ψηφιακής Εγκληματολογίας, όπου η ταυτοποίηση, η συλλογή, η οργάνωση και η παρουσίαση είναι διεργασίες που ασχολούνται με υποδομές του IoT για να εξακριβώσουν τα γεγονότα που συνέβησαν σε μια εγκληματική πράξη.

5.2 Προκλήσεις του IoT στην Ψηφιακή Εγκληματολογία

Όπως έχει προαναφερθεί, τα αποδεικτικά στοιχεία, που ένας ερευνητής μπορεί να αποκτήσει από τις συσκευές του Διαδικτύου των Πραγμάτων, μπορούν να αποτελέσουν έναν ιδιαίτερο σημαντικό παράγοντα κατά την διάρκεια μιας έρευνας έως την ολοκλήρωσή της. Σε περίπτωση που ο ερευνητής δεν χειριστεί σωστά αυτά τα δεδομένα θα βρεθεί σε σημείο να χάσει κάποια από αυτά τα οποία θα είναι σημαντικά ή αντιθέτως μπορεί να συλλέξει στοιχεία που δε θα είναι απαραίτητα για την έρευνα και αυτά ίσως τον παραπλανήσουν και τον οδηγήσουν σε λανθασμένα συμπεράσματα.

Τα εργαλεία και οι τεχνολογίες που χρησιμοποιούνται στην Ψηφιακή Εγκληματολογία δεν είναι σχεδιασμένα για να χειριστούν τις υποδομές του Διαδικτύου των Πραγμάτων (Zawoad &

Hasan, 2015). Για αυτό σε αυτήν την ενότητα θα παρουσιαστούν διάφορες προκλήσεις που συναντάει ένας ερευνητής ώστε να αναγνωρίζει ποιες πληροφορίες είναι σημαντικές να αποκτάει από τον τόπο του εγκλήματος. Τα βήματα του μοντέλου του NIST που παρουσιάστηκε στο δεύτερο κεφάλαιο αντιμετωπίζουν διάφορες προκλήσεις και η ανάλυση που θα ακολουθεί θα γίνει με βάση αυτά.

- **Συλλογή Δεδομένων (Collection).** Μία από τις μεγαλύτερες προκλήσεις είναι ο τεράστιος όγκος πληροφορίας. Η πρόκληση που αντιμετωπίζει ο ερευνητής είναι μέσα από τα πολλά στοιχεία και από τις πολλές συσκευές να συλλέξει αυτά που θα του χρησιμεύσουν για την έρευνά του.

  Οι συσκευές του IoT έχουν μικρό αποθηκευτικό μέγεθος και έτσι χρησιμοποιούν τεχνολογίες νέφους (cloud) για να αποθηκεύσουν τα δεδομένα. Άρα το νέφος είναι μία σημαντική πηγή που πρέπει να έχει υπόψη του ο ερευνητής ώστε να αντλήσει στοιχεία. Ένα σημαντικό πρόβλημα εδώ είναι η δύσκολη πρόσβαση στο νέφος. Στην Ψηφιακή Εγκληματολογία ο ερευνητής έχει πρόσβαση σε πηγές στοιχείων που έχουν όμως φυσική υπόσταση, όπως για παράδειγμα στον σκληρό δίσκο. Στην περίπτωσή μας όμως είναι πολύ πιθανό να μην γνωρίζουμε που βρίσκονται τα δεδομένα, διότι μπορεί να βρίσκονται σε διάφορα σημεία (Zawoad & Hasan, 2015).
- **Εξέταση (Examination).** Επί του παρόντος δεν υπάρχουν συγκεκριμένα πρωτόκολλα για το IoT. Οι κατασκευαστές χρησιμοποιούν πρωτόκολλα που έχουν αναπτύξει οι ίδιοι για την επικοινωνία των αντικειμένων. Η τεράστια ποικιλία των δεδομένων που παράγονται από αυτά τα πρωτόκολλα είναι δύσκολο να εξεταστεί, καθιστώντας την διαδικασία ιδιαίτερα περίπλοκη.
- **Ανάλυση (Analysis).** Η Ανάλυση στην Ψηφιακή Εγκληματολογία εξυπηρετεί τον ερευνητή στο να βρει την προέλευση των αποδεικτικών στοιχείων ώστε να αποδείξει ότι είναι αξιόπιστα. Εντούτοις, στο IoT υπάρχει διαφορά. Η συνεχής αλληλεπίδραση των συσκευών, αλλά και η αλληλεπίδραση με το cloud διευκολύνει την ενσωμάτωση πληροφοριών και δεδομένων. Αποτέλεσμα αυτού είναι όλα τα στοιχεία να συσσωματώνονται στο πλαίσιο του IoT και η διαδικασία της Ανάλυσης να γίνεται πολύ απαιτητική.

  Πέρα από τα παραπάνω η Ανάλυση σχετίζεται και με την ανάλυση των αρχείων καταγραφής (logs) των συσκευών. Όμως η δομή αυτών των αρχείων σε κάθε συσκευή διαφέρει, αφού δεν υπάρχει μια πρότυπη μορφή. Ο ερευνητής θα μπορούσε να συσχετίζει τα logs που έχει συλλέξει και μετά από την ανάλυσή τους να καταλήξει σε χρήσιμες πληροφορίες.

- **Αναφορά (Reporting).**Κατά την Αναφορά ο ερευνητής παρουσιάζει τα αποδεικτικά στοιχεία της έρευνάς του. Ωστόσο, ακόμα και αυτή η διαδικασία στην Εγκληματολογία στο IoT παρουσιάζει προκλήσεις. Τα δεδομένα πολλές φορές, όπως έχει προαναφερθεί, υπάρχει η πιθανότητα να έχουν συσσωματωθεί στο Διαδίκτυο των Πραγμάτων μεταξύ τους αλλά και με άλλα δεδομένα και αυτό τους αλλάζει της δομή και την σημασία. Από εγκληματολογικής σκοπιάς το πρόβλημα είναι πως οι συσκευές μπορεί να έχουν υιοθετήσει διαφορετικό τρόπο περιγραφής ή κάθε συσκευή να έχει τον δικό της. Στην διαδικασία της αναφοράς ο αντικρουόμενος τρόπος περιγραφής των δεδομένων μπορεί να αποδειχθεί αποπροσανατολιστικός (Hegarty, 2014).

5.3 Διαφορές Ψηφιακής Εγκληματολογίας και Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων

Στο Διαδίκτυο των Πραγμάτων οι συσκευές, ανάλογα με τις πληροφορίες που λαμβάνουν και επεξεργάζονται, είναι σε θέση να λαμβάνουν αποφάσεις για την επόμενη κίνησή τους. Κατά συνέπεια η τεχνολογία του IoT εισάγει νέες διαστάσεις, όπου οφείλει πλέον να προσέχει ο ερευνητής και να τις συμπεριλάβει στις συνηθισμένες πρακτικές του. Η Εγκληματολογία στο Διαδίκτυο των Πραγμάτων αντιμετωπίζει πολλές διαφορές σε σχέση με την κλασσική Ψηφιακή Εγκληματολογία και αυτές αναδεικνύονται σε αυτήν την ενότητα σύμφωνα με τους Oriwoh et al.(Oriwoh, Jazani, Epiphaniou, & Sant, 2013):

- **Πηγές αποδεικτικών στοιχείων**. Οι πηγές που μπορεί να βρει αποδεικτικά στοιχεία ένας ερευνητής είναι (όπως αναμένει κανείς εκτός όλων των άλλων) και διάφορες ηλεκτρονικές συσκευές. Αυτές οι συσκευές, όπως έχει προαναφερθεί σε προηγούμενο κεφαλαίο, είναι ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα, κτλ. Πλέον, σε αυτές τις συσκευές λόγω του IoT προστίθενται και διάφορες άλλες, όπως οι έξυπνες οικιακές συσκευές, έξυπνες λάμπες, έξυπνες κλειδαριές, από όπου θα μπορεί ο ερευνητής να αποκτήσει χρήσιμες πληροφορίες. Η διαφορετικότητα και η ανομοιογένεια μεταξύ όλων αυτών των συσκευών διαμορφώνουν το έργο του ερευνητή κάνοντάς το ακόμα πιο περίπλοκο.
- **Αριθμός των συσκευών.** Όλες αυτές οι συσκευές στο IoT είναι συνδεδεμένες μεταξύ τους, ανταλλάσσουν πληροφορίες και κάθε φορά πολλαπλασιάζονται. Άρα, ο αριθμός των συσκευών που θα πρέπει να ερευνηθεί, μεγαλώνει. Στην παραδοσιακή Ψηφιακή Εγκληματολογία ισχύει κάτι πολύ διαφορετικό: οι συσκευές που οφείλει να εξετάσει ένας ερευνητής είναι αρχικά ένας ηλεκτρονικός υπολογιστής και οποιαδήποτε άλλη συσκευή συνδεδεμένη με αυτόν. Τέτοιες συσκευές μπορεί να είναι εξωτερικός σκληρός δίσκος, μέσα αποθήκευσης USB, tablets, κλπ.

- **Ποσότητα και τύπος των δεδομένων**. Εφόσον οι πηγές των πιθανόν αποδεικτικών στοιχείων και ο αριθμός των συσκευών αυξάνεται, η ποσότητα και οι τύποι των αρχείων ποικίλουν. Οι Coetzee και Olivrin (Coetzee, 2012) προβλέπουν έναν κατακλυσμό από δεδομένα στον κόσμο του IoT. Η αύξηση της ποσότητας των δεδομένων από το 2005 μέχρι το 2020 θα είναι 40000 exabytes (όπου ένα Exabyte αντιστοιχεί σε 1 τρισεκατομμύριο gigabytes). Οι συσκευές του IoT είναι πάρα πολλές. Εκτός αυτού προστίθενται καινούργιες και οι πληροφορίες που μεταδίδουν συμβάλλουν στην αύξηση της ποσότητας επί καθημερινής βάσης. Οι επιπτώσεις στην διεξαγωγή μιας έρευνας είναι ο χρόνος που χρειάζεται για να εξεταστούν όλες αυτά τα στοιχεία. Επίσης, ο τύπος των αρχείων που ανακτάται από τις συσκευές που θεωρούνται πως ανήκουν στο IoT, είναι διαφορετικός από τους τύπους αρχείων που τυπικά αντιμετώπιζε ένας ερευνητής στην Ψηφιακή Εγκληματολογία. Σύμφωνα με αυτήν την συνθήκη προστίθεται και άλλος χρόνος ως το τελικό αποτέλεσμα της έρευνας, επειδή αυτοί οι τύποι αρχείων καλό είναι να μετατραπούν σε κατανοητό και εύχρηστο τύπο για καλύτερα αποτελέσματα.
- **Η τοποθεσία των αποδεικτικών στοιχείων.** Η αποθήκευση των δεδομένων του χρήστη σε πολλαπλές τοποθεσίες, στις οποίες θα έχει πιθανότατα και διαφορετικές δικαιοδοσίες είναι ένα ήδη γνωστό πρόβλημα στην κλασσική Ψηφιακή Εγκληματολογία. Λόγω των διαφορετικών τοποθεσιών όπου είναι αποθηκευμένα τα στοιχεία, καθώς και της διαφορετικής νομοθεσίας που διέπει την κάθε τοποθεσία, ο ερευνητής μπορεί να συναντήσει κωλύματα κατά την διεξαγωγή μιας έρευνας. Το πρόβλημα αυτό κληρονομείται και στην Εγκληματολογία στο Διαδίκτυο των Πραγμάτων, σύμφωνα με το οποίο πολλές συσκευές αποθηκεύουν στο cloud τις διάφορες πληροφορίες που παράγουν ή δέχονται. Αφ' ετέρου, υπάρχει αυξημένη νομική πολυπλοκότητα καθώς οι πληροφορίες ταξιδεύουν στα διάφορα δίκτυα και συναντούν πολλά εμπόδια. Μία ακόμα διάσταση που θα έπρεπε να υπολογιστεί είναι σε τι δίκτυο χρησιμοποιούνται οι συσκευές: αν δηλαδή είναι δημόσιο ή ιδιωτικό.
- **Μη ξεκάθαρα όρια μεταξύ των δικτύων.** Στην Ψηφιακή Εγκληματολογία τα όρια είναι συνήθως ξεκάθαρα σχετικά με τον αριθμό των συσκευών που θα κατασχέσει ο ερευνητής, πόσοι άνθρωποι εμπλέκονται στις επικοινωνίες, κτλ. Ωστόσο, στο IoT τα δίκτυα επηρεάζονται μεταξύ τους, όταν το Body Area Network κινείται ανάμεσα στο Wide Area Network, καθώς ένας χρήστης ταξιδεύει από την οικία του προς τον χώρο εργασίας του ή οπουδήποτε αλλού. Επακόλουθο είναι ο ερευνητής να αντιμετωπίζει δυσκολία εύρεσης εκείνων των στοιχείων που τον ενδιαφέρουν από μια συσκευή, καθότι αυτή έχει ταξιδέψει σε πολλά δίκτυα και έχει αφήσει τα ίχνη της σε όλα.

Σύγκριση Ψηφιακής Εγκληματολογίας και Ψηφιακής Εγκληματολογίας στο IoT		
	Ψηφιακή Εγκληματολογία	**Ψ.Ε στο IoT**
Πηγές αποδεικτικών στοιχείων	Υπολογιστές, σκληροί δίσκοι, έξυπνα κινητά τηλέφωνα, δίκτυα internet, εξυπηρετητές (servers),κοινωνικά δίκτυα	Έξυπνα σπίτια, έξυπνα αυτοκίνητα, έξυπνες συσκευές, RFID, ιατρικές συσκευές, αισθητήρες
Δικαιοδοσία	Ιδιώτες, εταιρείες, κυβέρνηση, κοινωνικά δίκτυα	
Αριθμός των συσκευών	Δισεκατομμύρια συσκευές	50 δισεκατομμύρια συσκευές έως το 2020
Τύπος αποδεικτικών στοιχείων	Ηλεκτρονικά στοιχεία, πρότυποι τύποι αρχεία π.χ. jpeg, mp3 κτλ	Οποιαδήποτε και όλες οι μορφές είναι πιθανές να εμφανίζονται.
Τύποι δικτύων	Συνδεδεμένα με το Διαδίκτυο μέσω καλωδίου, μέσα Wi-Fi, Bluetooth, δίκτυα κινητής τηλεφωνία	RFID, δίκτυα αισθητήρων, κτλ.
Ποσότητα και είδος των δεδομένων και των αποδεικτικών στοιχείων	Μέχρι και terabytes στοιχείων	Μέχρι και exabytes στοιχείων
Πρωτόκολλα	Ethernet, ασύρματο (802.11 a, b, g, n), bluetooth, IPv4 καιIPv6	RFID
Κατάσχεση	Κατάσχεση των συσκευών που χρειάζονται για την έρευνα	Εξακρίβωση των συσκευών που θα βοηθήσουν για εύρεση στοιχείων
Ιδιοκτησία	Ιδιώτες, εταιρείες, κυβέρνηση, κτλ.	
Όριο του δικτύου	Σχετικά ξεκάθαρα ορισμένα όρια και ιδιοκτησία	Αυξανόμενα μη ξεκάθαρα όρια

Πίνακας 2: Διαφορές Ψ.Ε. και Εγκληματολογίας στο IoT

5.4 Μοντέλα Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων

Στο τρίτο κεφάλαιο της συγκεκριμένης διπλωματικής μελετήθηκαν τα μοντέλα που έχει στην διάθεσή του ένας ερευνητής στην Ψηφιακή Εγκληματολογία. Αν και τα μοντέλα είναι πολλά, δεν βρίσκουν εύκολα εφαρμογή στο περιβάλλον του Διαδικτύου των Πραγμάτων. Αυτό συμβαίνει, αφού τα εργαλεία και οι διεργασίες της Ψηφιακής Εγκληματολογίας δεν είναι σε θέση να αντιμετωπίσουν την ανομοιογένεια που επικρατεί στο Διαδίκτυο των Πραγμάτων. Η αιτία έγκειται στο γεγονός, πως τα μοντέλα σχεδιάστηκαν για την Ψηφιακή Εγκληματολογία. Στην ενότητα αυτή θα αναδειχθούν τρία μοντέλα Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων που υπάρχουν στην βιβλιογραφία.

5.4.1 Digital Forensic Investigation Framework for Internet of Things (DFIF-IoT)

Το συγκεκριμένο μοντέλο έχει προταθεί από τους Victor Kebande και Indrakshi Ray (Kebande & Ray, 2016) και χωρίζεται σε τρεις διαφορετικές ενότητες οι οποίες αποτελούνται από την προληπτική διαδικασία (proactive process), Εγκληματολογία στο Διαδίκτυο των Πραγμάτων (IoT Forensics) και την διαδικασία αντίδρασης (reactive process). Στην εικόνα 7 όπου μπορούμε να παρατηρήσουμε το μοντέλο, φαίνονται οι τρεις ενότητες και είναι αριθμημένες από το 1 ως το 3.

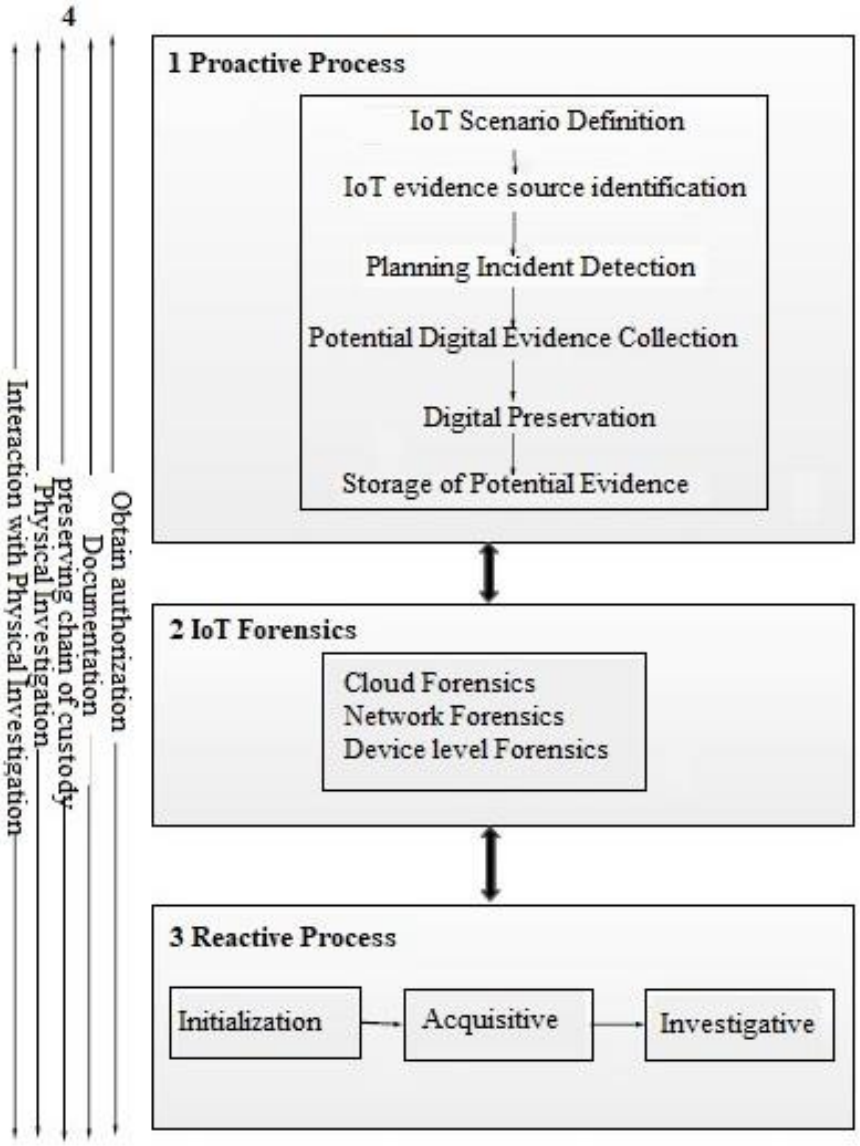
1)*Προληπτική διαδικασία (Proactive Process)*

Η προληπτική διαδικασία είναι αυτή που συμβαίνει πριν από ένα περιστατικό. Σε αυτό το σημείο εμπλέκεται ο σχεδιασμός και η προετοιμασία πριν από περιστατικά ασφάλειας που πιθανόν να προκύψουν σε συσκευές του IoT. Διαφορετικά, αυτό εμφανίζεται και ως Digital Forensics Readiness (DFR). Η διαδικασία αυτή αποτελείται από έξι δραστηριότητες: τον ορισμό του σεναρίου στο IoT (IoT scenario Definition), την αναγνώριση πηγών αποδεικτικών στοιχείων στο IoT (IoT evidence source identification), τον σχεδιασμό ανίχνευσης περιστατικών (Planning Incident Detection), την συλλογή πιθανών αποδεικτικών στοιχείων (Potential digital evidence collection), την διατήρηση των ψηφιακών στοιχείων (Digital Preservation) και την αποθήκευση πιθανών αποδεικτικών στοιχείων (Storage of Potential Evidence). Παρακάτω θα αναλυθούν οι επιμέρους δραστηριότητες:

- Ορισμός σεναρίου (IoT scenario Definition): Πιθανά σενάρια προβλημάτων ασφάλειας στο IoT, μέσω του οποίου μπορεί ένας ερευνητής να αναγνωρίσει ψηφιακά αποδεικτικά στοιχεία. Μέσω της δραστηριότητας αυτής μπορούν να υπολογιστούν οι κίνδυνοι και το κόστος σύμφωνα με το οποίο θα επιτευχθεί η ετοιμότητα ενός οργανισμού για τέτοια συμβάντα.
- Αναγνώριση πηγών αποδεικτικών στοιχείων (IoT evidence source identification): Οι πηγές αποδεικτικών στοιχείων αντιπροσωπεύουν πιθανές σκηνές εγκλήματος που βασίζονται στο

IoT. Οι πηγές αυτές μπορούν να είναι οικιακές συσκευές, υπολογιστές, ιατρικές συσκευές, κ.α.

- Σχεδιασμός ανίχνευσης περιστατικών (Planning Incident Detection): Ο σχεδιασμός της ανίχνευσης περιστατικών περιλαμβάνει τις δραστηριότητες οι οποίες καθορίζουν πώς ένα περιβάλλον IoT που έχει δεδομένα ενδέχεται να περιέχει πιθανά περιστατικά ασφαλείας. Ωστόσο, ένας ορισμός από ενέργειες, που είναι πιθανόν να συμβούν όταν εντοπίζονται περιστατικά, αποτυπώνεται σε αυτήν την δραστηριότητα.



Εικόνα 7: Μοντέλο DFIF-IoT

- Συλλογή πιθανών αποδεικτικών στοιχείων (Potential digital evidence collection): Στη φάση αυτή εμπλέκεται η συγκέντρωση και η διατήρηση διαφορετικών τύπων δεδομένων βάσει των κινδύνων που αξιολογούνται από ένα δεδομένο IoT περιβάλλον.

- Διατήρηση ψηφιακών στοιχείων (Digital Preservation): Μόλις συλλεχθούν τα δεδομένα, θα πρέπει να διατηρηθούν στην αρχική τους μορφή προτού οι ερευνητές ξεκινήσουν την διαδικασία της ανάλυσης.
- Αποθήκευση πιθανών αποδεικτικών στοιχείων (Storage of Potential Evidence): Σε περίπτωση που δεν γίνει επί τόπου ανάλυση ενός στοιχείου, τότε αυτό καλό είναι να αποθηκευτεί για μελλοντική ανάλυση.

2)*Εγκληματολογία στο Διαδίκτυο των Πραγμάτων (IoT Forensics)*

Η ενότητα αυτή παρέχει διαφορετικές πτυχές και υποδομές του IoT οι οποίες μπορούν να εξεταστούν χρησιμοποιώντας μεθόδους από την Ψηφιακή Εγκληματολογία. Οι μέθοδοι αυτοί είναι τρεις:

- Εγκληματολογία 'νέφους' (Cloud Forensics): Οι περισσότερες συσκευές του IoT έχουν σχεδιαστεί για να αλληλεπιδρούν στο δίκτυο μέσω εφαρμογών και πληροφοριών που μοιράζονται σε εικονικό περιβάλλον.
- Εγκληματολογία δικτύων (Network Forensics): Η Εγκληματολογία δικτύων περιστρέφεται γύρω από το IoT και στα διαφορετικά δίκτυα. Από αυτό το σύνολο ο ερευνητής μπορεί μέσα από τα logs που θα αποκτήσει να τα χρησιμοποιήσει για να διεξαγάγει έρευνα και να βγάλει συμπεράσματα.
- Εγκληματολογία σε συσκευές (Device Level Forensics): Σε αυτό το στάδιο εμπλέκεται η συλλογή στοιχείων προς εξέταση από συσκευές του IoT. Αυτά τα δεδομένα μπορούν να συλλεχθούν από μνήμες, σκληρούς δίσκους, Near Field Communication (NFC), κ.α.

3) *Διαδικασία αντίδρασης (Reactive Process)*

Η διαδικασία αντίδρασης συμβαίνει μετά από ένα περιστατικό το οποίο έλαβε χώρα σε περιβάλλον του Διαδικτύου των Πραγμάτων. Αποτελείται από τις παρακάτω οντότητες:

Αρχικοποίηση (Initialization): Συνίσταται από δραστηριότητες που ξεκινούν μια ψηφιακή έρευνα σε συνέχεια ενός περιστατικού που πραγματοποιήθηκε στο IoT. Το πρότυπο ISO/IEC 27043 υπογραμμίζει τις παρακάτω αρχικές διαδικασίες μετά από ένα περιστατικό: ανίχνευση περιστατικών, πρώτη αντίδραση, σχεδιασμός και προετοιμασία για την έρευνα.

Διαδικασία απόκτησης (Acquisitive process): Διαδικασία που είναι επιφορτισμένη με δραστηριότητες για απόκτηση αποδεικτικών στοιχείων από συσκευές του IoT. Η αναγνώριση, συλλογή, μεταφορά και αποθήκευση είναι διεργασίες που γίνονται σε αυτό το στάδιο.

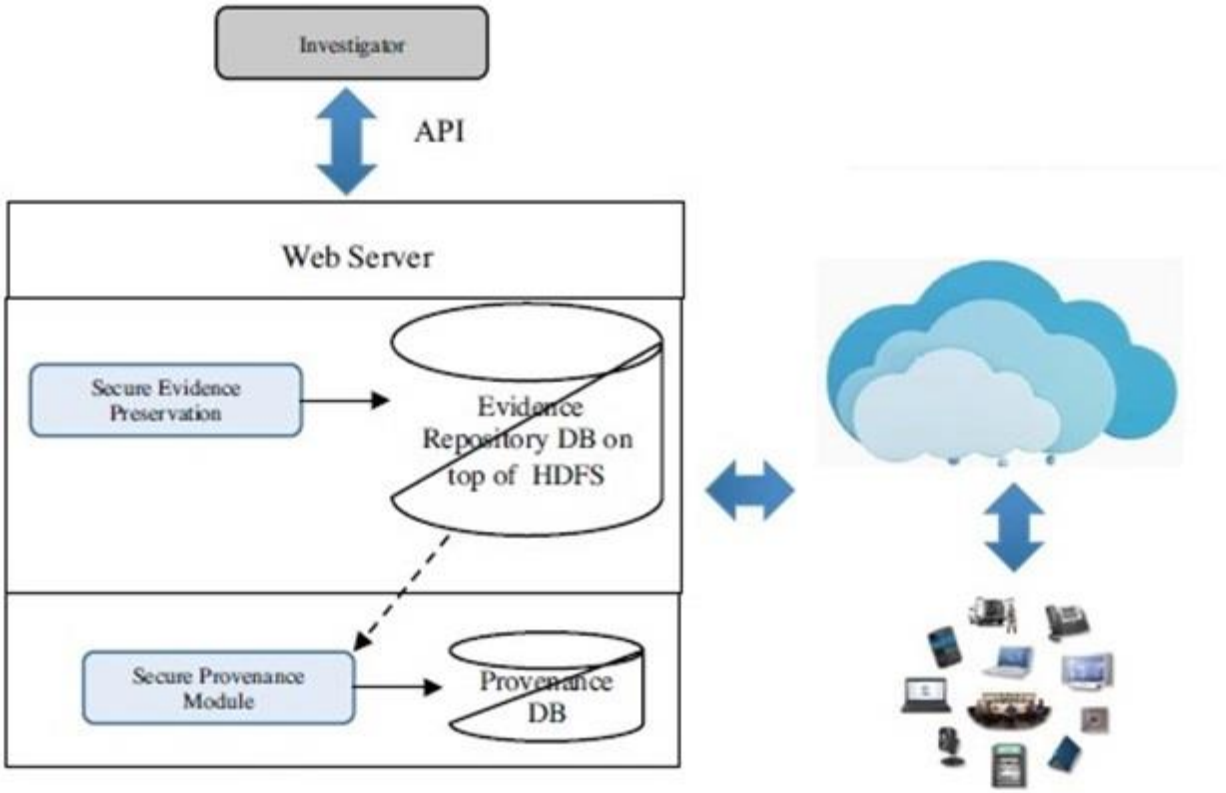
Έρευνα (Investigative): Εδώ οι ενέργειες που γίνονται ασχολούνται με την έρευνα περιστατικών στο IoT. Η ανάλυση των στοιχείων που περιλαμβάνουν περιστατικά γίνονται μαζί με την ερμηνεία και την αναφορά αυτών.

4) *Ταυτόχρονες διαδικασίες (Concurrent Processes)*

Οι ταυτόχρονες διαδικασίες λαμβάνουν χώρα σε κάθε έρευνα και συνδράμουν σε μια αποτελεσματική έρευνα. Η απόκτηση εξουσιοδότησης (Obtain Authorization) είναι η διαδικασία που αφορά την απόκτηση νόμιμης εντολής για εκτέλεση ψηφιακής έρευνας, ενώ για την επαναληψιμότητα των διαδικασιών θα πρέπει να καταγράφονται (Documentation). Η ακολουθία γεγονότων (Chain of Custody) διατηρείται για να καταδείξει την πορεία των ενεργειών που διεξήχθησαν καθ' όλη την διάρκεια της έρευνας. Η διαδικασία της φυσικής έρευνας (Physical Investigation) παρέχει ένα σύνδεσμο μεταξύ των διεργασιών που χρησιμοποιήθηκαν για να ερευνηθεί το συμβάν και της ίδιας της φυσικής έρευνας.

5.4.2 Forensics-Aware Internet of Things Model (FAIoT Model)

Οι Zawoad και Hasan (Zawoad & Hasan, 2015) πρότειναν ένα μοντέλο το οποίο θα διευκολύνει την συλλογή αποδείξεων και την ανάλυσή τους. Στο μοντέλο αυτό θα χρησιμοποιείται ένα έμπιστο αποθετήριο αποδείξεων. Είναι μια καινούργια υπηρεσία στην οποία θα καταχωρούν οι ιδιοκτήτες τις συσκευές και εκεί θα καταγράφονται χρήσιμες πληροφορίες όπως θα δούμε και παρακάτω. Στην εικόνα 8 φαίνεται το μοντέλο που αποτελείται από 3 τμήματα.



Εικόνα 8: Μοντέλο FAIoT

Secure Evidence Preservation Model (Ασφαλή Διατήρηση Αποδείξεων): Στο τμήμα αυτό θα παρακολουθούνται συνεχώς όλες οι εγγραμμένες συσκευές και θα αποθηκεύονται οι αποδείξεις στο αποθετήριο. Οι αποδείξεις μπορεί να είναι αρχεία καταγραφής (logs) του δικτύου, στοιχεία από τους αισθητήρες, κτλ. Όσο θα διατηρεί αυτά τα δεδομένα, το μοντέλο έχει την ικανότητα να φροντίζει για τον διαχωρισμό των στοιχείων βάση του ιδιοκτήτη και της συσκευής. Κατά αυτόν τον τρόπο δε θα συγχέονται οι πληροφορίες των χρηστών. Επίσης, με την χρήση κρυπτογραφημένου κλειδιού διατηρείται η εμπιστευτικότητα των στοιχείων και μόνο οι ερευνητές θα έχουν το δικαίωμα να τα δουν.

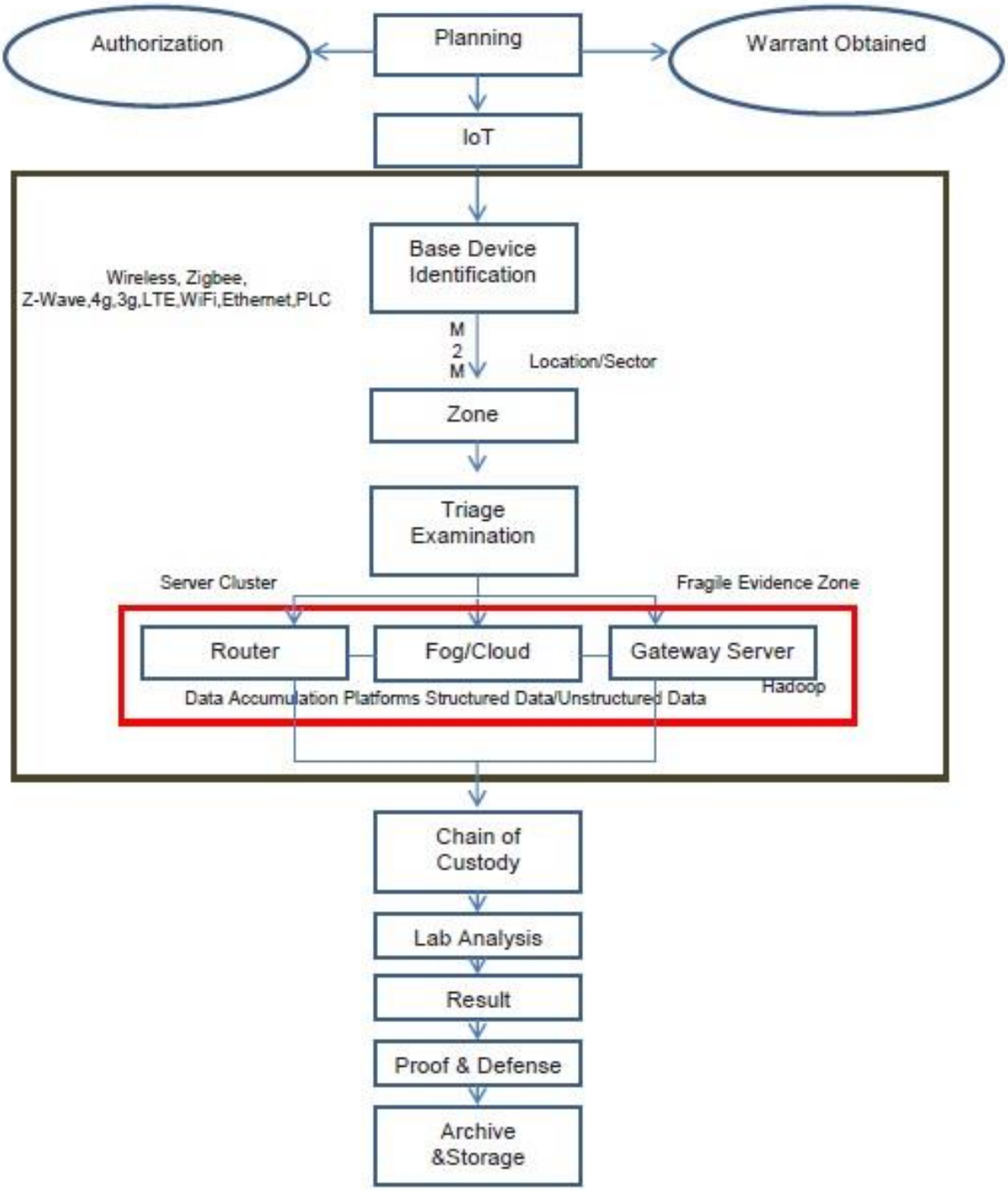
Οι ερευνητές, επειδή το αποθετήριο θα πρέπει να διαχειριστεί πολλές πληροφορίες, προτείνουν την χρήση του Hadoop Distributed File System (HDFS). Το HDFS είναι ένα σύστημα αρχείων που σχεδιάστηκε για να αποθηκεύει με ταχύτητα πολύ μεγάλα δεδομένα και η μετάδοση αυτών να γίνεται στον χρήστη επίσης γρήγορα. Επομένως, το HDFS(APACHE hadoop) θα έχει καλύτερη απόδοση από μια βάση δεδομένων όταν ο ερευνητής θα θέλει να ανακτήσει μια μικρή πληροφορία από ένα μεγάλο σύνολο αποδείξεων.

Secure Provenance Module (Ασφαλή Προέλευση): Στο τμήμα αυτό το μοντέλο FAIoTεξασφαλίζει την σωστή ακολουθία των γεγονότων διαφυλάττοντας την πρόσβαση στο ιστορικό των αποδείξεων. Χρησιμοποιώντας το σύστημα καταγραφής της προέλευσης (provenance aware file system (PASS, n.d.)) που πρότειναν οι Muniswamy-Reddy et al. (Muniswamy-Reddy, 2006) μπορεί η αποθήκη στοιχείων να παράγει το ιστορικό προέλευσης για τη χρήση των αποδεικτικών στοιχείων. Το αποθετήριο των αποδείξεων θα μπορεί να παράγει το αρχείο των προελεύσεων για την χρήση των αποδείξεων. Ωστόσο, αν και όλες οι αποδείξεις και τα ιστορικά πρόσβασης είναι υπό τον έλεγχο του παρόχου του αποθετηρίου, μπορούν να αλλοιωθούν από το αρχείο προελεύσεων. Επιπλέον, από τις πληροφορίες προέλευσης στο cloud, ένας επιτιθέμενος μπορεί να μάθει έμπιστες πληροφορίες για τα δεδομένα που είναι αποθηκευμένα. Για την προστασία αυτών των πληροφοριών από επιθέσεις απαιτείται ένα ασφαλές σχέδιο προελεύσεων.

Access to Evidence Through API (Πρόσβαση στις Αποδείξεις μέσω API): Σε αυτό το σημείο οι ερευνητές προτείνουν ένα ασφαλές API με δικαιώματα ανάγνωσης μόνο στις υπηρεσίες. Οι μόνοι που θα έχουν πρόσβαση σε αυτό θα είναι το δικαστήριο και οι ερευνητές. Το APIτους δίνει την δυνατότητα να συλλέγουν αποδείξεις και στοιχεία. Για την εφαρμογή αυτής της λειτουργίας χρειάζεται η χρήση ενός εξυπηρετητή, ο οποίος θα επικοινωνεί με τα προηγούμενα τμήματα.

5.4.3 IoT Based Digital Forensic Model

Το τρίτο και τελευταίο μοντέλο, είναι αποτέλεσμα της έρευνας των Perumal et al. (Perumal, Norwawi, & Raman, 2015). Πρόκειται για ένα μοντέλο που περιέχει τις διεργασίες της εξουσιοδότησης (authorization), του σχεδιασμού (planning), της ακολουθίας των γεγονότων (chain of custody), της ανάλυσης (analysis) και της αποθήκευσης (storage), όπως φαίνεται και στην παρακάτω εικόνα.



Εικόνα 9: IoT Digital Forensics Investigation Model

Παρατηρώντας το συγκεκριμένο μοντέλο η επικοινωνία μηχανής με μηχανής (machine to machine communication) είναι η βάση αναγνώρισης των συσκευών. Οι συσκευές του IoT, όπως έχει ειπωθεί πολλές φορές, επικοινωνούν μεταξύ τους ανταλλάσσοντας πληροφορίες, ενώ επίσης αποθηκεύουν δεδομένα. Η επικοινωνία αυτή διαχωρίζεται από την γεωγραφική θέση της συσκευής ανάλογα με τις ρυθμίσεις. Αυτή η επικοινωνία μεταξύ των συσκευών γίνεται είτε μέσω Z-Wave, 4G, 3G, LTE, Wi-Fi, Ethernet, Power Line Communication (PLC).

Όταν ο ερευνητής θα εντοπίσει την ύποπτη συσκευή με κάποια άλλη συσκευή του IoT, τότε θα μπορεί να διεξάγει την έρευνα του, στην οποία οφείλει να είναι ιδιαίτερα προσεκτικός αφού τα στοιχεία στο περιβάλλον του Διαδικτύου των Πραγμάτων (όπως έχει αναφερθεί παραπάνω) είναι ευαίσθητα. Καθώς γίνεται η εξέταση, ο ερευνητής θα βρεθεί αντιμέτωπος με πολλά στοιχεία και πολλά δεδομένα κάποια από τα οποία θα έχουν μια συγκεκριμένη δομή και κάποια άλλα όχι. Τα μέσα που είναι πιο κοινά προς εξέταση είναι router, gateway, cloud,κτλ.

Μετά την απόκτηση των απαραίτητων δεδομένων και την κατάσχεση συγκεκριμένων συσκευών, η διαδικασία αποκτά μια μορφή που είναι πιο κοντά στην Ψηφιακή Εγκληματολογία και περιέχει τις διαδικασίες της ακολουθίας των γεγονότων, της εργαστηριακής ανάλυσης, του αποτελέσματος, των αποδείξεων και της αποθήκευσης.

6. Προσομοιώσεις σεναρίων Ψηφιακής Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων με τον προσομοιωτή CupCarbon.

6.1 Προσομοιωτής CupCarbon

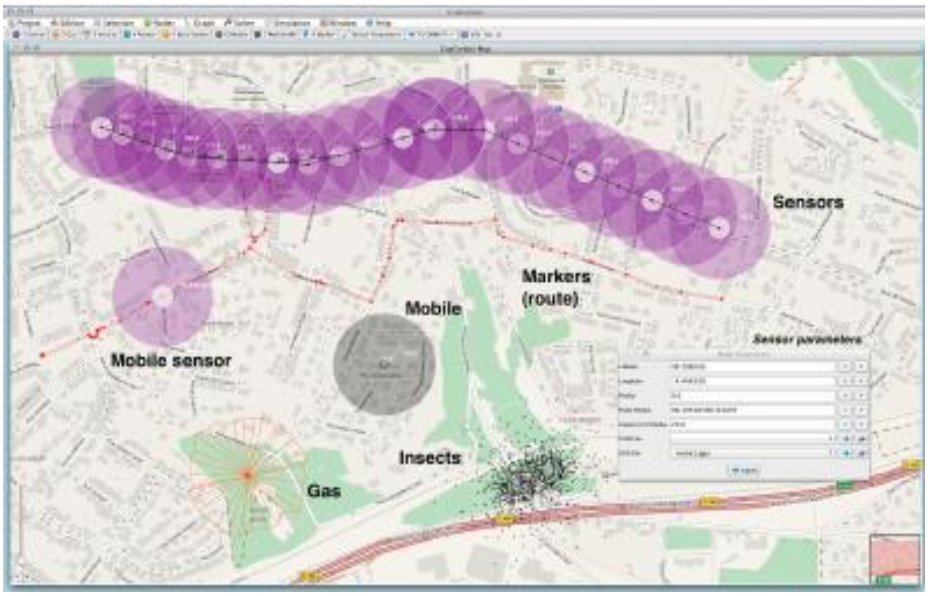
Στα προηγούμενα κεφάλαια εξετάσαμε το Διαδίκτυο των Πραγμάτων και όλες τις εξελίξεις που έχουν ήδη γίνει ή πρόκειται να γίνουν στην καθημερινότητά μας. Αυτές οι εξελίξεις θα συμβάλλουν στην ενίσχυση της ποιότητας των αστικών υπηρεσιών, στην μείωση του κόστους (στις μετακινήσεις, στα καύσιμα, στην ενέργεια, στις επικοινωνίες κτλ). Έχοντας αυτό ως δεδομένο, απαιτούνται νέα εργαλεία προσομοίωσης τα οποία θα προετοιμάσουν το έδαφος για την ανάπτυξη μεγάλων υποδομών IoTστις έξυπνες πόλεις, υπό τις καλύτερες δυνατές συνθήκες όσον αφορά την αξιοπιστία, την κατανάλωση ενέργειας και το κόστος.

Ένα τέτοιο εργαλείο προσομοίωσης λογίζεται το CupCarbon. Πρόκειται για μια πλατφόρμα στην οποία μπορεί ο χρήστης να σχεδιάσει μια έξυπνη πόλη και Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks) στο Διαδίκτυο των Πραγμάτων. Ο χρήστης μπορεί να σχεδιάσει, να απεικονίσει, να αποσφαλματώσει (debug) ή να επικυρώσει αλγορίθμους για παρακολούθηση περιβαλλοντολογικών δεδομένων σε ένα Ασύρματο Δίκτυο Αισθητήρων. Επίσης, δίνεται η δυνατότητα για δημιουργία σεναρίων που μπορεί να περιλαμβάνουν φωτιά ή κινητό τηλέφωνο και όλα αυτά στο πλαίσιο εκπαιδευτικών ή επιστημονικών προγραμμάτων.

Το CupCarbon προσφέρει δύο διαφορετικούς τρόπους προσομοίωσης. Ο πρώτος αφορά ένα περιβάλλον στο οποίο παρέχεται στον χρήστη η δυνατότητα σχεδιασμού σεναρίων που περιλαμβάνουν μια συλλογή γεγονότων, όπως φωτιά, καθώς επίσης και προσομοιώσεις με κινητές συσκευές, όπως οχήματα και αντικείμενα με δυνατότητα πτήσης. Το δεύτερο περιβάλλον αντιπροσωπεύει μια διακριτή προσομοίωση συμβάντων του Ασύρματου Δικτύου Αισθητήρων η οποία λαμβάνει υπόψη το σενάριο που δημιουργήθηκε στο πρώτο περιβάλλον.

Τα σενάρια και τα δίκτυα σχεδιάζονται και κατασκευάζονται σε ένα εργονομικό και εύκολο στη χρήση γραφικό περιβάλλον το οποίο χρησιμοποιεί το OpenStreetMap (OSM)[3] (όπως φαίνεται στην εικόνα 10) και επιτρέπει την εγκατάσταση αισθητήρων απευθείας στον χάρτη. Ακόμα, είναι κατασκευασμένο με Java, διανέμεται δωρεάν και είναι λογισμικού ανοικτού κώδικα. Ο χρήστης χρησιμοποιεί την γλώσσα σεναρίων SenScript ώστε να προγραμματίσει τους αισθητήρες του προσομοιωτή. Πέρα από τους αισθητήρες, με την SenScript είναι δυνατόν να παραχθεί κώδικας για Arduino.

[3]Το OpenStreetMap (www.openstreetmap.org) είναι παγκόσμιος χάρτης που μπορεί να χρησιμοποιηθεί ελεύθερα από τους χρήστες.



Εικόνα 10: Το γραφικό περιβάλλον του CupCarbon

6.2 Προσομοιώσεις

Σε αυτό το σημείο θα δημιουργηθεί ένα σενάριο επίθεσης σε ένα απλό δίκτυο που περιλαμβάνει αντικείμενα από το Διαδίκτυο των Πραγμάτων και θα επιχειρηθεί η συλλογή ψηφιακών αποδεικτικών στοιχείων τα οποία θα αποκομίζονται από τα ίδια τα αντικείμενα.

6.2.1 Περιγραφή Πρώτη Προσομοίωσης

Η προσομοίωση περιλαμβάνει ένα δίκτυο στο οποίο διαμοιράζονται δεδομένα μεταξύ δύο αντικειμένων του Διαδικτύου των Πραγμάτων και ένα τρίτο αντικείμενο το οποίο κινείται. Πιο συγκεκριμένα το δίκτυο αποτελείται από τα στοιχεία που εμφανίζονται στον Πίνακα 3.

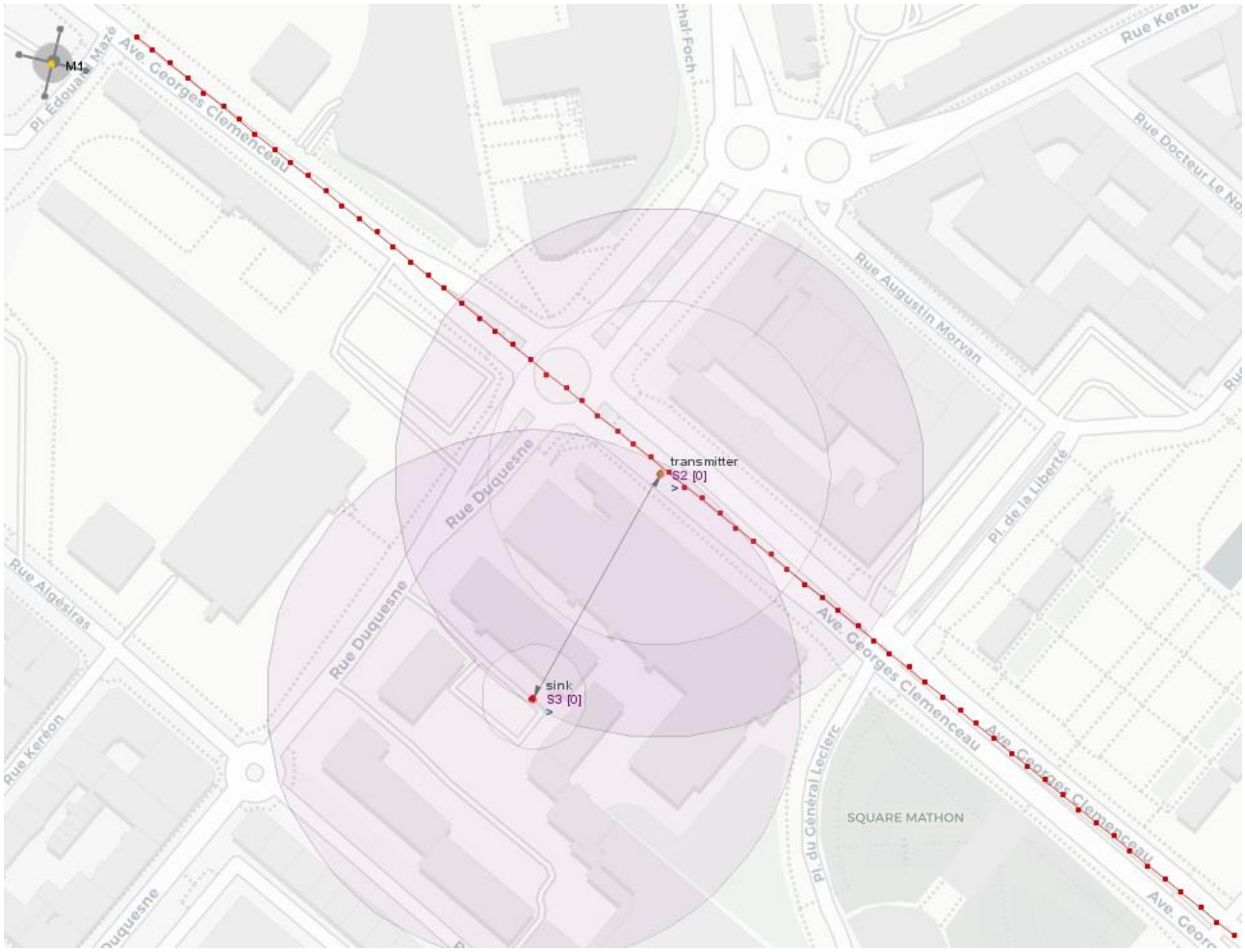
id Συσκευής	Όνομα Συσκευής	Περιγραφή
M1	M1	Έξυπνο Κινητό Τηλέφωνο
S2	transmitter	Έξυπνη Κλειδαριά
S3	sink	Έξυπνο Κινητό Τηλέφωνο

Πίνακας 3:Περιγραφή Συσκευών Πρώτης Προσομοίωσης

1. Μια κινητή συσκευή με όνομα M1 η οποία είναι ένα κινητό τηλέφωνο.
2. Τα κόκκινα markerpoints που χρησιμοποιούνται για να υποδηλώσουν το εναρκτήριο και το τελικό σημείο που θα πρέπει να διασχίσει η κινητή συσκευή.
3. Δύο αντικείμενα που ονομάστηκαν S2 και S3. Είναι τα δύο σημαντικότερα στοιχεία του δικτύου και διαμοιράζονται πληροφορίες πριν την άφιξη της κινητής συσκευήςM1. Ο

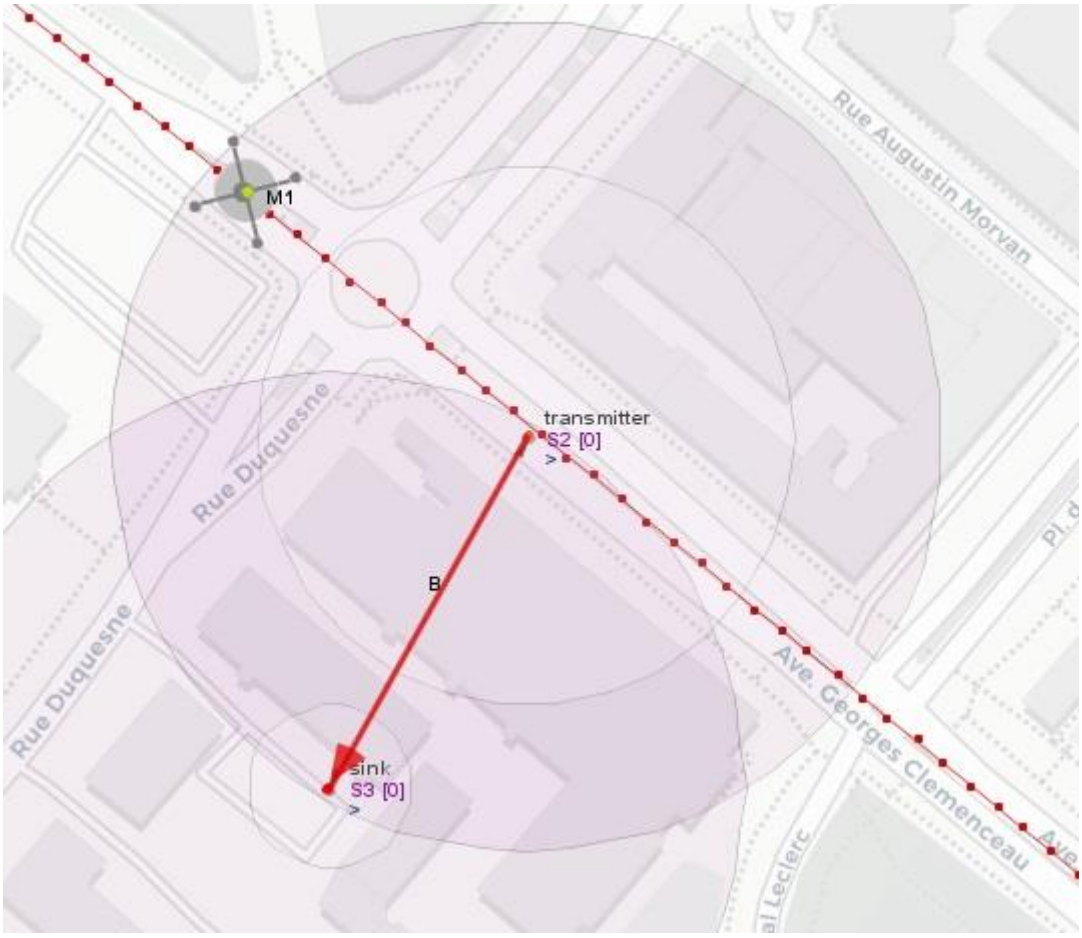
αισθητήρας S2 (που είναι ο αναμεταδότης) είναι μία έξυπνη κλειδαριά στην κεντρική πόρτα μιας οικίας. Το αντικείμενο S3 είναι ένα έξυπνο κινητό τηλέφωνο. Η κλειδαριά έχει τη δυνατότητα σύνδεσης με το διαδίκτυο για να προσφέρει στον χρήστη πλήρη απομακρυσμένο έλεγχο μέσω της αντίστοιχης εφαρμογής του κινητού. Χρησιμοποιώντας Bluetooth, η πόρτα ανοίγει αφού ο χρήστης κάνει την αντίστοιχη επιλογή στην εφαρμογή που έχει στο κινητό του. Η κλειδαριά κλείνει όταν ο χρήστης φεύγει από το σπίτι με τη χρήση ξανά της εφαρμογής. Επιπλέον δυνατότητα της κλειδαριάς είναι η χρήση ενός τετραψήφιου κωδικού (PIN) ο οποίος χρησιμοποιείται ως πρόσθετο μέτρο ασφάλειας κατά το ξεκλείδωμα της συσκευής. Η κλειδαριά καταγράφει κάθε φορά ποίος εισέρχεται και εξέρχεται από την οικεία. Σε αυτά τα δεδομένα δεν έχει ο ιδιοκτήτης της κλειδαριάς πρόσβαση ώστε να μπορέσει να τροποποιήσει ή να διαγράψει τις καταγραφές

Το σενάριο έχει ως εξής: το μήνυμα Β που στέλνεται σε ορισμένα χρονικά διαστήματα σε συγκεκριμένη εφαρμογή στο κινητό τηλέφωνο με το όνομα S3, υποδηλώνει πως η κλειδαριά συνεχίζει να είναι κλειδωμένη κανονικά και δεν έχει συμβεί κάποια παράνομη δραστηριότητα. Στην εικόνα 11 διακρίνονται τα κύρια στοιχεία πριν την έναρξης της προσομοίωσης. Το σενάριο αυτό επιλέχθηκε, αφού οι έξυπνες κλειδαριές χρησιμοποιούνται πλέον αρκετά και οι κακόβουλοι χρήστες τις προτιμούν για επιθέσεις.



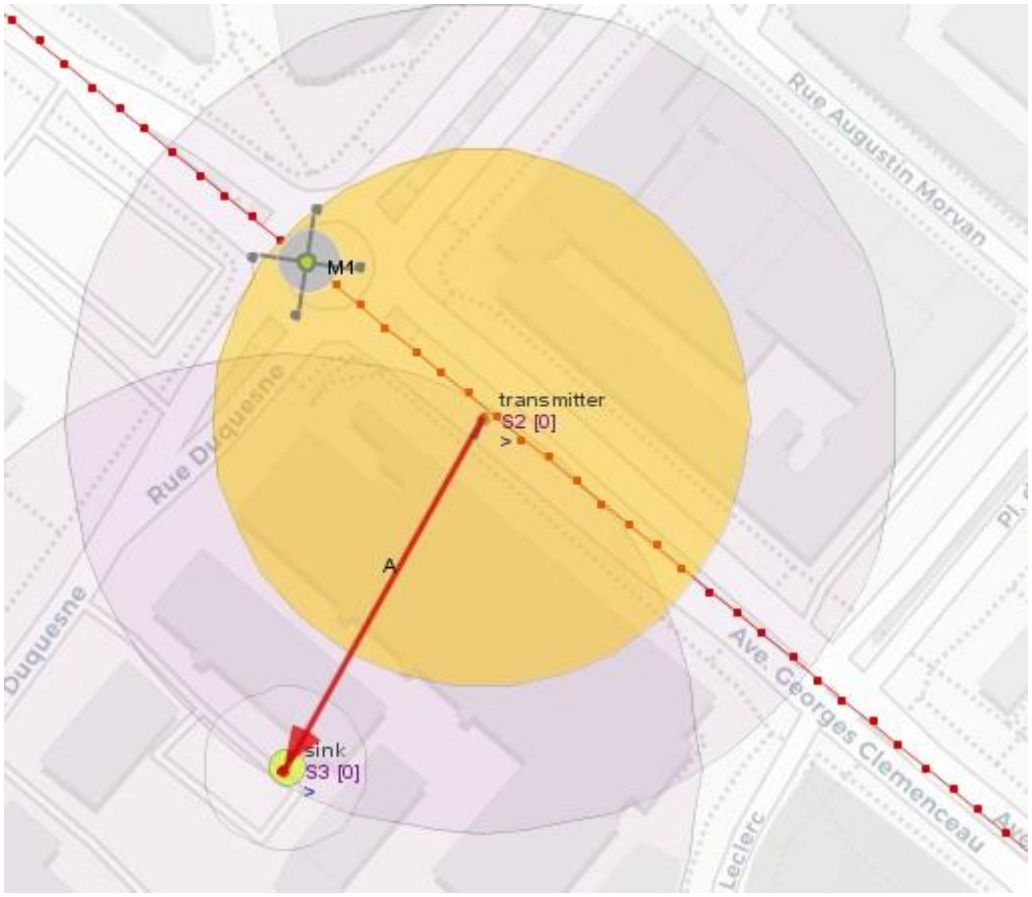
Εικόνα 11: Κύρια στοιχεία προσομοίωσης

Τα δεδομένα που διαμοιράζονται μεταξύ των δύο αντικειμένων υποδηλώνονται με το γράμμα Β.Στην εικόνα 12 η προσομοίωση έχει ήδη ξεκινήσει. Ο κινητός αισθητήρας M1 κινείται σύμφωνα με τα marker points που ορίζουν την διαδρομή του και το μήνυμα Β στέλνεται στον αισθητήρα S3.



Εικόνα 12: Έναρξη της προσομοίωσης

Όταν φθάνει το αντικείμενο M1στην κλειδαριά S2, μια επίθεση μέσω κινητού πυροδοτείται και ένας κακόβουλος χρήστης μέσω ενός λογισμικού ξεκλειδώνει την έξυπνη κλειδαριά. Το μήνυμα που ανταλλάσσεται από τα αντικείμενα S2 και S3 -το οποίο δηλώνει μια κανονικότητα- παραποιείται από B σε A όπως παρουσιάζεται και στην εικόνα 13. Υποθέτουμε πως κατά το διάστημα παραμονής του M1 στην ακτίνα ανίχνευσης (η ακτίνα υποδηλώνεται με κίτρινο χρώμα) της κλειδαριάς S2, διεξάγεται παράνομη δραστηριότητα εντός της οικίας.



Εικόνα 13:Η παραποίηση του μηνύματος

Στη συνέχεια όταν το M1 εξέρχεται από την περιοχή ανίχνευσης του S2 το μήνυμα επιστρέφει στο B και η προσομοίωση φτάνει στο τέλος της όπως φαίνεται στην εικόνα 14.

Εικόνα 14:Τέλος προσομοίωσης

Ο χρήστης του κινητού και ιδιοκτήτης της οικείας δεν αντιλαμβάνεται την αλλαγή μηνύματος από την κλειδαριά στο έξυπνο κινητό του και αντιλαμβάνεται το συμβάν μόλις επιστρέφει στο σπίτι του. Η πρώτη ενέργειά του είναι να καλέσει την αστυνομία.

6.2.2 Ανάλυση της Προσομοίωσης σύμφωνα με το μοντέλο DFIF-IoT

Η ανάλυση της συγκεκριμένης προσομοίωσης επιλέχθηκε να γίνει με το μοντέλο εγκληματολογίας Digital Forensic Investigation Framework for Internet of Things (DFIF-IoT), που προτάθηκε από τους Kebande και Ray και αναλύθηκε στο πέμπτο κεφάλαιο.

Είναι σημαντικό να υπενθυμίσουμε πως στο συγκεκριμένο μοντέλο στην πρώτη από τις τρεις ενότητες ορίζεται από τους ερευνητές τι είδους διαδικασίες θα πρέπει να ακολουθηθούν από κάποιον πριν από ένα περιστατικό. Αναφέρεται δηλαδή στον σχεδιασμό και στην προετοιμασία κατά την εγκατάσταση ενός δικτύου με αντικείμενα του IoT.

Εμείς θα αναλύσουμε το περιστατικό από την σκοπιά του ερευνητή. Έτσι η έρευνά μας θα στηριχθεί κυρίως στην ενότητα 3 του μοντέλου που είναι η Διαδικασία Αντίδρασης (Reactive Process).

Η πρώτη οντότητα της ενότητας αυτής που είναι η Αρχικοποίηση (Initialization) που περιλαμβάνει την ανίχνευση του περιστατικού από τον ιδιοκτήτη και την πρώτη αντίδρασή του που είναι να καλέσει, όπως ήδη αναφέρθηκε την αστυνομία. Μαζί με την αστυνομία καταφθάνει εξειδικευμένος ερευνητής. Ο ιδιοκτήτης της οικείας του εξηγεί τον τρόπο που επικοινωνούνε τα δύο αντικείμενα μεταξύ τους. Κατόπιν όλων αυτών ο ερευνητής σχεδιάζει τον τρόπο που θα διεξάγει την ερεύνα και πως θα αποκτήσει τα στοιχεία που χρειάζεται, αφού πλέον του είναι γνωστά τα αντικείμενα που πήραν μέρος στο γεγονός.

Αυτά τον οδηγούν στην δεύτερη οντότητα της ενότητας που είναι η Διαδικασία απόκτησης (Acquisitive process). Κατά την διάρκεια αυτής της διεργασίας ο ερευνητής έρχεται σε επαφή με την έξυπνη κλειδαριά και το έξυπνο κινητό τηλέφωνο τα οποία καταγράφονται και μπορούν να προσφέρουν ατράνταχτα αποδεικτικά στοιχεία. Ο ερευνητής συλλέγει τα δύο αντικείμενα και τα αποθηκεύει σε ηλεκτροστατική σακούλα, ώστε να τα μεταφέρει στο εργαστήριο για να τα εξετάσει. Να σημειωθεί πως το κινητό τηλέφωνο έχει ενέργεια (μπαταρία) και μπορεί να διατηρηθεί ανοιχτό, όπως και η έξυπνη κλειδαριά που διαθέτει αποσπώμενες μπαταρίας για περιπτώσεις λειτουργίας χωρίς την παροχή ηλεκτρικού ρεύματος, που είναι κ η κύρια πηγή ενέργειας. Βέβαια, ο ερευνητής σε καμιά περίπτωση δε θα ήθελε να απενεργοποιηθούν οι δύο συσκευές λόγω αποφόρτισης των μπαταριών, αφού ελλοχεύει ο κίνδυνος καταστροφής των στοιχείων.

Ο ερευνητής περνάει αυτή την στιγμή στην τρίτη οντότητα της ενότητας που είναι η Έρευνα (Investigative).Ο στόχος του είναι να ερευνήσει τα αντικείμενα, ώστε να βρει τα κατάλληλα στοιχεία, ξεκινώντας από την έξυπνη κλειδαριά.

Συνδέοντας το αντικείμενο στον ηλεκτρονικό υπολογιστή αποκτάει πρόσβαση μέσω ειδικού λογισμικού στις ρυθμίσεις και στον κώδικα της έξυπνης κλειδαριάς S2 και ξεκινάει την ανάλυση. Ο κώδικα του αντικειμένου φαίνεται παρακάτω:

```
Loop
getinfop
timez
printfile $z $x $p
dreadsensor x
if($x==1)
     send A 3
else
     send B 3
end
delay 500
```

Ο ερευνητής από την μελέτη του κώδικα αντιλαμβάνεται πως η κλειδαριά είναι προγραμματισμένη με την εντολή printfile να δημιουργεί αρχείο καταγραφής (log). Στο αρχείο καταγραφής με την εντολή getinfo θα καταγράφεται η ανίχνευση μίας κινητής συσκευής μαζί με την ταυτότητά της και οι συντεταγμένες της με την μορφή id#longitude#latitude. Ακόμα, καταγράφεται η ώρα αποστολής κάθε μηνύματος με την εντολή time. Ο κατασκευαστής της έξυπνης κλειδαριάς πρόσθεσε στον κώδικα της, την εντολή dreadsensor. Με την εντολή αυτή έχουμε x=1, αν ο αισθητήρας S2 ανιχνεύσει κάποιο κινητό αισθητήρα. Διαφορετικά x=0. Πέρα από τις παραπάνω πληροφορίες και αυτές καταγράφονται στο αρχείο.

Αμέσως μετά ο ερευνητής εξετάζει το κινητό τηλέφωνο S3. Στο κινητό θα εντοπίσει την εφαρμογή που είναι συνδεδεμένη με την έξυπνη κλειδαριά και τον κώδικά της.

```
loop
 wait
 time z
 printfile $z $x
 read x
 if($x==A)
      mark 1
 else
      mark 0
 end
```

Ένα ακόμα αρχείο καταγραφής δημιουργείται σύμφωνα με το κώδικα και την εντολή printfile στο κινητό τηλέφωνο. Εκεί καταγράφεται το μήνυμα (read), που θα είναι είτε A, είτε B και ο χρόνος (time) στον οποίο διαβάζεται ένα μήνυμα.

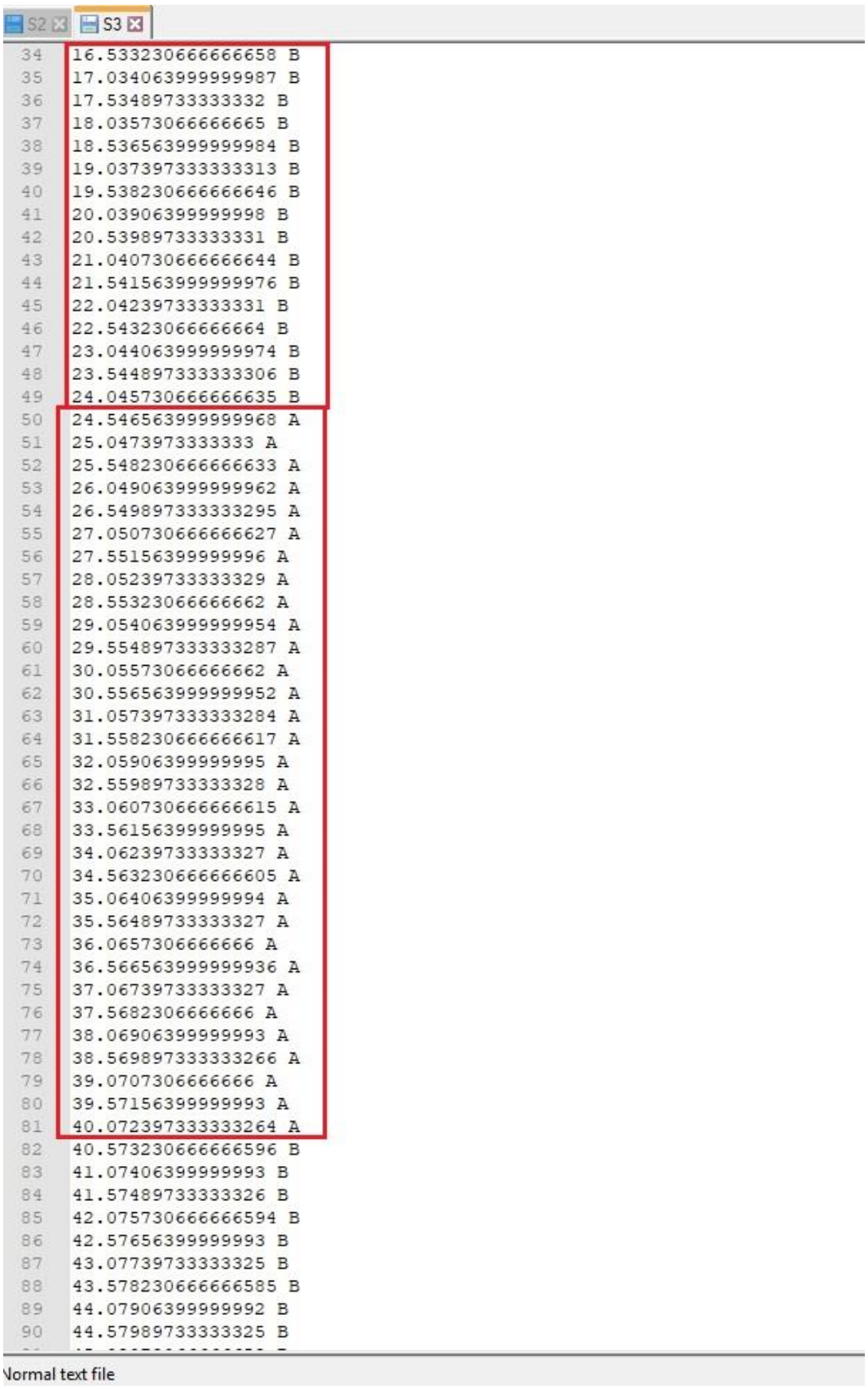
Έχοντας αναλύσει τους κώδικες των δύο αντικειμένων, μέλημα του ερευνητή είναι τώρα να βρει τα αρχεία καταγραφής, όπου θα τον βοηθήσουν να καταλήξει σε ένα ασφαλές συμπέρασμα. Ο ερευνητής εντοπίζει το αρχείο καταγραφής (log) της κλειδαριάς. Το όνομα του αρχείου είναι S2 και φαίνεται παρακάτω στην εικόνα 15.

Εικόνα 15: Αρχείο καταγραφής S2

Από το αρχείο καταγραφής ο ερευνητής αντιλαμβάνεται πως μέχρι την γραμμή 48 και το 23,53 sec όλα φαίνονταν φυσιολογικά, αφού το x=0. Αντίθετα στην γραμμή 49 και στο 24,03 sec και ως την

γραμμή 80 και στο 39,56 sec εντοπίζονται αλλαγές και καταγράφεται στο αρχείο η ταυτότητα ενός αντικειμένου και οι συντεταγμένες του.

Επόμενη κίνηση του ερευνητή είναι να εντοπίσει το αρχείο καταγραφής του κινητού τηλεφώνου S3, όπως και φαίνεται στην εικόνα 16.



Εικόνα 16: Αρχείο καταγραφής S3

Στο αρχείο καταγραφής του έξυπνου κινητού τηλεφώνου και έως την γραμμή 49 φυσιολογικά καταγράφεται σύμφωνα με τον κώδικα του S3 το μήνυμα Β. Ωστόσο, από την γραμμή 50 και στο 24,54 sec έως την γραμμή 81 και στο 40,07 sec καταγράφεται το μήνυμα Α.

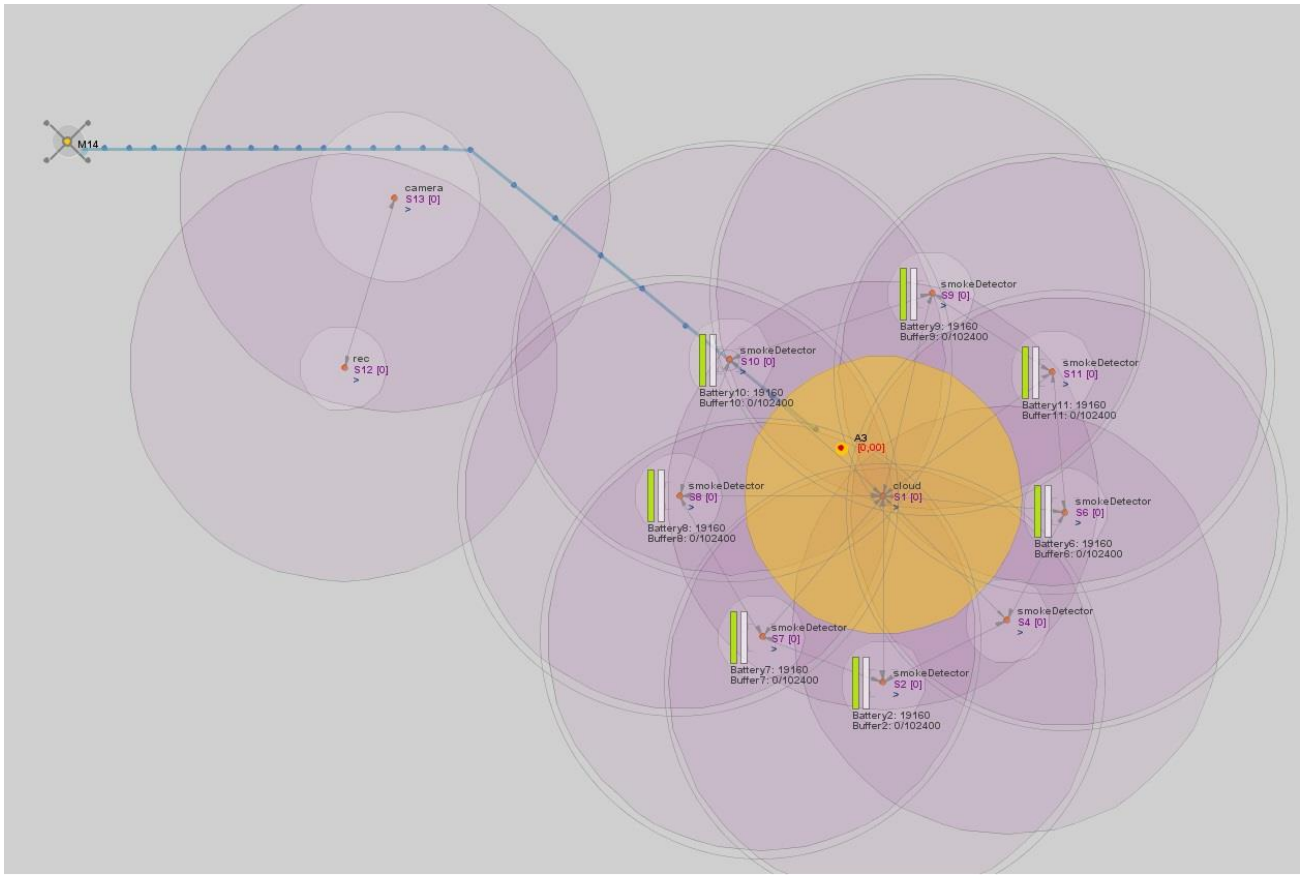
Έχοντας αυτά ως απόρροια της έρευνας του και παρατηρώντας ο ερευνητής πως περίπου την ίδια χρονική στιγμή παρατηρήθηκαν μη φυσιολογικές μεταβολές στα αρχεία καταγραφής των δύο έξυπνων αντικειμένων, καταλήγει στο συμπέρασμα πως ο χρήστης του έξυπνου κινητού τηλεφώνου με ταυτότητα id=1, παραβίασε την έξυπνη κλειδαριά μέσω ειδικού λογισμικού που είχε στο κινητό του τηλέφωνο και επιχείρησε να προβεί σε παράνομες δραστηριότητες στην οικεία του θύματος. Όλα αυτά τα στοιχεία ο ερευνητής μπορεί να τα καταθέσει στο δικαστήριο και να εξηγήσει τον τρόπο που έφτασε σε αυτό το συμπέρασμα.

6.3 Δεύτερη Προσομοίωση

Στο σημείο αυτό της εργασίας θα προχωρήσουμε σε ακόμη μία προσομοίωση η οποία θα είναι πιο περίπλοκη από την προηγούμενη και θα περιλαμβάνει περισσότερους αισθητήρες από τους οποίους θα περισυλλέξουμε δεδομένα τα οποία θα μας βοηθήσουν ώστε να παρουσιάσουμε στο δικαστήριο τα στοιχεία.

6.3.1 Περιγραφή Δεύτερης Προσομοίωσης

Σε αυτήν την προσομοίωση υποθέτουμε πως έχουμε μια αποθήκη η οποία περιέχει διάφορα προϊόντα μιας εταιρίας και εξ’ αιτίας μια ενδοεταιρικής αντιζηλίας ένας υπάλληλος καταστρέφει τα προϊόντα βάζοντας φωτιά. Στην παρακάτω εικόνα μπορούμε να δούμε τα αντικείμενα που λαμβάνουν μέρος σε αυτήν την προσομοίωση.



Εικόνα 17: Κύρια στοιχειά δεύτερης προσομοίωσης

Παρατηρώντας πιο προσεκτικά βλέπουμε πως συνολικά υπάρχουν 12 συσκευές IoT στην προσομοίωσή μας, όπως φαίνεται στον Πίνακα 4.

id συσκευής	**Όνομα συσκευής**	**Περιγραφή**
M14	M14	Έξυπνο κινητό τηλέφωνο
S13	camera	Έξυπνη κάμερα
S12	rec	Νέφος (cloud)
S1	cloud	Νέφος (cloud)
S2	smokeDetector	Έξυπνος ανιχνευτής καπνού
S4	smokeDetector	Έξυπνος ανιχνευτής καπνού
S6	smokeDetector	Έξυπνος ανιχνευτής καπνού
S7	smokeDetector	Έξυπνος ανιχνευτής καπνού
S8	smokeDetector	Έξυπνος ανιχνευτής καπνού
S9	smokeDetector	Έξυπνος ανιχνευτής καπνού
S10	smokeDetector	Έξυπνος ανιχνευτής καπνού
S11	smokeDetector	Έξυπνος ανιχνευτής καπνού

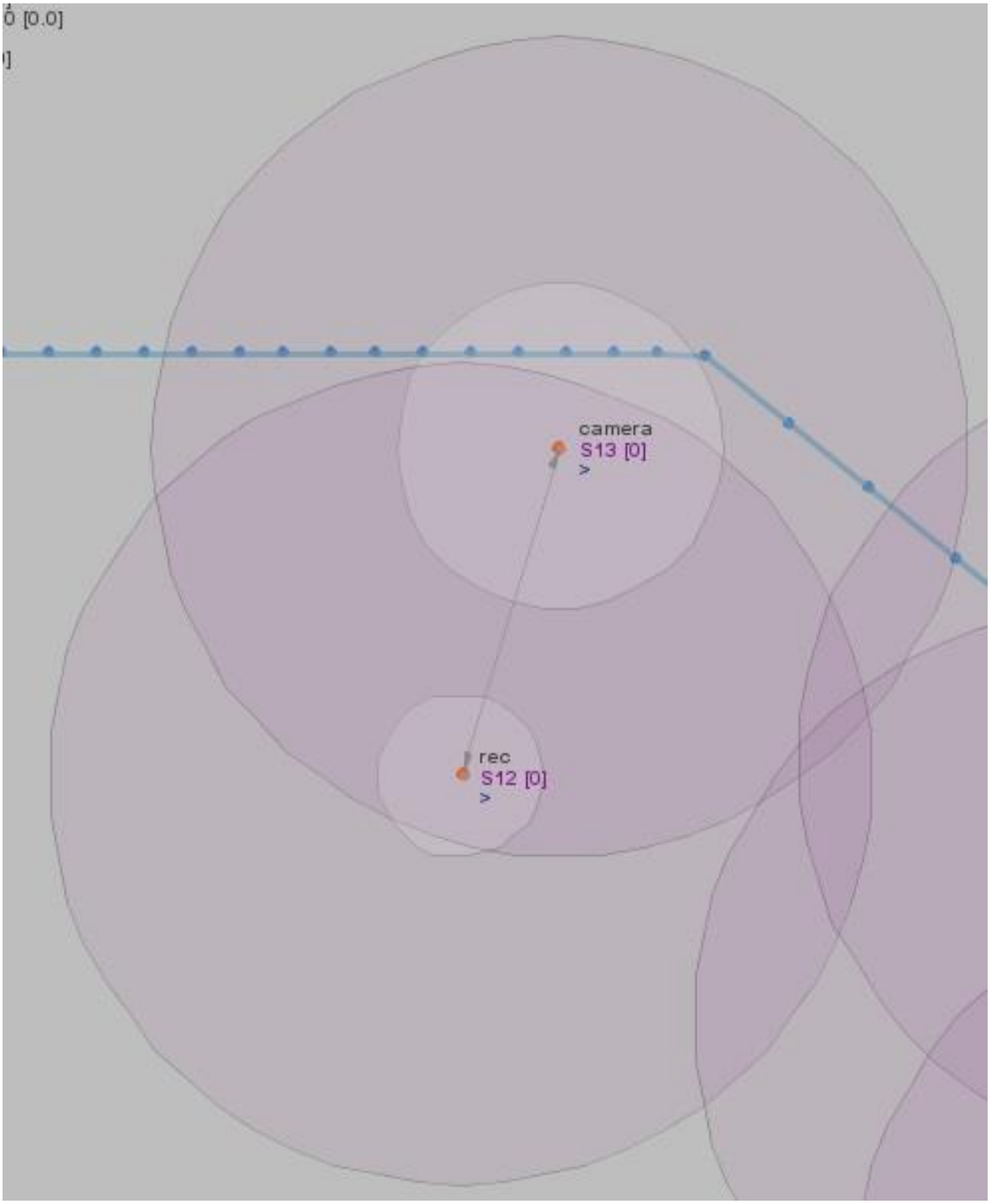
Πίνακας 4: Περιγραφή Συσκευών Δεύτερης Προσομοίωσης

Πιο συγκεκριμένα:

Μια κινητή συσκευή με id M14 η οποία είναι ένα έξυπνο κινητό τηλέφωνο με αισθητήρες GPS, μαγνητόμετρο, γυροσκόπιο, κ.α. Ο χρήστης μαζί με την συσκευή ακολουθεί την διαδρομή που ορίζεται από τα μπλε markers.

Εικόνα 18: Κινητό τηλέφωνο M14

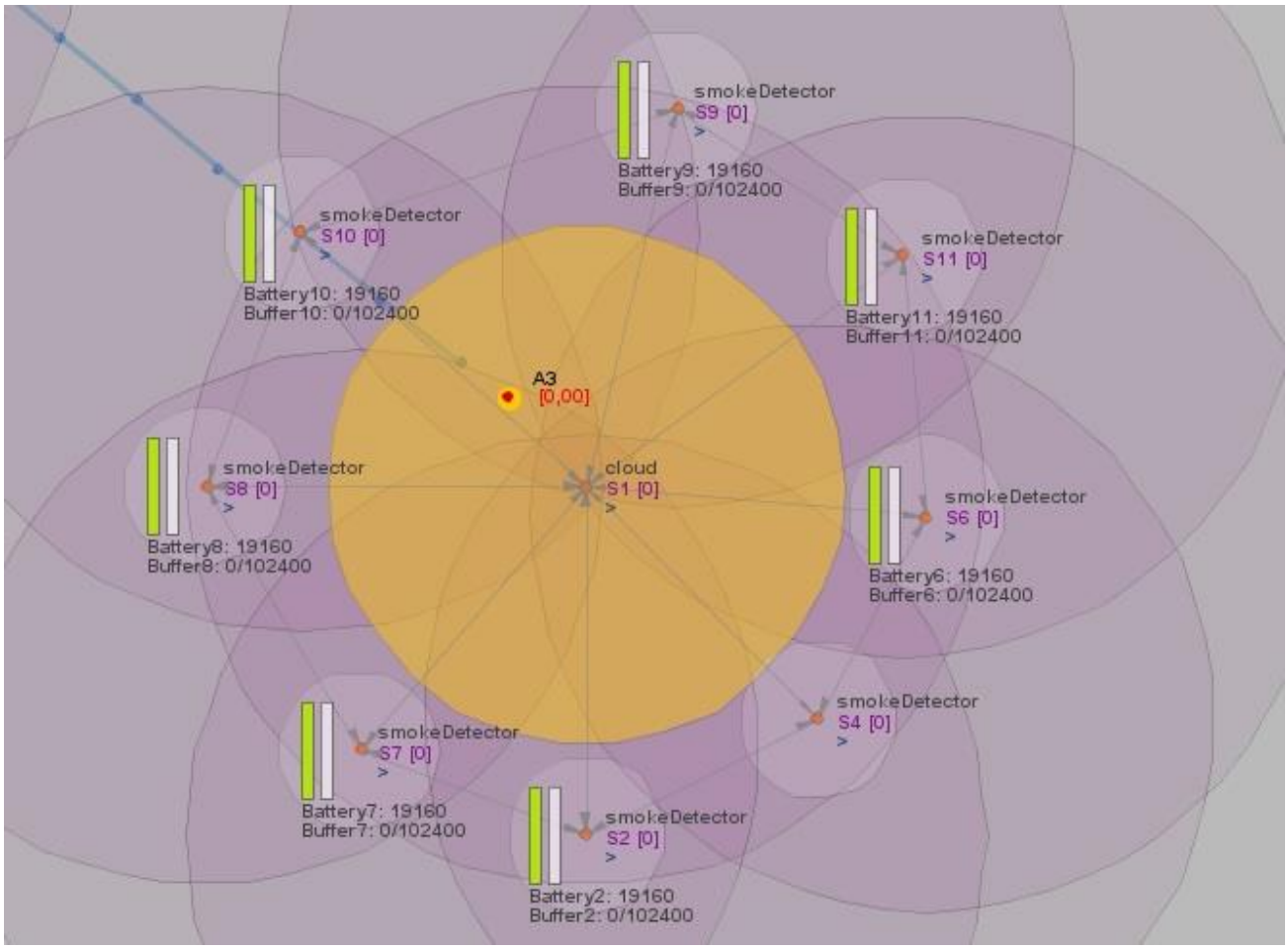
Η συσκευή S13 είναι μία έξυπνη κάμερα η οποία ειδοποιεί τον ιδιοκτήτη όταν αντιλαμβάνεται ήχο ή κίνηση. Ακόμα συνδέεται με wifi και ο χρήστης μπορεί να την ελέγχει μέσα από εφαρμογή που θα έχει στο κινητό του. Εκτός από τα παραπάνω έχει την δυνατότητα της νυχτερινής καταγραφής. Η συγκεκριμένη κάμερα μπορεί να καταγράψει έως 7 μέρες συνεχόμενα και να αποθηκεύει τις εγγραφές (βίντεο) στο νέφος (cloud). Υποθέτουμε πως το νέφος είναι ο αισθητήρας με id S12 και όνομα rec. Η κάμερα είναι τοποθετημένη στην πόρτα της αποθήκης, ώστε να καταγράφει τις κινήσεις που τυχόν γίνονται εκεί.



Εικόνα 19: Έξυπνη κάμερα

Συνεχίζοντας παρακάτω εντοπίζουμε τους αισθητήρες με id S2, S4, S6, S7, S8, S9, S10, S11 και όνομα smokeDetector. Πρόκειται για έξυπνους ανιχνευτές καπνού, οι οποίοι βρίσκονται στο χώρο της αποθήκης. Οι ανιχνευτές καπνού ειδοποιούν μέσω της εφαρμογής την οποία έχει εγκατεστημένη ο χρήστης στο κινητό του τηλέφωνο για το σημείο που εντοπίστηκε ο καπνός. Πέρα από αυτό είναι εξοπλισμένοι με ηχείο το οποίο με φυσική φωνή ειδοποιεί σε περίπτωση που χρειαστεί. Οι μπαταρίες που έχουν οι ανιχνευτές και τους επιτρέπουν την λειτουργία ελέγχονται από τον ίδιο τον ανιχνευτή και σε περίπτωση που απαιτούν αλλαγή ειδοποιούν αναλόγως. Οι

πράσινες μπάρες που παρατηρούμε δίπλα από τους αισθητήρες είναι οι μπαταρίες των αισθητήρων και τα ποσοστά τους. Ένα ακόμα χαρακτηριστικό που διαθέτει το CupCarbon είναι οι γραφικές αναπαραστάσεις κατανάλωσης της ενέργειας από τις μπαταρίες των αισθητήρων. Οι ανιχνευτές επικοινωνούν μεταξύ τους και όπως και η κάμερα που περιγράψαμε παραπάνω στέλνουν δεδομένα στον αισθητήρα με id S1 και όνομα cloud.

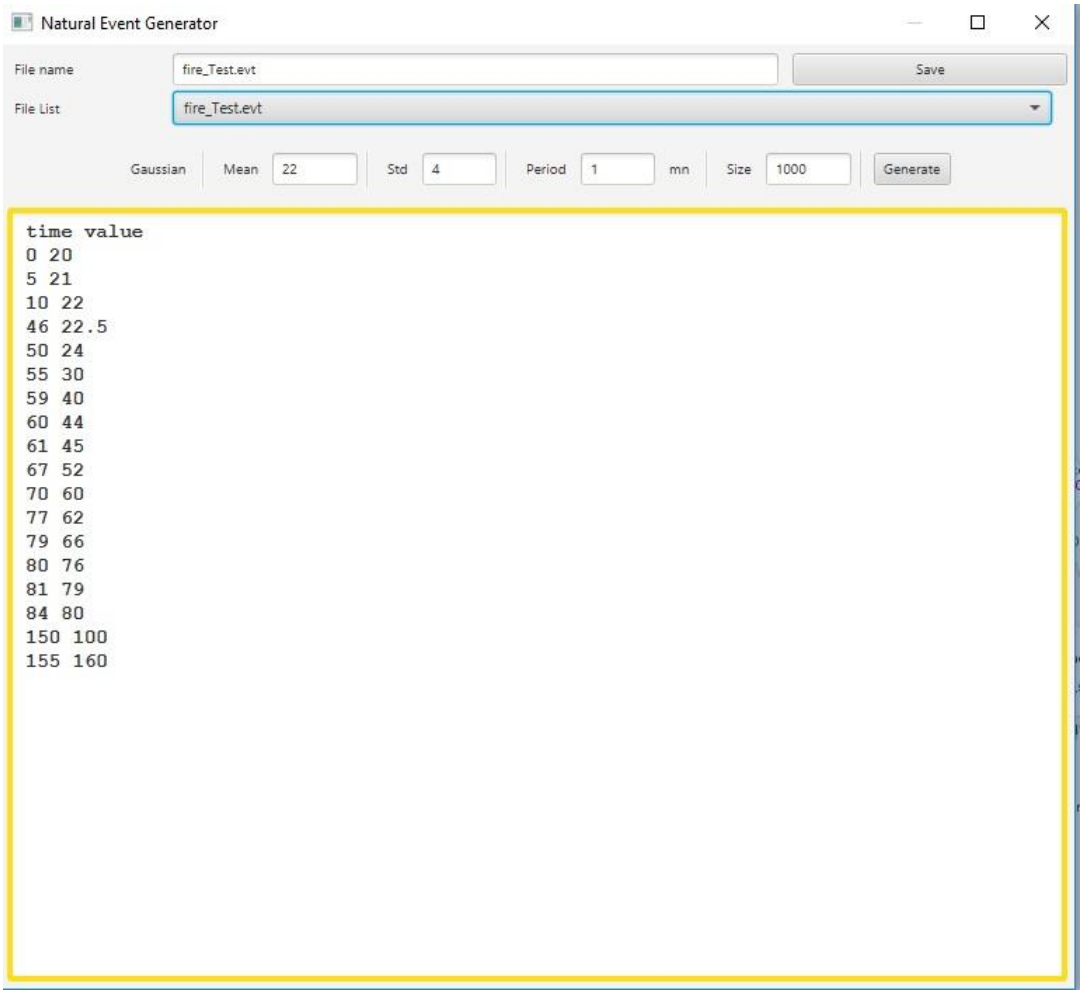


Εικόνα 20: Ανιχνευτές καπνού

Σε αυτό το σημείο θα ήταν καλό να αναφερθούμε σε μια ιδιαίτερη δυνατότητα που προσφέρει ο προσομοιωτής CupCarbon και οι δημιουργοί του το ονομάζουν Natural Event Generator. Το συγκεκριμένο χαρακτηριστικό είναι μια γεννήτρια τιμών οι οποίες προσομοιώνουν κάποιο φαινόμενο της φύσης και οι αισθητήρες που έχουν κάποιες συσκευές του IoT τις εντοπίζουν. Τέτοιες είναι η αλλαγή θερμοκρασίας, η υγρασία, η φωτιά, κτλ. Επίσης, χρησιμοποιείται για εντοπισμό των καιρικών θερμοκρασιών. Στην εικόνα 21 βλέπουμε πώς συμβολίζεται η φωτιά που θα λάβει χώρα στην προσομοίωσή μας. Ο αισθητήρας με το εξωτερικό κίτρινο χρώμα και το εσωτερικό κόκκινο συμβολίζει την φωτιά που θα ξεσπάσει.

Εικόνα 21: Natural Event

Στην εικόνα 22 που ακολουθεί είναι το παράθυρο του Natural Event Generator στο οποίο ο χρήστης μπορεί να προγραμματίζει καθορίζοντας τις τιμές που επιθυμεί ώστε να δημιουργηθεί ένα φυσικό φαινόμενο. Να σημειωθεί σε αυτό το σημείο με το κουμπί Generate, κατασκευάζεται αυτόματα ένα φυσικό φαινόμενο έτοιμο να το χρησιμοποιήσει ο χρήστης. Στη συγκεκριμένη εικόνα πρόκειται για ένα φαινόμενο που δημιουργήθηκε για τις ανάγκες της προσομοίωσης από εμάς.



Εικόνα 22: Natural Event Generator

Το σενάριο έχει ως εξής: Στη συγκεκριμένη αποθήκη, που η είσοδος γίνεται με το ξεκλείδωμα μιας κλειδαριάς υπάρχουν προϊόντα αξίας πολλών χιλιάδων ευρώ, που σκοπεύει να πουλήσει η επιχείρηση. Εκτός από τον πρόεδρο της εταιρίας, σε αυτήν έχουν πρόσβαση δύο μόνο άτομα. Τα δύο αυτά άτομα είναι οι κύριοι X και Z. Οι δύο αυτοί εργαζόμενοι διεκδικούν μια προαγωγή και επιθυμούν την καινούργια θέση το ίδιο. Ο πρόεδρος της εταιρίας αποφάνθηκε πως ο κύριος Z αξίζει την θέση και έτσι κερδίζει την προαγωγή αυτός. Αυτή η απόφαση εξοργίζει τον κύριο X και τον οδηγεί στην αποθήκη, όπου και βάζει φωτιά στο εμπόρευμα.

Στο σημείο φτάνει πρώτη από όλους η Πυροσβεστική Υπηρεσία, την οποία κάλεσαν οι περίοικοι. Ωστόσο η αποθήκη είχε καταστραφεί με όλα τα προϊόντα. Στη συνέχεια καλείται από την Πυροσβεστική ο ερευνητής, ώστε να ρίξει φως στην υπόθεση, ερευνώντας τα αίτια κάτω από τα οποία η αποθήκη τυλίχτηκε στις φλόγες.

6.3.2 Ανάλυση της Προσομοίωσης σύμφωνα με το μοντέλο FAIoT

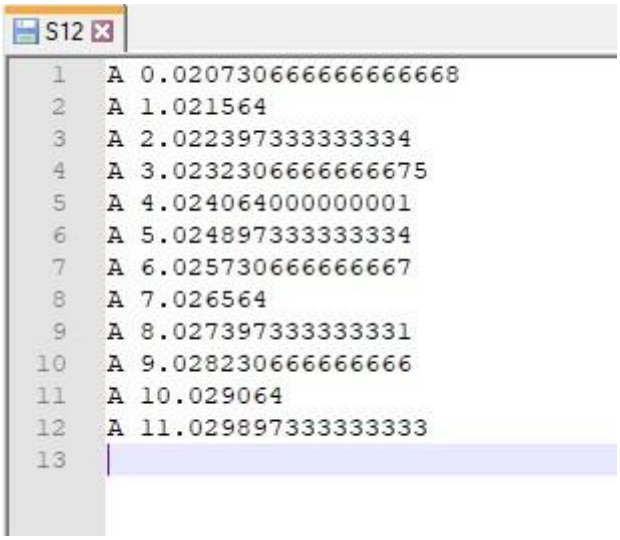
Η έρευνα του ειδικού στην καμένη αποθήκη τον οδήγησε να ανακαλύψει την έξυπνη κάμερα και τους ανιχνευτές καπνού καταστραμμένα όπως και αναμενόταν, αλλά και ένα δοχείο που πιθανότατα είχε εύφλεκτο υγρό ώστε να προξενήσει την φωτιά. Το ερωτηματικό που προέκυψε στον ερευνητή, με την ανακάλυψη αυτών των συσκευών αφορά την μη έγκαιρη ειδοποίηση της Πυροσβεστικής, αλλά ούτε και των υπευθύνων.

Ο ερευνητής μαθαίνει από τον ιδιοκτήτη (έπειτα από συνομιλία τους) πως οι συσκευές είναι καταχωρημένες στο αποθετήριο αποδείξεων και εκεί είναι καταγεγραμμένες όλες οι χρήσιμες πληροφορίες. Γνωρίζοντας αυτά ο ερευνητής μπορεί να προβεί στην ανάλυση του συμβάντος σύμφωνα με το μοντέλο FAIoT που προτάθηκε από τους Zawoad και Hasan και αναλύθηκε στο κεφάλαιο πέντε. Επιπλέον, μαθαίνει ποιοι έχουν πρόσβαση στην αποθήκη και το έχει υπόψη του, διότι πρόκειται για σημαντικό στοιχείο που θα παίξει ρόλο για την τελική έκβαση της υπόθεσης.

Ο ερευνητής όντας διαπιστευμένος έχει δικαίωμα πρόσβασης στο API για να συλλέξει τα στοιχεία που χρειάζεται. Έτσι, με την χρήση ενός εξυπηρετητή επικοινωνεί με τα άλλα τμήματα του μοντέλου. Με τη χρήση κρυπτογραφημένου κλειδιού αποκτάει ο ερευνητής πρόσβαση στα στοιχεία. Τα στοιχεία υποθέτουμε πως δεν μπορεί κανείς να τα τροποποιήσει και το κρυπτογραφημένο κλειδί το έχει στην κατοχή του μόνον ο ερευνητής. Στο τμήμα Secure Evidence Preservation (Ασφαλή Διατήρηση Αποδείξεων) ο ερευνητής βρίσκει καταγεγραμμένες τις εν λόγω συσκευές του ιδιοκτήτη της αποθήκης μαζί με διάφορα δεδομένα όπως αρχεία καταγραφής (logs), κ.α., που μπορεί να αποδειχθούν πολύτιμες πηγές στοιχείων.

Η πρώτη συσκευή που διερευνά ο εγκληματολόγος είναι η έξυπνη κάμερα (id S13) και το σημείο όπου αποθηκεύονται οι καταγραφές το οποίο είναι στο νέφος (id S12), αλλά δεν βρίσκει

κάποια ασυνήθιστη καταγραφή μέχρι το χρονικό σημείο 11.029 όπου και οι καταγραφές σταματάνε όπως μπορούμε να παρατηρήσουμε στο αρχείο καταγραφής του S12 στην εικόνα 23.



Εικόνα 23: Αρχείο καταγραφής S12

Υποθέτουμε πως με το «A» σημαίνονται βιντεοσκοπήσεις του εξωτερικού χώρου της αποθήκης χωρίς όμως κάποια αξιόλογη καταγραφή όπως και αναφέρθηκε προηγουμένως. Αυτή η απότομη διακοπή μετάδοσης της βίντεο είναι αρκετή ώστε να κινήσει την περιέργεια του ερευνητή και για αυτό το λόγο καταγράφεται σαν σημαντικό στοιχείο. Παρατηρώντας το αρχείο log ο εγκληματολόγος αναζητεί το χρονικό σημείο 11.029 και αντιλαμβάνεται πως εκεί πράγματι είναι η τελευταία καταγραφή βίντεο (A) στο νέφος με το id S12. Άρα, το ερώτημα που προκύπτει τώρα είναι για ποιο λόγο έχει σταματήσει τις καταγραφές η κάμερα.

```
--------------------------------------------------
Time : 11.029897333333333
Min (milliseconds) : 0.004897333333333333
S12 Buffer available, exit waiting.
S12 GET TIME.
S12 READ
S12 is reading from its buffer "A" and puts it in x
S12 PRINT [println, $x]
S12 PRINTFILE [printfile, $x, $t]
S12 Starts the loop section.
S12 is waiting for data ...
```

Εικόνα 24: Τμήμα του log

Αφού τελειώσει την έρευνά του στην έξυπνη κάμερα, συνεχίζει παρακάτω και συναντά τους ανιχνευτές καπνού όπου και αναμένει να βρει ακόμα πιο χρήσιμες πληροφορίες. Όπως και στην κάμερα έτσι και στους ανιχνευτές ο ερευνητής θα μελετήσει τα αρχεία καταγραφής, διότι είναι από

τις πιο σημαντικές πηγές άντλησης στοιχείων. Παρακάτω έχουμε δύο εικόνες δείγματα αρχείων καταγραφής για τους ανιχνευτές με id S6 και S10 τους οποίους ανέκτησε ο ερευνητής από το cloud που ήταν αποθηκευμένοι.

S6

```
1  0.009064000000000001 0.0 -4.4905757904052734#48.392004071467085
2  1.0132306666666666 20.0 -4.4905757904052734#48.392004071467085
3  2.0165640000000002 20.0 -4.4905757904052734#48.392004071467085
4  3.019897333333334 20.0 -4.4905757904052734#48.392004071467085
5  4.0232306666666675 20.0 -4.4905757904052734#48.392004071467085
6  5.0265640000000005 21.0 -4.4905757904052734#48.392004071467085
7  6.029897333333333 21.0 -4.4905757904052734#48.392004071467085
8  7.0332306666666655 21.0 -4.4905757904052734#48.392004071467085
9  8.036563999999998 21.0 -4.4905757904052734#48.392004071467085
10 9.039897333333332 21.0 -4.4905757904052734#48.392004071467085
11 10.043230666666666 21.0 -4.4905757904052734#48.392004071467085
12 11.046564 21.0 -4.4905757904052734#48.392004071467085
13 12.049897333333332 21.0 -4.4905757904052734#48.392004071467085
14 13.053230666666666 21.0 -4.4905757904052734#48.392004071467085
15 14.056564 21.0 -4.4905757904052734#48.392004071467085
16 15.059897333333334 22.0 -4.4905757904052734#48.392004071467085
17 16.063230666666666 22.0 -4.4905757904052734#48.392004071467085
18 17.066564 22.0 -4.4905757904052734#48.392004071467085
19 18.069897333333333 22.0 -4.4905757904052734#48.392004071467085
20 19.073230666666667 22.0 -4.4905757904052734#48.392004071467085
21 20.076563999999998 22.0 -4.4905757904052734#48.392004071467085
```

Εικόνα 25: Αρχείο καταγραφής ανιχνευτή S6

S10

```
1  0.009064000000000001 0.0 -4.4923138618469238#48.39252414097353
2  1.0132306666666666 20.0 -4.4923138618469238#48.39252414097353
3  2.0165640000000002 20.0 -4.4923138618469238#48.39252414097353
4  3.019897333333334 20.0 -4.4923138618469238#48.39252414097353
5  4.0232306666666675 20.0 -4.4923138618469238#48.39252414097353
6  5.0265640000000005 21.0 -4.4923138618469238#48.39252414097353
7  6.029897333333333 21.0 -4.4923138618469238#48.39252414097353
8  7.0332306666666655 21.0 -4.4923138618469238#48.39252414097353
9  8.036563999999998 21.0 -4.4923138618469238#48.39252414097353
10 9.039897333333332 21.0 -4.4923138618469238#48.39252414097353
11 10.043230666666666 21.0 -4.4923138618469238#48.39252414097353
12 11.046564 21.0 -4.4923138618469238#48.39252414097353
13 12.049897333333332 21.0 -4.4923138618469238#48.39252414097353
14 13.053230666666666 21.0 -4.4923138618469238#48.39252414097353
15 14.056564 21.0 -4.4923138618469238#48.39252414097353
16 15.059897333333334 22.0 -4.4923138618469238#48.39252414097353
17 16.063230666666666 22.0 -4.4923138618469238#48.39252414097353
18 17.066564 22.0 -4.4923138618469238#48.39252414097353
19 18.069897333333333 22.0 -4.4923138618469238#48.39252414097353
20 19.073230666666667 22.0 -4.4923138618469238#48.39252414097353
21 20.076563999999998 22.0 -4.4923138618469238#48.39252414097353
```

Εικόνα 26: Αρχείο καταγραφής ανιχνευτή S10

Ο ερευνητής μελετώντας τα αρχεία και τους αριθμούς που υπάρχουν εκεί βλέπει αρκετές ομοιότητες σε όλα τα log των ανιχνευτών. Οι αριθμοί που υπάρχουν μεταφράζονται σε χρόνο, θερμοκρασία, συντεταγμένες. Αυτό σημαίνει πως στην αριθμητική ακολουθία 1.0132306666666666 20.0 -4.492313861846924#48.392524140973533, ο αριθμός 1.0123066666666666 είναι χρονικό σημείο, ο αριθμός 20.0 είναι η θερμοκρασία και το -4.492313861846924#48.39252414097353 μεταφράζεται σε γεωγραφικό μήκος#πλάτος. Οι ανιχνευτές βρίσκονται στον ίδιο χώρο σε διαφορετικά σημεία και γι' αυτό το κάθε ένα από αυτά τα αντικείμενα έχει διαφορετική καταγραφή στη γεωγραφική του θέση μέσα στην αποθήκη. Οι άλλες τιμές (χρόνος, θερμοκρασία) είναι ακριβώς ίδιες.

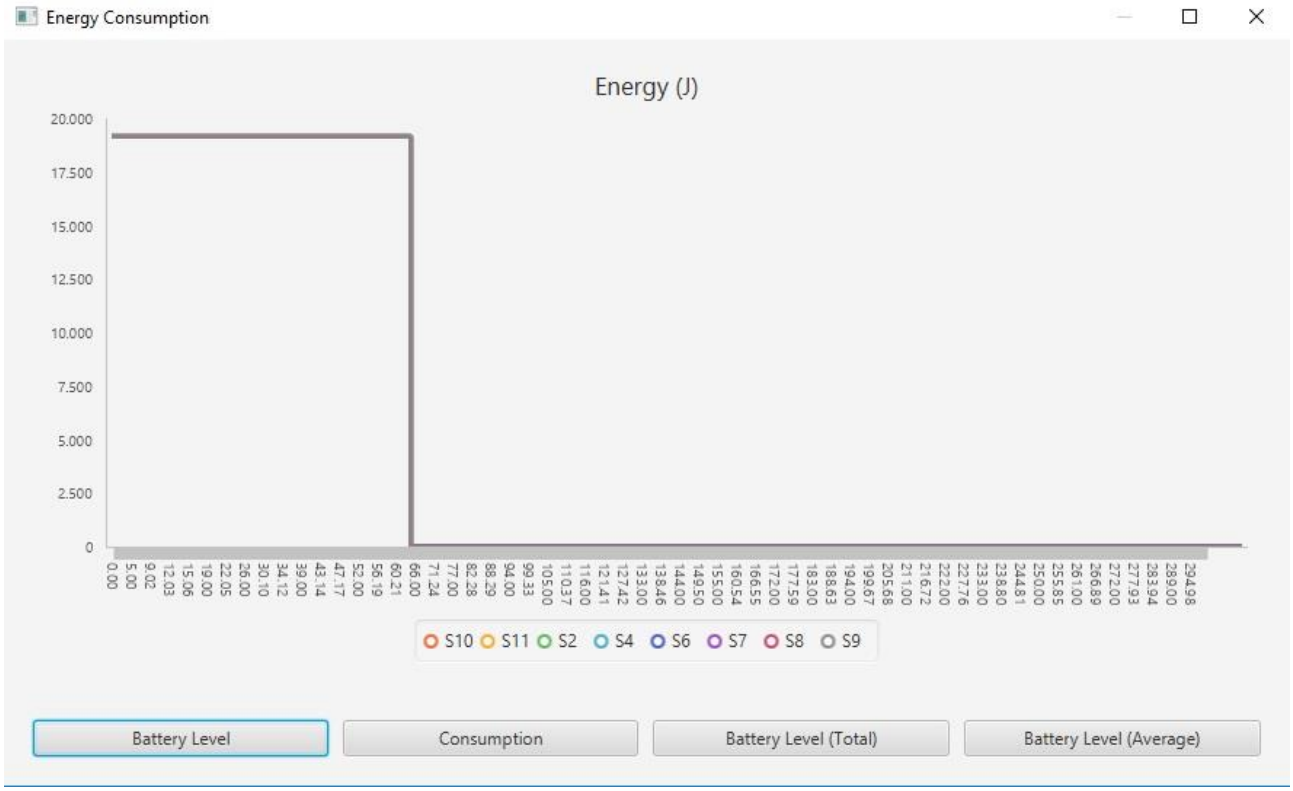
Μέσα από την αναζήτηση ο ειδικός της ψηφιακής εγκληματολογίας συνειδητοποιεί πως στο χρονικό σημείο 61.21323066666648, με θερμοκρασία 22.5 και στη γεωγραφική θέση -4.490575790405273#48.392004071467085 (ανιχνευτής με id S6) οι καταγραφές τερματίζονται, όπως φαίνεται και στην εικόνα 27. Η θερμοκρασία 22.5 είναι φυσιολογική, άρα απορρίπτεται η ιδέα πως ο τερματισμός των καταγραφών οφείλεται στη καταστροφή από την φωτιά.

```
40  39.13989733333329 22.0 -4.490575790405273#48.392004071467085
41  40.14323066666662 22.0 -4.490575790405273#48.392004071467085
42  41.14656399999994 22.0 -4.490575790405273#48.392004071467085
43  42.14989733333327 22.0 -4.490575790405273#48.392004071467085
44  43.153230666666595 22.0 -4.490575790405273#48.392004071467085
45  44.15656399999992 22.0 -4.490575790405273#48.392004071467085
46  45.15989733333325 22.0 -4.490575790405273#48.392004071467085
47  46.16323066666657 22.0 -4.490575790405273#48.392004071467085
48  47.1665639999999 22.0 -4.490575790405273#48.392004071467085
49  48.169897333333225 22.0 -4.490575790405273#48.392004071467085
50  49.173230666666555 22.0 -4.490575790405273#48.392004071467085
51  50.176563999999885 22.0 -4.490575790405273#48.392004071467085
52  51.17989733333321 22.0 -4.490575790405273#48.392004071467085
53  52.18323066666654 22.0 -4.490575790405273#48.392004071467085
54  53.18656399999986 22.0 -4.490575790405273#48.392004071467085
55  54.18989733333319 22.0 -4.490575790405273#48.392004071467085
56  55.193230666666516 22.0 -4.490575790405273#48.392004071467085
57  56.196563999999846 22.0 -4.490575790405273#48.392004071467085
58  57.199897333333176 22.0 -4.490575790405273#48.392004071467085
59  58.2032306666665 22.0 -4.490575790405273#48.392004071467085
60  59.20656399999983 22.0 -4.490575790405273#48.392004071467085
61  60.20989733333315 22.0 -4.490575790405273#48.392004071467085
62  61.21323066666648 22.5 -4.490575790405273#48.392004071467085
```

Εικόνα 27: Τερματισμός καταγραφής ανιχνευτών

Ο ερευνητής θα ελέγξει από το cloud που είναι καταγεγραμμένες οι πληροφορίες, τα ποσοστά των μπαταριών και αν αυτά φαίνεται ότι έχουν τροποποιηθεί από κακόβουλους χρήστες. Στην εικόνα 28 στην γραφική παράσταση, παρατηρείται μια μη φυσιολογική εξέλιξη και αυτή είναι η απότομη πτώση της ενέργειας της μπαταρίας των ανιχνευτών, η οποία οδήγησε στον τερματισμό

της λειτουργίας τους. Προστίθεται ένα ακόμα ερώτημα που είναι το εξής: Πώς μειώθηκε ξαφνικά στο μηδέν η ενέργεια όλων των μπαταριών;



Εικόνα 28: Κατανάλωση μπαταρίας ανιχνευτών

Οι έρευνες πλέον στρέφονται στους δύο εργαζόμενους της εταιρείας, που είχαν εκτός του προέδρου πρόσβαση στην αποθήκη, τον κύριο Χ και τον κύριο Ζ. Στις περιπτώσεις των δύο κυρίων πέρα από τις ερωτήσεις που μπορεί να τους υποβληθούν, ο ερευνητής θα πρέπει να ερευνήσει εξονυχιστικά τα κινητά τους τηλέφωνα για να βρει πληροφορίες για την θέση τους. Ξεκινώντας από τον κύριο Ζ, (που κέρδισε και την προαγωγή) στην ερώτηση πού βρισκόταν την μέρα της φωτιάς απάντησε εκτός της πόλης. Ο ερευνητής για να το επιβεβαιώσει δεν έχει παρά να ελέγξει το GPS του κινητού του τηλεφώνου. Στην εικόνα 29, βλέπουμε πως ο κύριος Ζ έχει δίκιο, αφού στο GPS του κινητού του είναι αποτυπωμένες διαφορετικές συντεταγμένες σε σχέση με εκείνες της αποθήκης και των ανιχνευτών της.

routeZ.gps

```
1  1 -4.359651803970337 48.23224862198875 0.0 4.0
2  1 -4.358965158462524 48.23222003546573 0.0 4.0
3  1 -4.358278512954712 48.2321914489427 0.0 4.0
4  1 -4.357591867446899 48.23216286241967 0.0 4.0
5  1 -4.356905221939087 48.23213427589664 0.0 4.0
6  1 -4.356218576431274 48.23210568937361 0.0 4.0
7  1 -4.355531930923462 48.23207710285058 0.0 4.0
8  1 -4.354845285415649 48.23204851632755 0.0 4.0
9  1 -4.354158639907837 48.23201992980452 0.0 4.0
```

Εικόνα 29: GPS κινητού τηλεφώνου κυρίου Z

Συνέχεια έχει τώρα ο κύριος Χ, ο οποίος στην ερώτηση που βρισκόταν την ώρα της φωτιάς απάντησε και αυτός εκτός πόλης. Αυτό όμως δεν επιβεβαιώνεται από τον έλεγχο του GPS του έξυπνου κινητού του. Στην εικόνα 30 βλέπουμε πως το GPS του κύριου Χ προδίδει την τοποθεσία του, αφού οι συντεταγμένες είναι ίδιες με αυτές των ανιχνευτών.

routeX.gps

```
1  1 -4.495677351951599 48.39325080441507 0.0 4.0
2  1 -4.495551288127899 48.393250581786916 0.0 4.0
3  1 -4.495425224304199 48.39325035915877 0.0 4.0
4  1 -4.495299160480499 48.393250136530625 0.0 4.0
5  1 -4.495173096656799 48.39324991390247 0.0 4.0
6  1 -4.495047032833099 48.39324969127432 0.0 4.0
7  1 -4.494920969009399 48.393249468646175 0.0 4.0
8  1 -4.4947949051856995 48.393249246018O3 0.0 4.0
9  1 -4.4946688413619995 48.39324902338988 0.0 4.0
10 1 -4.4945427775383 48.393248800761725 0.0 4.0
11 1 -4.4944167137146 48.39324857813358 0.0 4.0
12 1 -4.4942906498909 48.393248355505435 0.0 4.0
13 1 -4.4941645860672 48.39324813287728 0.0 4.0
14 1 -4.4940385222435 48.39324791024913 0.0 4.0
15 1 -4.4939124584198 48.393247687620985 0.0 4.0
16 1 -4.4937863945961 48.39324746499284 0.0 4.0
17 1 -4.4936603307724 48.39324724236469 0.0 4.0
18 1 -4.493436366319656 48.39312657675913 0.0 4.0
19 1 -4.493212401866913 48.393005911153566 0.0 4.0
20 1 -4.492988437414169 48.392885245548 0.0 4.0
21 1 -4.492764472961426 48.39276457994244 0.0 4.0
22 1 -4.492540508508682 48.39264391433687 0.0 4.0
23 1 -4.492316544055939 48.39252324873131 0.0 4.0
24 1 -4.492092579603195 48.392402583125744 0.0 4.0
25 1 -4.491868615150452 48.39228191752019 0.0 4.0
26
```

S6

```
1  0.009064000000000001 0.0 -4.4905757904052738#48.392004071467085
2  1.0132306666666666 20.0 -4.4905757904052738#48.392004071467085
3  2.0165640000000002 20.0 -4.4905757904052738#48.392004071467085
4  3.019897333333334 20.0 -4.4905757904052738#48.392004071467085
5  4.0232306666666675 20.0 -4.4905757904052738#48.392004071467085
6  5.0265640000000005 21.0 -4.4905757904052738#48.392004071467085
7  6.029897333333333 21.0 -4.4905757904052738#48.392004071467085
8  7.0332306666666655 21.0 -4.4905757904052738#48.392004071467085
9  8.036563999999998 21.0 -4.4905757904052738#48.392004071467085
10 9.039897333333332 21.0 -4.4905757904052738#48.392004071467085
11 10.043230666666666 21.0 -4.4905757904052738#48.392004071467085
12 11.046564 21.0 -4.4905757904052738#48.392004071467085
13 12.049897333333332 21.0 -4.4905757904052738#48.392004071467085
14 13.053230666666666 21.0 -4.4905757904052738#48.392004071467085
15 14.056564 21.0 -4.4905757904052738#48.392004071467085
16 15.059897333333334 22.0 -4.4905757904052738#48.392004071467085
17 16.063230666666666 22.0 -4.4905757904052738#48.392004071467085
18 17.066564 22.0 -4.4905757904052738#48.392004071467085
19 18.069897333333333 22.0 -4.4905757904052738#48.392004071467085
20 19.073230666666667 22.0 -4.4905757904052738#48.392004071467085
21 20.076563999999998 22.0 -4.4905757904052738#48.392004071467085
22 21.07989733333333 22.0 -4.4905757904052738#48.392004071467085
23 22.083230666666665 22.0 -4.4905757904052738#48.392004071467085
24 23.086564000000003 22.0 -4.4905757904052738#48.392004071467085
25 24.089897333333337 22.0 -4.4905757904052738#48.392004071467085
26 25.09323066666667 22.0 -4.4905757904052738#48.392004071467085
```

Εικόνα 30: Σύγκριση GPS κινητού τηλεφώνου και ανιχνευτών

Ένα ακόμα ακράδαντο στοιχείο που εξυπηρετεί τον ερευνητή και μπορεί να το παρουσιάσει στο δικαστήριο προέρχεται από το αρχείο log και μας επιβεβαιώνει όπως φαίνεται στην εικόνα 31 πως στο χρονικό σημείο 61.213230666666648 τερματίστηκε η λειτουργία των ανιχνευτών, επειδή ο κύριος Χ συνδέθηκε μέσω της εφαρμογής με αυτές τις συσκευές και μέσω κάποιου λογισμικού κατάφερε τον τερματισμό της λειτουργίας τους.

```
Time : 61.21323066666648
Min (milliseconds) : 0.007397333333333334
S10 Buffer available, exit waiting.
S10 READ
S10 is reading from its buffer "22.5" and puts it in x
S10 PRINT [println, $x]
S10 GET TIME.
S10 GET POSITION.
S10 PRINTFILE [printfile, $t, $x, $pos]
S10 BATTERY SET0.
S10 Starts the loop section.
S10 is waiting for data ...
S11 Buffer available, exit waiting.
S11 READ
S11 is reading from its buffer "22.5" and puts it in x
S11 PRINT [println, $x]
S11 GET TIME.
S11 GET POSITION.
S11 PRINTFILE [printfile, $t, $x, $pos]
S11 BATTERY SET0.
S11 Starts the loop section.
S11 is waiting for data ...
S2 Buffer available, exit waiting.
S2 READ
S2 is reading from its buffer "22.5" and puts it in x
S2 PRINT [println, $x]
S2 GET TIME.
S2 GET POSITION.
S2 PRINTFILE [printfile, $t, $x, $pos]
S2 BATTERY SET0.
S2 Starts the loop section.
S2 is waiting for data ...
S4 Buffer available, exit waiting.
S4 READ
S4 is reading from its buffer "22.5" and puts it in x
S4 PRINT [println, $x]
S4 GET TIME.
S4 GET POSITION.
S4 PRINTFILE [printfile, $t, $x, $pos]
S4 BATTERY SET0.
S4 Starts the loop section.
S4 is waiting for data ...
S6 Buffer available, exit waiting.
S6 READ
S6 is reading from its buffer "22.5" and puts it in x
S6 PRINT [println, $x]
S6 GET TIME.
S6 GET POSITION.
S6 PRINTFILE [printfile, $t, $x, $pos]
S6 BATTERY SET0
S6 Starts the loop section.
S6 is waiting for data ...
S7 Buffer available, exit waiting.
S7 READ
```

Εικόνα 31: Μηδενισμός μπαταριών ανιχνευτών

Φτάνοντας προς τέλος της έρευνας του δεύτερου σεναρίου ο ερευνητής σύμφωνα με το μοντέλο FAIoT, που βάση με αυτό διεξήγαγε την έρευνά του, εξασφάλισε χάρις το χαρακτηριστικό Secure Provenance (Ασφαλής Προέλευση) την σωστή ακολουθία των γεγονότων, αφού διαφυλάσσεται η ακριβής ιεραρχία των αποδεικτικών στοιχείων χρησιμοποιώντας το σύστημα καταγραφής της προέλευσης (PASS) και έτσι μπορεί να αναπαραχθεί το ιστορικό προέλευσης για τη χρήση των αποδείξεων.

Έχοντας συγκεντρωμένα όλα αυτά τα στοιχεία ο ερευνητής μπορεί να παραστεί στην δικαστική αίθουσα, να αναπαράγει την εγκληματολογική σκηνή και να παρουσιάσει τα ευρήματά του ώστε να καταδικαστούν οι υπεύθυνοι. Το εν λόγω σενάριο είναι αντιπροσωπευτικό αφού περιλαμβάνει συσκευές του IoT που δεν είναι ασυνήθιστες και μπορεί να επωφεληθεί από αυτές ένας ερευνητής για να εξάγει σημαντικά στοιχεία που μπορεί να τον οδηγήσουν σε σωστά συμπεράσματα.

6.4 Τρίτη προσομοίωση

Συνεχίζουμε με το τρίτο σενάριο όπου θα παρουσιάσουμε άλλη μια επίθεση σε συσκευές του IoT. Μέσα από τα στοιχεία που προσφέρει ο προσομοιωτής CupCarbon θα προσπαθήσουμε να συγκεντρώσουμε τα δεδομένα αυτά που θα μας οδηγήσουν να καταλήξουμε σε ένα συμπέρασμα για την εγκληματική ενέργεια που διεξήχθη.

6.4.1 Περιγραφή Τρίτης Προσομοίωσης

Στην τρίτη προσομοίωση βρισκόμαστε σε ένα εργοστάσιο το οποίο παράγει ηλεκτρολογικό υλικό. Οι υπεύθυνοι, για την ασφάλεια του προσωπικού έχουν εγκαταστήσει στον χώρο της παραγωγής διάφορους ανιχνευτές αερίου. Οι συσκευές αυτές στην περίπτωση που ανιχνεύσουν υψηλές τιμές αερίου ειδοποιούν, ώστε οι εργαζόμενοι να εγκαταλείψουν τον χώρο για να μην υπάρξουν θύματα. Συνέπεια αυτού βέβαια είναι να σταματάει η παραγωγή και οι καθυστερήσεις (μέχρι να επανέλθουν όλα σε φυσιολογικά επίπεδα) να είναι μεγάλες.

Ένας κακόβουλος χρήστης (χωρίς κάποιον συγκεκριμένο λόγο) προσπαθεί να αποκτήσει πρόσβαση στον ανιχνευτή αερίου ώστε να εξετάσει την άμυνά του. Τελικά, χωρίς να αντιμετωπίσει ιδιαίτερη δυσκολία καταφέρνει να αποκτήσει πρόσβαση στον ανιχνευτή καπνού και στις υπόλοιπες συσκευές IoT. Εξαιτίας της σχεδόν ανύπαρκτης άμυνας των συσκευών ξεπερνάει την διαδικασία αυθεντικοποίησης και έχει πλέον την δυνατότητα να κάνει αλλαγές σε όποια συσκευή επιθυμεί.

Εικόνα 32:Κύρια στοιχεία τρίτης προσομοίωσης

Στην προσομοίωση αυτή χρησιμοποιήσαμε άλλο ένα χαρακτηριστικό του CupCarbon, το οποίο είναι η δυνατότητα σχεδιασμού κτιρίων, όπως φαίνεται και στην εικόνα 32. Οι συσκευές του IoT που έχουμε είναι 5, όπως φαίνονται συγκεντρωτικά και στον Πίνακα 5.

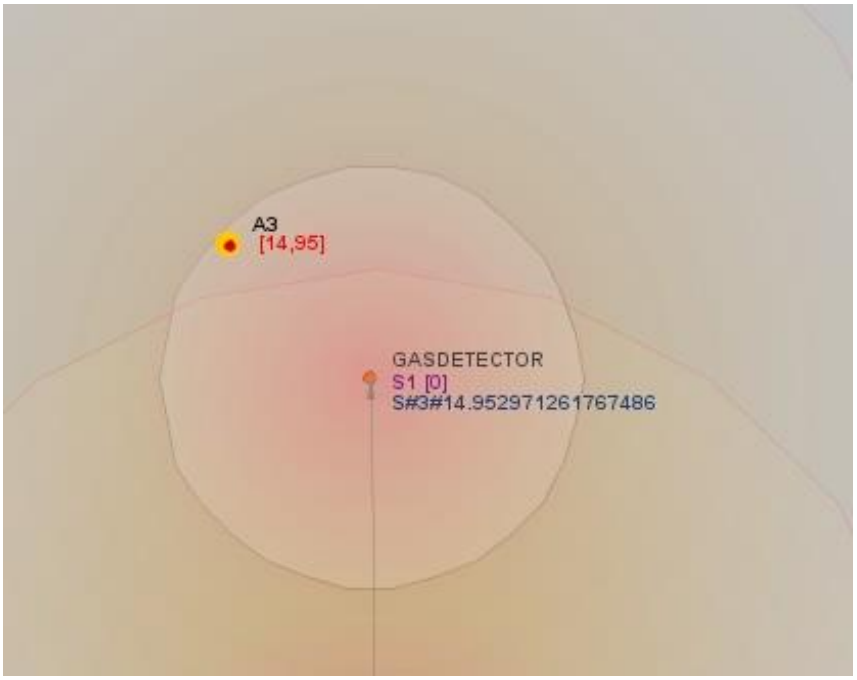
id συσκευής	**Όνομα συσκευής**	**Περιγραφή**
S1	GAS DETECTOR	Ανιχνευτής Καπνού
S4	sensor 1	Αισθητήρας 1
S5	sensor 2	Αισθητήρας 2
S2	receiver	Receiver
S6	ALARM	Συναγερμός

Πίνακας 5: Περιγραφή Συσκευών Τρίτης Προσομοίωσης

Πιο συγκεκριμένα έχουμε:

Στην εικόνα 33 φαίνεται ένας αισθητήρας με id A3. Υποθέτουμε πως είναι η ατμόσφαιρα του χώρου, όπου ο ανιχνευτής καπνού αντλεί τις τιμές του αερίου.

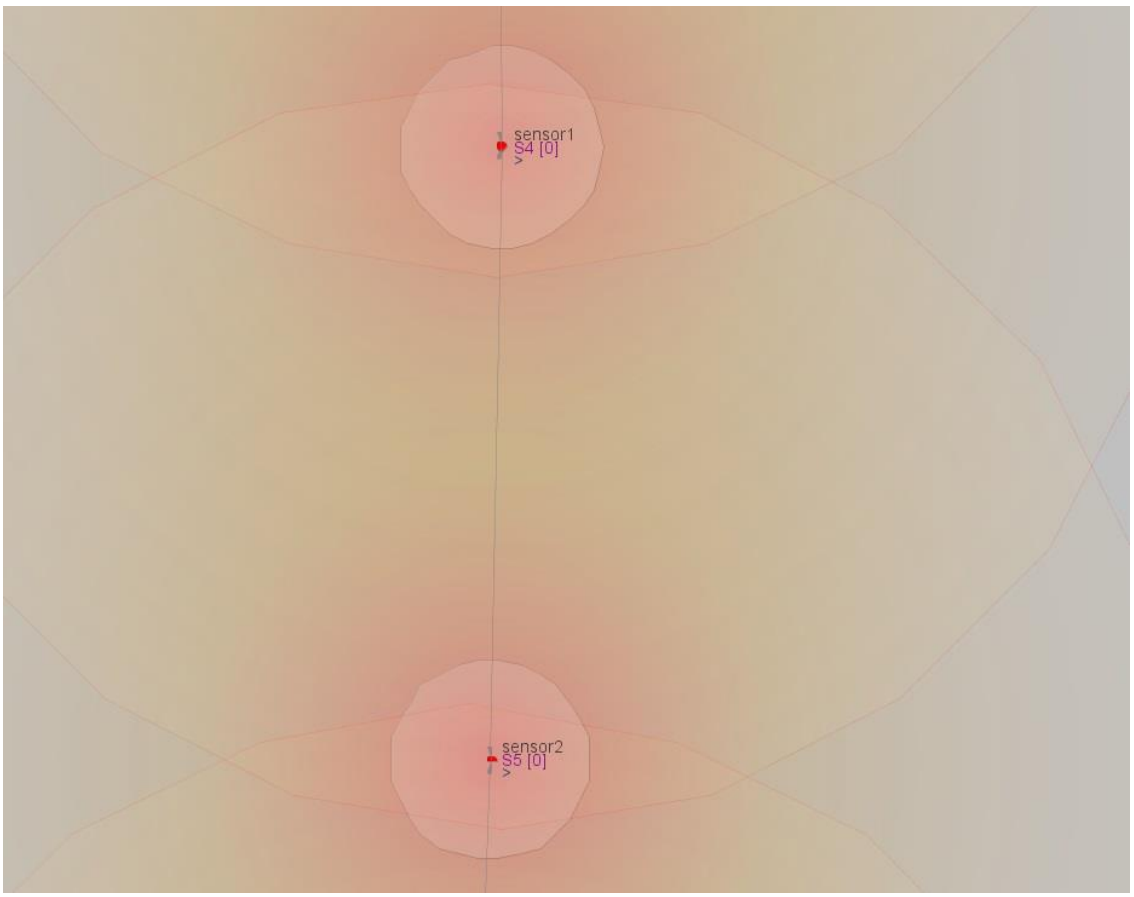
Την συσκευή με id S1, που είναι ο βασικός ανιχνευτής καπνού που λαμβάνει τις τιμές από την ατμόσφαιρα, τις αποθηκεύει, δημιουργεί αρχεία logs και ειδοποιεί για υψηλές τιμές αερίου. Το αέριο (gas) μετριέται σε ppm (partspermillion) και όταν η τιμή του είναι μεγαλύτερη από 100 ppm αρχίζουν οι παρενέργειες στο ανθρώπινο σώμα, όπως πονοκέφαλοι, ζαλάδα, ναυτία. Όσο τα ποσοστά ανεβαίνουν οι παρενέργειες γίνονται όλο και χειρότερες και μέσα σε 30 λεπτά ένας άνθρωπος μπορεί να πεθάνει[4].



Εικόνα 33: Ανιχνευτής Καπνού

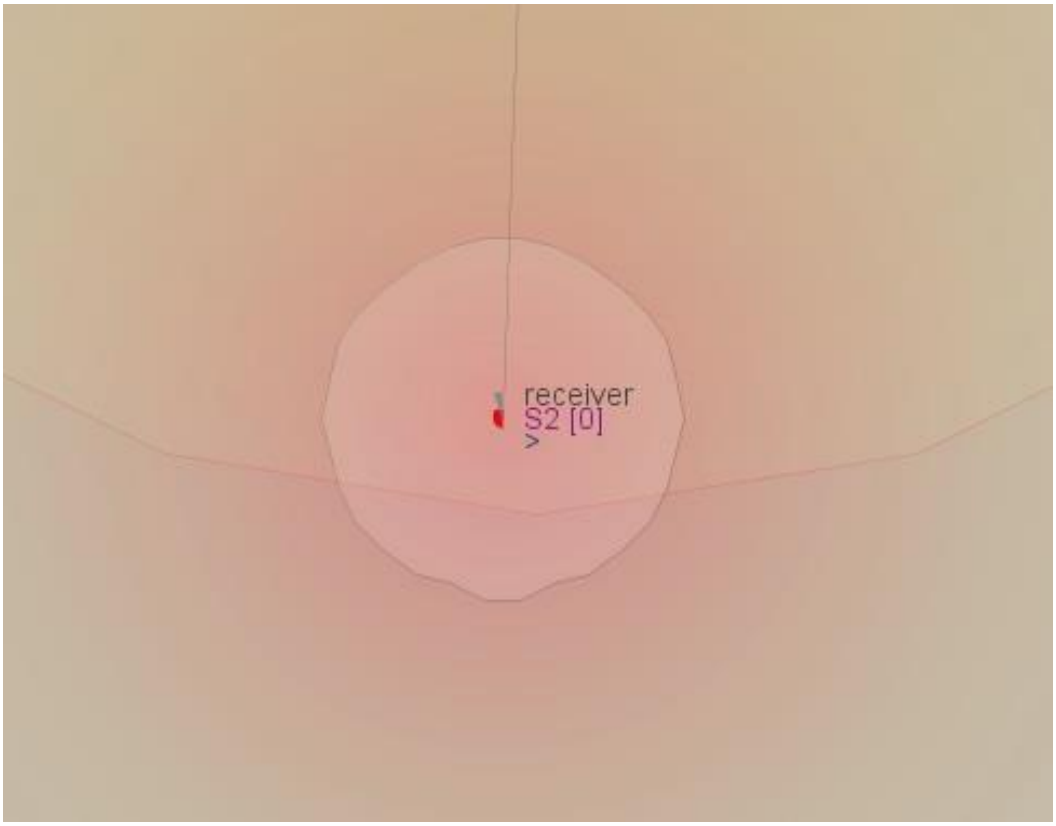
Ακολουθούν δύο συσκευές με id S4, S5 που είναι αισθητήρες, οι οποίες λαμβάνουν τις τιμές από τον ανιχνευτή καπνού για να τις στείλουν στον receiver. Οι δύο αυτοί αισθητήρες (εκτός από την αποστολή των τιμών) είναι επιφορτισμένοι και για τον έλεγχο των τιμών που λαμβάνουν. Σε περίπτωση που για οποιοδήποτε λόγο, λάβουν μια τιμή η οποία ξεπερνάει το επιτρεπτό όριο, μπορούν να επικοινωνήσουν με τον συναγερμό. Ουσιαστικά, πρόκειται για δικλείδες ασφαλείας, αν δεν λειτουργήσει σωστά ο ανιχνευτής καπνού.

[4]https://www.detectcarbonmonoxide.com/co-health-risks/



Εικόνα 34: Αισθητήρες

Παρατηρώντας την Εικόνα 35, βλέπουμε και τον αισθητήρα με id S2 και όνομα receiver που λαμβάνει τις τιμές που στέλνονται από τον ανιχνευτή αερίου. Ο receiver είναι και αυτός συνδεδεμένος με τον συναγερμό. Επιπλέον, μπορεί να σταματήσει τα μηχανήματα παραγωγής, αφού ανιχνευθούν υψηλά ποσοστά.



Εικόνα 35:Receiver

Εκτός από όλα τα παραπάνω υπάρχει και η συσκευή με το όνομα ALARM και id S6 με την ιδιότητα του συναγερμού. Μπορεί να ειδοποιηθεί από όλες τις συσκευές ασφαλείας IoT που βρίσκονται στον χώρο.

Εικόνα 36: Συναγερμός

Το σενάριο έχει ως εξής: Η πρόσβαση που έχει αποκτήσει ο κακόβουλος χρήστης (όπως έχει αναφερθεί παραπάνω), του επιτρέπει να απενεργοποιεί τον συναγερμό και να αλλάζει τις τιμές που καταγράφονται, σύμφωνα με την θέλησή του. Με αυτό τον τρόπο τροποποιεί τις τιμές που στέλνονται στον αισθητήρα 1 με id S4 από τον ανιχνευτή αερίου.

Λόγω του γεγονότος της αυξημένης πρόσβασης που έχει αποκτήσει, κατάφερε (όπως προαναφέραμε) να αλλάξει τις τιμές που λαμβάνει ο αισθητήρας S4. Έτσι, όταν οι τιμές του αερίου έφθασαν σε υψηλά επίπεδα, ο δράστης άλλαξε τις τιμές που λαμβάνουν οι αισθητήρες και ο receiver, με αποτέλεσμα να μην ειδοποιηθούν από τον συναγερμό να εγκαταλείψουν το εργοστάσιο και να μην σταματήσει η παραγωγή. Το αποτέλεσμα αυτής της επίθεσης ήταν οι εργαζόμενοι που βρίσκονταν στο χώρο της παραγωγής εκείνη την στιγμή να βρεθούν νεκροί.

Τα ερωτήματα που προκύπτουν είναι:

- Γιατί δεν ειδοποιήθηκαν από τον ανιχνευτή αερίου;
- Για ποίο λόγο οι αισθητήρες που λογίζονται και ως δικλείδες ασφαλείας δεν σταμάτησαν την παραγωγή;
- Γιατί δεν ειδοποίησε τους εργαζόμενους ο συναγερμός;

Σε αυτά τα ερωτήματα θα προσπαθήσει να δώσει απαντήσεις ο ερευνητής που κάλεσαν οι υπεύθυνοι του εργοστασίου.

6.4.2 Ανάλυση της Προσομοίωσης σύμφωνα με το μοντέλο IoT Based Digital Forensic Model

Όπως και στις προηγούμενες δύο προσομοιώσεις που παρουσιάστηκαν σε αυτήν την διπλωματική εργασία, έτσι και σε αυτήν, θα χρησιμοποιήσουμε ένα μοντέλο εγκληματολογίας που έχει παρουσιαστεί και αναλυθεί. Το μοντέλο των Perumal et al. θα βοηθήσει τον ερευνητή σε αυτήν την υπόθεση.

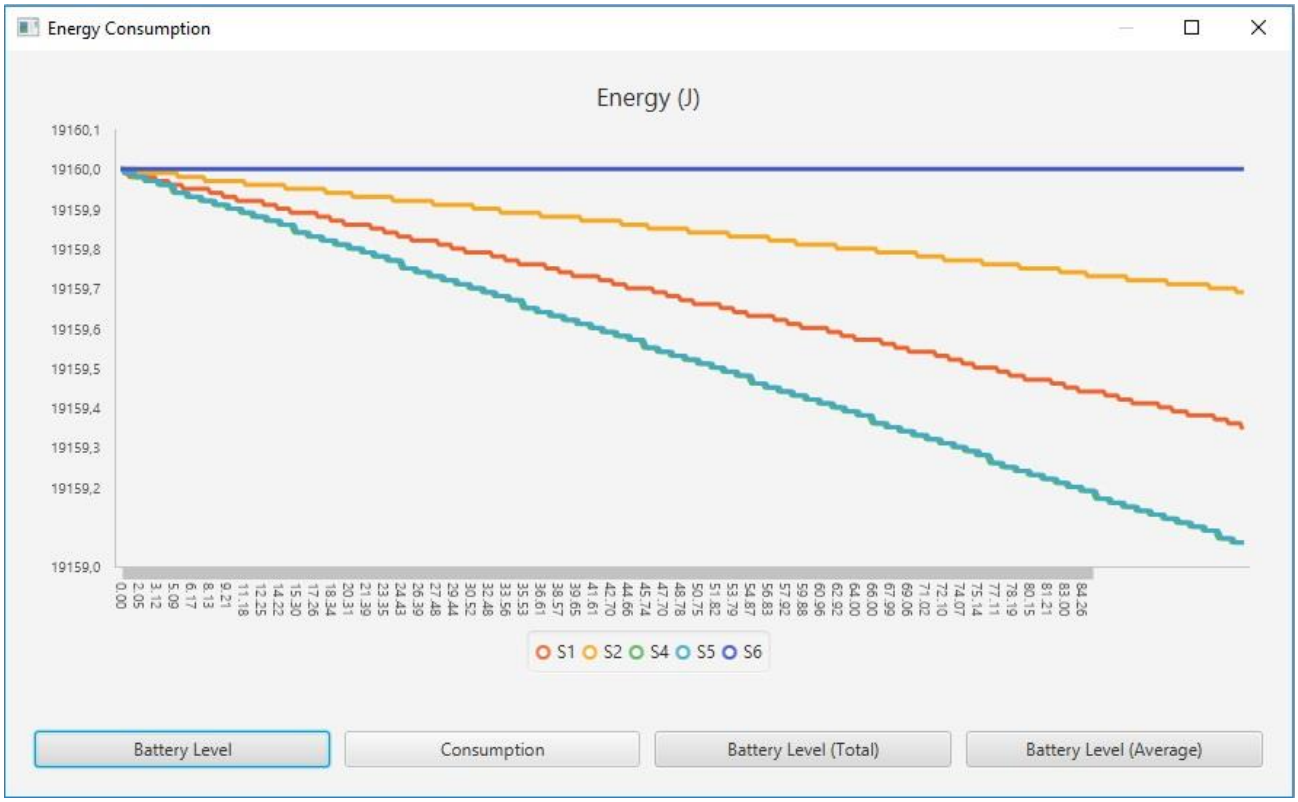
Σύμφωνα με αυτό το μοντέλο ο εγκληματολόγος οφείλει να ξεκινήσει την έρευνά του έχοντας λάβει τις κατάλληλες εξουσιοδοτήσεις (πρόσβαση στον χώρο, στις συσκευές,κτλ) και έχοντας σχεδιάσει τις κινήσεις του.

Στην συνέχεια, έχοντας την πρόσβαση στην παραγωγή, καταγράφει την τοποθεσία των συσκευών στο χώρο. Οι συσκευές IoT συχνά επικοινωνούν μεταξύ τους όπως γίνεται και στο δικό μας σενάριο. Έχοντας βρει τις συσκευές που τον ενδιαφέρουν για την έρευνά του ο ερευνητής προχωράει στην διαλογή. Αυτό σημαίνει πως ταξινομεί τις συσκευές ανάλογα με το πόσο εύθραυστες είναι. Για παράδειγμα, πρώτο του μέλημα είναι να φροντίσει να εξετάσει μία συσκευή η οποία έχει χαμηλή μπαταρία και θα απενεργοποιηθεί σύντομα. Στην δική μας περίπτωση οι συσκευές μας έχουν υψηλά ποσοστά ενέργειας (εικόνα 37).

Ο ερευνητής βρίσκεται στο σημείο όπου θα κατασχέσει τις συσκευές που θεωρεί ότι θα συνδράμουν στην έρευνά του και τις πηγαίνει στο εργαστήριο για ενδελεχή έρευνα. Σημαντικό είναι να καταγράψει την ακριβή ιεραρχία των αποδεικτικών στοιχείων (chain of custody), από ποίο σημείο ακριβώς απέσπασε μια συσκευή, πού θα την οδηγήσει, κτλ. Αυτό θα πρέπει να συμβεί για όλες τις συσκευές.

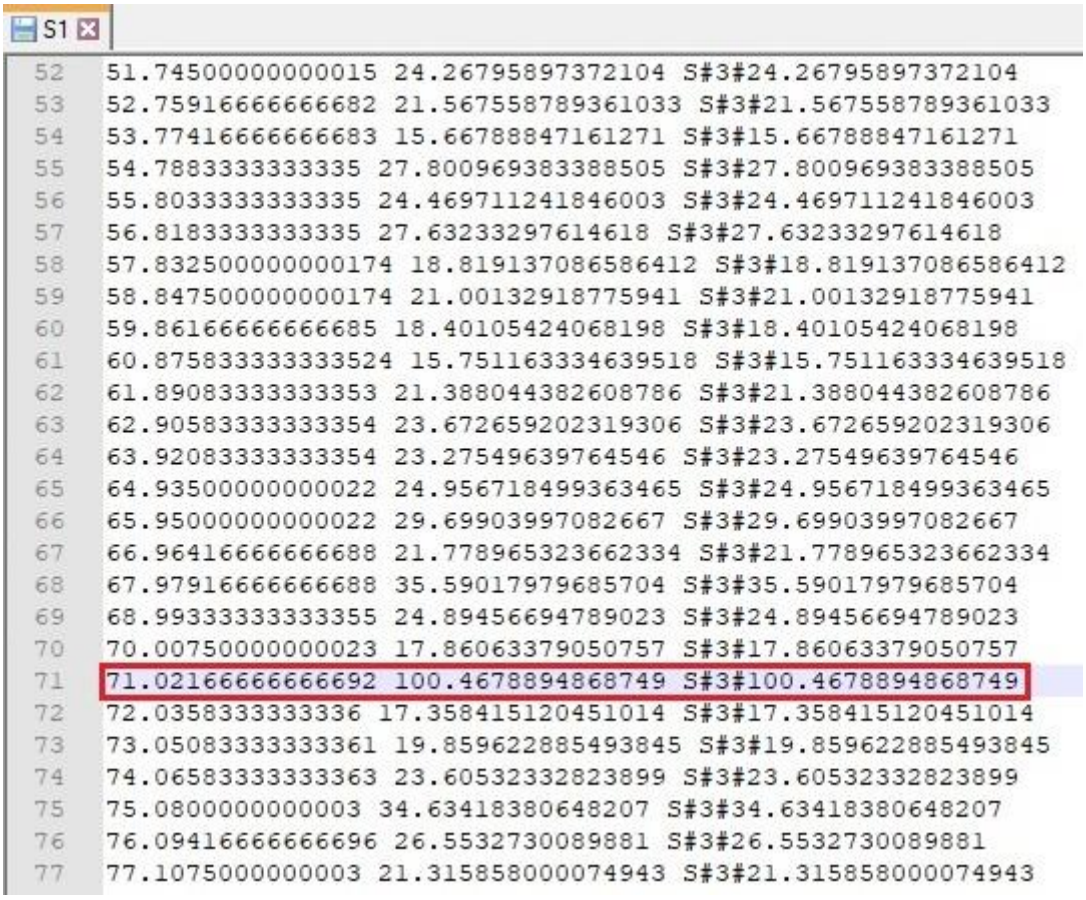
Το συγκεκριμένο μοντέλο απαιτεί σε αυτό το σημείο την εργαστηριακή ανάλυση των συσκευών. Γι' αυτό και ο ερευνητής αναλύει την κάθε συσκευή ψάχνοντας για χρήσιμα δεδομένα.

Η συσκευή που ξεκινάει την ανάλυσή του είναι ο ανιχνευτής αερίου με id S1. Έχει ήδη παρατηρήσει πως η μπαταρία του είναι σε υψηλά ποσοστά, άρα αποκλείει το γεγονός πως κάτι συνέβη στην ενέργεια του, την στιγμή του άτυχου συμβάντος, όπως φαίνεται και στην Εικόνα 37.



Εικόνα 37: Επίπεδα Μπαταρίας Συσκευών

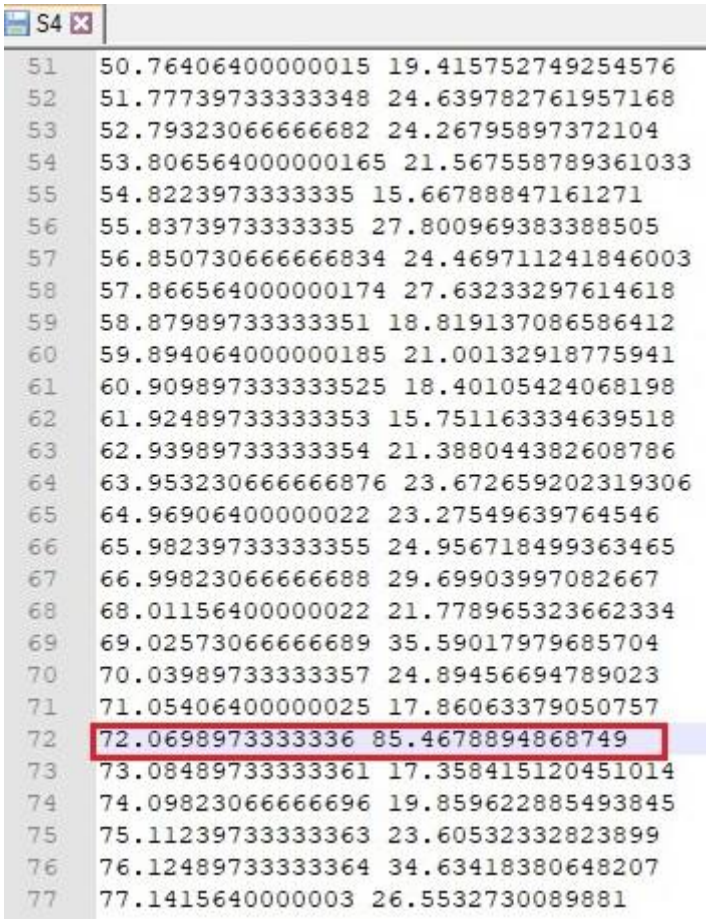
Επόμενο βήμα είναι εξεταστούν τα αρχεία καταγραφής (log) του ανιχνευτή για τυχόν χρήσιμα στοιχεία. Πράγματι, ο ερευνητής βρίσκει κάποια στοιχεία που θα του είναι ωφέλιμα για την έρευνά του. Παρατηρεί λοιπόν πως στο log που διατηρεί η συσκευή, υπάρχει μια τιμή στο χρονικό σημείο 71.02166666666692 που δεν είναι φυσιολογική και δεν έχει σχέση με τις υπόλοιπες (εικόνα 38). Αυτή η τιμή είναι η 100.4678894868749.



Εικόνα 38: Αρχείο Καταγραφής S1

Έχοντας αυτό το στοιχείο πλέον ο ερευνητής ξέρει το χρονικό σημείο που ξεκίνησε η διαρροή υψηλών επιπέδων αερίου στο χώρο της παραγωγής. Αυτό όμως που προκαλεί ακόμα ερωτήματα είναι για ποιο λόγο δεν ειδοποίησε η συσκευή τον συναγερμό και τους εργαζόμενους. Ο κακόβουλος χρήστης με τη χρήση κατάλληλου κώδικα διέκοψε την επικοινωνία του ανιχνευτή με τον συναγερμό. Ακόμα, απενεργοποίησε την δυνατότητα της συσκευής να ειδοποιήσει.

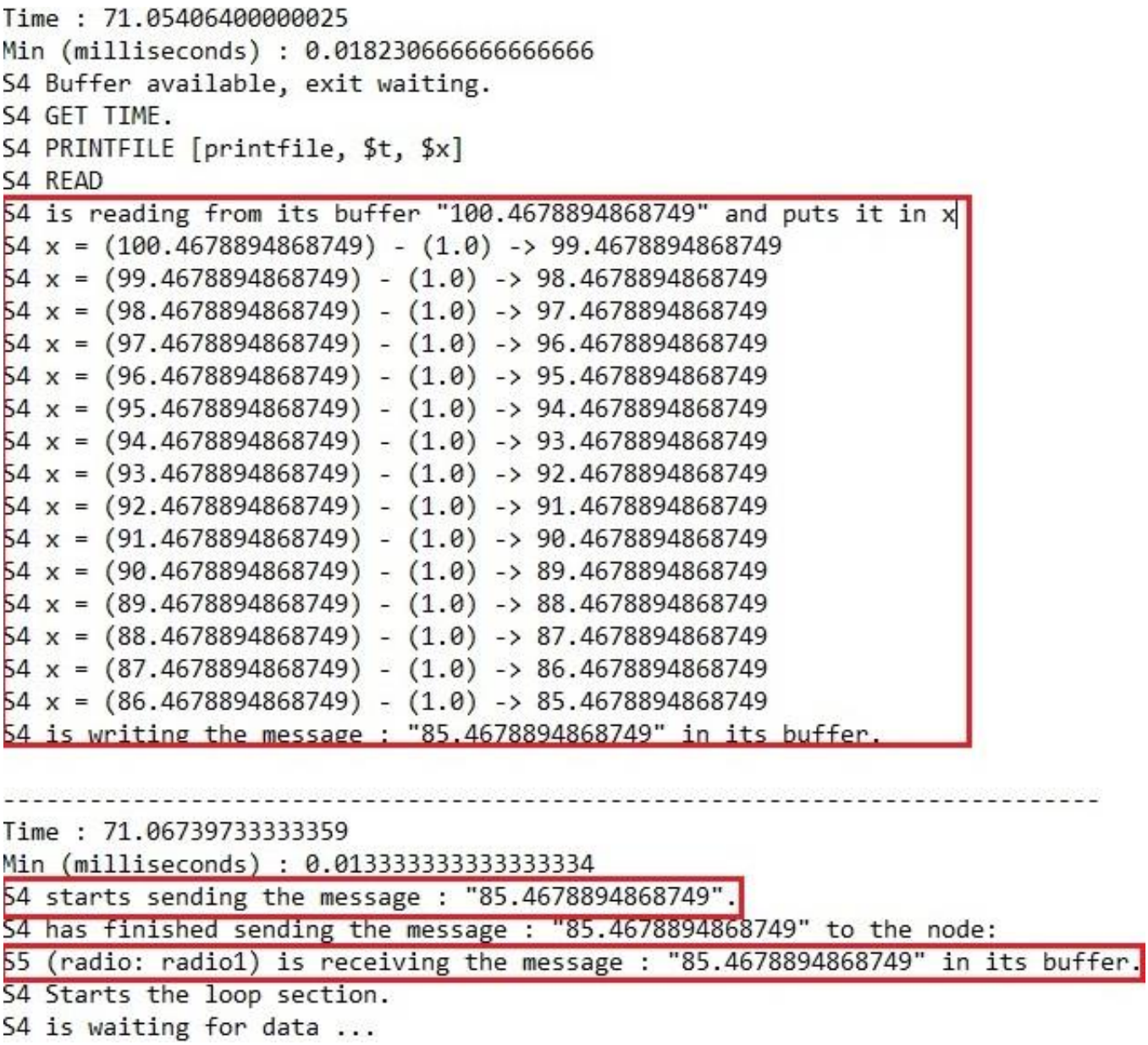
Περνώντας στην επόμενη συσκευή που είναι αυτή με id S4 και γνωρίζοντας πως δεν αντιμετώπισε προβλήματα ενέργειας (Εικόνα 37), ο ερευνητής στρέφει την έρευνα του στο αρχείο καταγραφής της συσκευής. Σε αυτό, πέρα από τις φυσιολογικές τιμές, ψάχνει για την χρονική στιγμή 71.02166666666692 ή ακόμα και για όμορες τιμές και εκεί βρίσκει το πιο σημαντικό του στοιχείο (Εικόνα 39).



Εικόνα 39:Αρχείο Καταγραφής S4

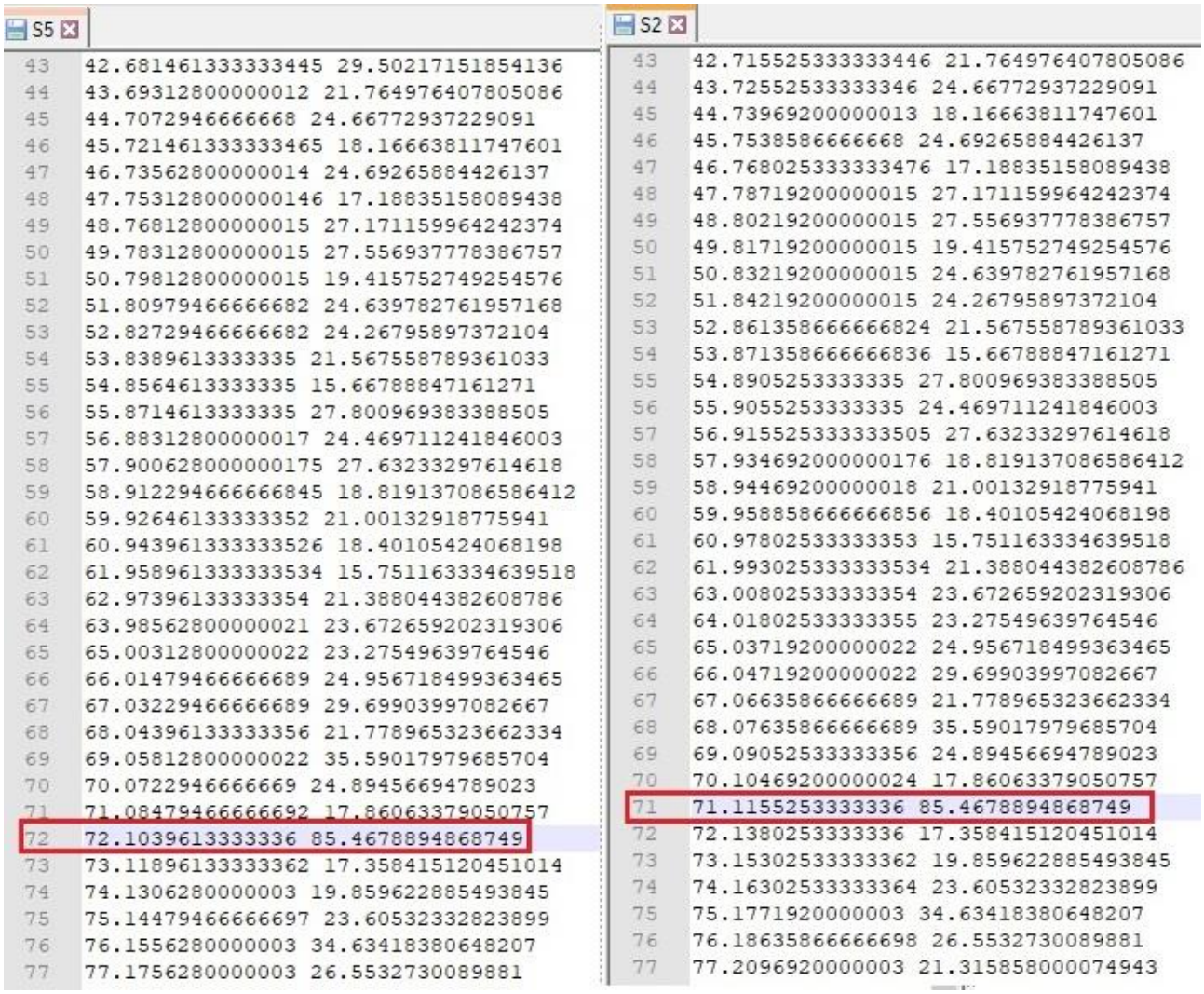
Ενώ οι προηγούμενες τιμές μέχρι περίπου το χρονικό σημείο 71.05406400000025 είναι ακριβώς ίδιες, στο χρονικό σημείο 72.0698973333336 παρατηρείται μία τιμή που δεν είναι φυσιολογική αλλά όχι ίδια με την προηγούμενη που στάλθηκε από τον ανιχνευτή S1. Ο ερευνητής καταγράφει την τιμή 85.4678894868749.

Επόμενη κίνηση του εγκληματολόγου είναι να ερευνήσει στο log του δικτύου για περαιτέρω στοιχεία. Από αυτό το αρχείο καταγραφής (Εικόνα 40), αντιλαμβάνεται πως ο κακόβουλος χρήστης κατάφερε να τροποποιήσει τις τιμές που έστελνε ο ανιχνευτής αερίου στον αισθητήρα S4, όταν τα επίπεδα αερίου ήταν υψηλά.



Εικόνα 40:Αρχείο Καταγραφής Δικτύου

Προχωρώντας στην ανάλυσή του ο ερευνητής περνάει στους αισθητήρες S5, S2 όπου και παρατηρεί πως κοντά στην χρονική στιγμή που παρατηρήθηκε η αλλαγή της τιμής από τον κακόβουλο χρήστη, στα αρχεία καταγραφής τους είναι καταγεγραμμένη η λάθος τιμή (Εικόνα 41). Αυτό εξάλλου φαίνεται και από την Εικόνα 39, που ο αισθητήρας S4 στέλνει την τροποποιημένη τιμή στον S5.



Εικόνα 41:Αρχεία Καταγραφής S5, S2

Σύμφωνα με το μοντέλο των Perumal et al. ο ερευνητής έχει τα αποτελέσματα και μπορεί να τα παρουσιάσει ως αποδείξεις στο δικαστήριο. Τελευταία διεργασία του μοντέλου είναι η αποθήκευση της υπόθεσης μαζί με όλα τα ευρήματα για τυχόν χρήση τους στο μέλλον. Όπως και στο προηγούμενο σενάριο, έτσι και σε αυτό χρησιμοποιήθηκαν συσκευές που στη βιομηχανία αλλά και σε οικίες τυγχάνουν ευρείας χρήσης.

Συμπεράσματα

Οι εξελίξεις στον ευρύτερο χώρο της πληροφορικής μέρα με την μέρα αυξάνονται, ωστόσο ταυτόχρονα υπάρχει και αύξηση των κακόβουλων ενεργειών και έτσι η ανάγκη για προστασία είναι ιδιαίτερα μεγάλη. Είναι γεγονός, πως στην εποχή μας δίνεται περισσότερο βάρος στην λειτουργικότητα, στο περιβάλλον και την χρηστικότητα μια εφαρμογής ή μιας συσκευής του IoT, αλλά όχι τόσο στα ζητήματα ασφαλείας.

Στα πλαίσια αυτής της διπλωματικής έγινε η προσπάθεια να καλυφθούν οι βασικές αρχές της Ψηφιακής Εγκληματολογίας και να τονιστεί η σημαντικότητα των Ψηφιακών Πειστηρίων. Αναλύθηκαν τα βασικά μοντέλα που ένας ερευνητής μπορεί να χρησιμοποιήσει στην Ψηφιακή Εγκληματολογία κατά την διάρκεια μιας έρευνας, όπως και οι προκλήσεις που μπορεί να συναντήσει. Ακόμα, αναδείχθηκαν τα πιο δημοφιλή εργαλεία που χρησιμοποιούνται στον τομέα αυτόν.

Ο αναγνώστης αντιλαμβάνεται πως το IoT είναι πολύ σημαντικό και αποτελεί μια επανάσταση, αφού αν εκμεταλλευτεί σωστά τα χαρακτηριστικά του μπορεί να τον ωφελήσει στην καθημερινότητά του και όχι μόνο. Από την άλλη πλευρά όμως, οι προκλήσεις ασφάλειας είναι μεγάλες και οι κακόβουλοι χρήστες τις εκμεταλλεύονται προκειμένου να ωφεληθούν με κάθε τρόπο.

Ο αλματώδεις ρυθμός που εξελίσσεται η επιστήμη του IoT και η φύση των συσκευών, απαιτούν την χρήσης της Ψηφιακής Εγκληματολογίας στο περιβάλλον του IoT. Επιπλέον, παρουσιάστηκαν οι προκλήσεις που μπορεί ένας εγκληματολόγος να συναντήσει στο περιβάλλον του Διαδικτύου των Πραγμάτων, ώστε να είναι σε θέση να αναγνωρίσει και να αποσπάσει τις σημαντικότερες πληροφορίες. Εκτός από αυτά, είναι ιδιαίτερα σημαντικό να γνωρίζουμε τις διαφορές ανάμεσα στην Ψηφιακή Εγκληματολογία και στην Εγκληματολογία στο Διαδίκτυο των Πραγμάτων. Επίσης, παρουσιαστήκαν και αναλύθηκαν τα μοντέλα εγκληματολογίας που μπορεί να συναντήσει κάποιος στην βιβλιογραφία.

Στο τελευταίο κεφάλαιο έγιναν τρεις προσομοιώσεις με τη χρήση του CupCarbon. Μέσω των προσομοιώσεων αυτών δοκιμάστηκε ο προσομοιωτής CupCarbon, όπου είναι μια πλατφόρμα που μπορεί ο χρήστης να σχεδιάσει μια έξυπνη πόλη και Ασύρματα Δίκτυα Αισθητήρων. Μέσα από τα τρία αυτά σενάρια είδαμε πώς ένας ερευνητής πρέπει να ελέγχει τον τόπο του εγκλήματος προσεκτικά ώστε να εντοπίζει τις συσκευές που θα τον βοηθήσουν στην έρευνά του, καθώς και τον τρόπο κατά τον οποίο θα συμπεριφέρεται σε αυτές τις συσκευές, για να μην χαθούν χρήσιμα δεδομένα. Στα τρία αυτά σενάρια χρησιμοποιήθηκαν τα μοντέλα εγκληματολογίας που παρουσιάστηκαν στο πέμπτο κεφάλαιο για την ανακάλυψη των Ψηφιακών Πειστηρίων που θα ωφελήσουν στην έρευνα.

Τα πλεονεκτήματα του CupCarbon είναι πολλά. Ειδικότερα για τον σχεδιασμό μιας έξυπνης πόλης ή ενός έξυπνου κτιρίου. Ακόμα πιο χρήσιμο είναι όταν ο χρήστης θέλει να δοκιμάσει ένα Ασύρματο Δίκτυο Αισθητήρων. Στις προσομοιώσεις που έλαβαν χώρα σε τούτη την διπλωματική το CupCarbon ανταποκρίθηκε με μεγάλη επιτυχία. Το χαρακτηριστικό να δημιουργούνται αρχεία καταγραφής (log) σε κάθε αισθητήρα αποδείχθηκε ιδιαίτερα ευεργετικό, αφού ήταν ένα πάρα πολύ ωφέλιμο εργαλείο, ώστε να φτάσουμε σε κάποιο συμπέρασμα για κάθε μια προσομοίωση. Πέραν αυτού και στις πραγματικές έρευνες όπως διαπιστώσαμε, τα αρχεία καταγραφής (log) έχουν κυρίαρχο ρόλο κατά την διάρκεια μιας έρευνας.

Αφετέρου, θα αποτελούσε χρήσιμη βελτίωση αν οι κατασκευαστές του εν λόγω προσομοιωτή προσέθεταν κάποιους αισθητήρες οι οποίοι θα προσομοίωναν αντικείμενα που χρησιμοποιούμε στην καθημερινότητά μας, για παράδειγμα έξυπνες κλειδαριές, wearables, έξυπνους ανιχνευτές, έξυπνα αυτοκίνητα, κτλ. Ο λόγος που θα ήταν καλό να γίνει αυτό, είναι πως οι συσκευές του IoT παρουσιάζουν ποικίλουν. Επιπρόσθετα, ένα ενδιαφέρον χαρακτηριστικό θα ήταν αν θα υπήρχε η δυνατότητα το CupCarbon να συνεργάζεται και με κάποια άλλα λογισμικά όπως είναι το EnCase, το Forensic Toolkit, το The Sleuth Kit,το Digital Forensics Framework κ.α.

Γίνεται αντιληπτό πως εξαιτίας της συνεχής ανάπτυξης των συσκευών του IoT η παραδοσιακή Ψηφιακή Εγκληματολογία ίσως δεν είναι αρκετή κατά την διεξαγωγή των ερευνών. Κρίνεται επιτακτική η ανάγκη της εκμετάλλευσης αυτών των μοντέλων που παρουσιάστηκαν σε αυτήν την διπλωματική εργασία από τους ερευνητές, της συνεχούς βελτιστοποίησης των υπαρχόντων ή και τη δημιουργίας καινούργιων μοντέλων αν αυτό είναι απαραίτητο.

Τέλος, προτείνεται η προσθήκη στο πρόγραμμα σπουδών ή η ενίσχυση των συναφών μαθημάτων ασφαλείας στα εκπαιδευτικά ιδρύματα, με επίκεντρο την Ψηφιακή Εγκληματολογία και την Εγκληματολογία στο Διαδίκτυο των Πραγμάτων. Είναι καλό να δοθεί έμφαση στο πρακτικό κομμάτι μέσω προσομοιώσεων, διότι όπως διαπιστώθηκε η επιστήμη της Ψηφιακής Εγκληματολογίας έχει ανάγκη από επιστήμονες που γνωρίζουν σε βάθος το αντικείμενο.

Βιβλιογραφία

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

Ashton, K. (2009). That ‘internet of things’ thing. *RFID journal*, 97-114.

Atamli, A. W. (2014). Threat-based security analysis for the internet of things. In Secure Internet of Things (SIoT). Στο I. Workshop (Επιμ.). (σσ. 35-43). IEEE.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, σσ. 1-20.

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

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet.* Academic press.

Coetzee, L. &. (2012). *Inclusion through the Internet of Things. In Assistive Technologies.* InTech.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). *Internet of Things security and forensics: Challenges and opportunities.*

Hegarty, R. L. (2014). Digital Evidence Challenges in the Internet of Things. σσ. 163-172.

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

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

Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for internet of things (iot). *In Future Internet of Things and Cloud* (σσ. 356-362). IEEE.

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

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT). Στο 1. I. Conference (Επιμ.). (σσ. 257-260). IEEE.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016).* Florida, USA.

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

Muniswamy-Reddy, K. K. (2006). Provenance-aware storage systems. *In USENIX Annual Technical Conference* (σσ. 43-56). General Track.

Oriwoh, E. a. (2017). *"Internet of Things: The argument for smart forensics." The Internet of Things: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice.*

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of things forensics: Challenges and approaches. Στο 9. I. Conference (Επιμ.), *In Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)* (σσ. 608-615). IEEE.

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

Patel, K. K., & Patel, S. M. (2016). *Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges." International Journal of Engineering Science and Computing.*

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

Perumal, S., Norwawi, N. M., & Raman, V. (2015). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. Στο F. I. Conference (Επιμ.), *Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology* (σσ. 19-23). IEEE.

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

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

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

Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., & Du, H.-Y. (2010). Research on the architecture of Internet of Things. *In Advanced Computer Theory and Engineering (ICACTE), 3rd International Conference.Vol. 5*, σσ. V5-484. IEEE.

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

Zawoad, S., & Hasan, R. (2015). Faiot: Towards building a forensics aware eco system for the internet of things. *Faiot: Towards building a forensics aware eco system for the internet of things* (σσ. 279-284). IEEE.

Ηλεκτρονικές Διευθύνσεις

Accessdata. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://accessdata.com/

Amazon. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://developer.amazon.com/echo

APACHE hadoop. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://hadoop.apache.org/

Arduino. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.arduino.cc/

August. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://august.com/products/doorbell-camera/

AWAIR. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://getawair.com

Blackbagtech Technologies. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.blackbagtech.com

Bussiness Insider. (2016, Δεκέμβριος 11). Retrieved Σεπτέμβριος 25, 2018, from https://www.businessinsider.com/companies-making-driverless-cars-by-2020-2016-11#uber-released-its-autonomous-cars-in-pittsburgh-as-part-of-a-pilot-program-in-september-2

CAINE. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.caine-live.net/

CargoSense. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from http://www.cargosense.com/

Coetzee, L. &. (2012). *Inclusion through the Internet of Things. In Assistive Technologies.* InTech.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). *Internet of Things security and forensics: Challenges and opportunities.*

deft. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from http://www.deftlinux.net/

Digital Forensics. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://digital-forensics.sans.org/

Digital Forensics Framework. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from http://digitalforensicsframework.blogspot.com/

Encase Forensic. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.guidancesoftware.com/encase-forensic

Ericsson. (2016, Ιούνιος 1). Retrieved Σεπτέμβριος 25, 2018, from https://www.ericsson.com/en/press-releases/2016/6/internet-of-things-to-overtake-mobile-phones-by-2018-ericsson-mobility-report

Garmin. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://explore.garmin.com/en-IE/forerunner/

Gartner. (2013, Νοέμβριος 11). Retrieved Σεπτέμβριος 2018, 2018, from https://www.gartner.com/newsroom/id/2621015

Honeywell. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://smarthomesecurity.honeywell.com/

https://www.guidancesoftware.com/encase-forensic . (n.d.). Retrieved 218, from https://www.guidancesoftware.com/encase-forensic

MSAB. (n.d.). Retrieved Σεπτεμβριος 25, 2018, from https://www.msab.com/products/xry/

NFC. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://nfc-forum.org/what-is-nfc/about-the-technology/

NIST. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://toolcatalog.nist.gov/index.php: https://toolcatalog.nist.gov/populated_taxonomy/index.php

PASS. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://syrah.eecs.harvard.edu/pass

Roost. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.getroost.com/

Samsung. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.samsung.com/us/smart-home/smartthings/

Sleuthkit. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.sleuthkit.org/index.php

X-Ways. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from http://www.x-ways.net/forensics/

Magnetforensics. (n.d.). Retrieved Σεπτέμβριος 25, 2018, from https://www.magnetforensics.com/magnet-ief/

ΣΕΠΕ. (2015, Δεκεμβρίου 22). Retrieved Σεπτέμβριος 22, 2018, from http://www.sepe.gr/gr/information/news/article/4844412/250000-unique-apps-iot-will-be-worldwide-till-2020/