ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

««Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ψηφιακή Εγκληματολογία των Συστημάτων μη Επανδρωμένων Αεροσκαφών** **Drone Forensics**
Ονοματεπώνυμο Φοιτητή	**Γεώργιος Καμπάς**
Πατρώνυμο	**Γρηγόριος**
Αριθμός Μητρώου	**ΜΠΚΣΑ 18010**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Νοέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Πατσάκης Κωνσταντίνος Αναπληρωτής Καθηγητής	Αλέπης Ευθύμιος Αναπληρωτής Καθηγητής	Σακκόπουλος Ευάγγελος Αναπληρωτής Καθηγητής

Ευχαριστίες

«Το παρόν έγγραφο με τίτλο: «Drone Forensics», πραγματοποιήθηκε στο πλαίσιο της εκπόνησης της διατριβής για το πρόγραμμα μεταπτυχιακών σπουδών «Κατανεμημένα Συστήματα, Ασφάλεια Και Αναδυόμενες Τεχνολογίες Πληροφορίας» του τμήματος Πληροφορικής του Πανεπιστημίου Πειραιά.

Με την ολοκλήρωση της μεταπτυχιακής διατριβής μου, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της. Ευχαριστώ ιδιαιτέρως τον καθηγητή μου, Δρ. Κωνσταντίνο Πατσάκη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, την επιστημονική του καθοδήγηση, τις υποδείξεις του, την υπομονή και την επιμονή του, καθώς και για τη συνεχή του υποστήριξη.

Περίληψη

Η παρούσα διατριβή πραγματεύεται την δημιουργία ενός εύχρηστου και επεκτάσιμου αλγορίθμου που σκοπεύει να συνεισφέρει στην ψηφιακή εγκληματολογία των Συστημάτων μη Επανδρωμένων Αεροσκαφών (ΣμηΕΑ), μέσω της εύκολης και γρήγορης ανάλυσης αρχείων καταγραφής πτήσης. Ο αλγόριθμος υλοποιήθηκε σε γλώσσα Python και αποτελεί επέκταση των δυνατοτήτων του αλγόριθμου Gryphon, ο οποίος έχει την δυνατότητα να αναλύει δεδομένα τύπου .bin. Ο αλγόριθμος υποστηρίζει δύο τρόπους λειτουργίας: την ανάλυση δεδομένων τύπου .bin μέσω του αλγορίθμου Gryphon και την ανάλυση δεδομένων τύπου .dat προερχόμενων από ΣμηΕΑ της κατασκευάστριας εταιρίας DJI. Η ανάλυση πραγματοποιήθηκε μέσω του parser DatCon, και η γεωγραφική αναπαράσταση της πτήσης με την χρήση του χάρτη αναφοράς Basemap.

Abstract

The current dissertation focuses on the creation of an easy-to-use and scalable algorithm that contributes to the Drone Digital Forensics, through the easy and fast analysis of flight log files. The algorithm was implemented in Python and constitutes the extension of the Gryphon's capabilities, which has the ability to analyse .bin log files. The algorithm supports 2 modes of operation: the analysis of .bin log files through the Gryphon algorithm and the analysis of .dat log files derived from DJI drones. The analysis was performed utilising the DatCon parser, while the geographic representation of the flight was implemented using the Basemap reference map.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

Εισαγωγή

Ο τομέας των μικρών Συστημάτων μη Επανδρωμένων Αεροσκαφών (ΣμηΕΑ), επίσης γνωστά και ως Drones, έχει βιώσει ραγδαία ανάπτυξη εδώ και αρκετά χρόνια, τόσο για όσους τα χρησιμοποιούν για ψυχαγωγία όσο και αναφορικά με τους επαγγελματίες που χρησιμοποιούν τα ΣμηΕΑ ως μέσα για φωτογράφηση, βιντεοσκόπηση, χαρτογράφηση, επιθεώρηση, κ.ο.κ. Οι δείκτες εσόδων από αγορές ΣμηΕΑ συνεχώς αυξάνονται, το οποίο αναμφίβολα θα οδηγήσει στην αυξημένη και πιο μαζική χρήση των ΣμηΕΑ σε τομείς της καθημερινότητας.

Η δημοτικότητα όμως που έχουν αποκτήσει τα ΣμηΕΑ, έχει επιφέρει και τους αντίστοιχους κινδύνους και απειλές που συνδέονται άμεσα με την αμελή ή κακόβουλη χρήση των ΣμηΕΑ. Εκτός από ατυχήματα που ενδέχεται να συμβούν, όπως και με κάθε καινοτόμα ψηφιακή συσκευή, οι κακόβουλοι χειριστές είναι σαφές ότι προσπαθούν να εκμεταλλευτούν τα τρωτά σημεία ή ακόμα και τις δυνατότητες των ΣμηΕΑ για να διευκολύνουν τις εγκληματικές ή τρομοκρατικές ενέργειές τους. Με την αύξηση της πιθανότητας συμμετοχής των ΣμηΕΑ σε τέτοιες ενέργειες καθώς και σε ατυχήματα, προκύπτει αναμφισβήτητα η ανάγκη για την ανάπτυξη ενός «νέου» και ξεχωριστού τομέα ψηφιακής εγκληματολογικής που αφορά αποκλειστικά τα ΣμηΕΑ.

Ο τομέας των Drone Forensics είναι σχετικά λιγότερο ανεπτυγμένος, συγκριτικά με άλλες έρευνες που αφορούν «δημοφιλείς» ψηφιακές συσκευές και τεχνολογίες όπως τα έξυπνα κινητά τηλέφωνα (π.χ. Android, iOS, κ.ο.κ.), ή οι Η/Υ (Computer Forensics). Από το 2015 και μετά έχουν δημοσιευθεί σχετικές έρευνες που αφορούσαν την μελέτη των βασικών στοιχείων της ψηφιακής εγκληματολογίας των ΣμηΕΑ, την προτεινόμενη διαδικασία απόκτησης δεδομένων, καθώς το μοντέλο του ΣμηΕΑ στο οποίο έγινε η ανάλυση. Οι υφιστάμενες προσεγγίσεις ψηφιακής εγκληματολογίας των ΣμηΕΑ ακολουθούν τις οδηγίες ή παραλλαγές των οδηγιών αυτών που δημοσιεύτηκαν από το Εθνικό Ινστιτούτο Επιστήμης και Τεχνολογίας των Ηνωμένων Πολιτειών Αμερικής (NIST) «Οδηγίες για την Εγκληματολογία Κινητών Συσκευών».

Ως εκ τούτου, σε αυτή την μελέτη, εξετάζουμε την υπάρχουσα βιβλιογραφία αναφορικά με την ψηφιακή εγκληματολογία των ΣμηΕΑ, καταγράφουμε τους πιθανούς τύπους των δεδομένων και τις τοποθεσίες αποθήκευσης αυτών και σημειώνουμε τα εργαλεία digital forensics που υπάρχουν διαθέσιμα και βοηθούν σε τέτοιες μελέτες. Έχοντας ως βάση τις οδηγίες που δημοσίευσε η Interpol και αφορούν τα Digital Drone Forensics [42], προτείνουμε μια ψηφιακή εγκληματολογική διαδικασία επικεντρωμένη στην έρευνα των δεδομένων πτήσης των ΣμηΕΑ, αναπτύσσοντας έναν αλγόριθμο ικανό να εξάγει και αναλύσει δεδομένα από ΣμηΕΑ διαφορετικών κατασκευαστών, μοντέλων και τύπων. Αυτός ο αλγόριθμος έχει δημιουργηθεί για να υποστηρίξει την διαδικασία των Digital Drone Forensics και για να εξάγει χρήσιμα συμπεράσματα κατά τα στάδια της εξέτασης και ανάλυσης των δεδομένων που παράγονται κατά την πτήση ενός ΣμηΕΑ.

Εισαγωγή στην τεχνολογία των Συστημάτων μη Επανδρωμένων Αεροσκαφών

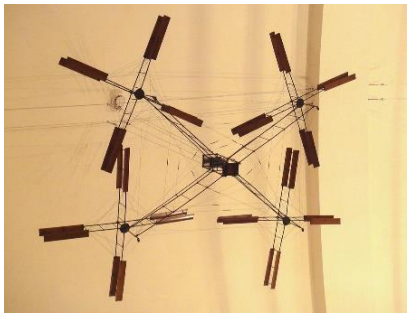
Τα Συστήματα μη Επανδρωμένων Αεροσκαφών (ΣμηΕΑ) είναι η επίσημη ορολογία που έχει δοθεί στα εν λόγω συστήματα από την Υπηρεσία Πολιτικής Αεροπορίας (Υ.Π.Α.) της Ελλάδας, τα οποία όμως φέρουν εκτός αυτού του τίτλου, δεκάδες άλλους, είτε ελληνικούς είτε αγγλικούς, για να περιγράψουν ουσιαστικά την ίδια τεχνολογία ή πιο σωστά μέρος αυτής. Κάποιοι από αυτούς τους όρους είναι:

- ΣμηΣΑ – Σύστημα μη Στελεχωμένων Αεροσκαφών
- ΜΕΑ – Μη Επανδρωμένο Αεροσκάφος, ο όρος αναφέρεται αποκλειστικά στο μη επανδρωμένο όχημα και όχι στο πλήρες σύστημα (σταθμός απομακρυσμένου ελέγχου, κτλ.) σε αντίθεση με τους όρους ΣμηΕΑ και ΣμηΣΑ
- UAS – Unmanned Aerial System
- RPAS – Remotely Piloted Aircraft System
- ROAS – Remotely Operated Aircraft System
- UAV – Unmanned Aerial Vehicle, ο όρος αναφέρεται μόνο στο μη επανδρωμένο όχημα και όχι στο πλήρες σύστημα (σταθμός απομακρυσμένου ελέγχου, κτλ.) σε αντίθεση με τον όρο “UAS”.
- sUAV – Small Unmanned Aerial Vehicle, ο όρος «Small» αναφέρεται κυρίως στο μέγεθος του ΣμηΕΑ
- Drone, ο όρος αναφέρεται σε μη επανδρωμένο εναέριο ή υποβρύχιο όχημα (unmanned aerial or underwater vehicle)

Για λόγους ευκολίας και ομοιογένειας, στην παρούσα μελέτη θα χρησιμοποιηθεί ο όρος ΣμηΕΑ, ο οποίος αναφέρεται στο αεροσκάφος, στον επίγειο σταθμό ελέγχου και στην επικοινωνία μεταξύ αυτών.

1.1 Σύντομη ιστορική αναδρομή

Η ιδέα των ΣμηΕΑ χρονολογείται από το 1849, όταν η Αυστρία επιτέθηκε στη Βενετία χρησιμοποιώντας μη επανδρωμένα μπαλόνια για να μεταφέρουν εκρηκτικά [1]. Οι αυστριακές δυνάμεις, που πολιορκούσαν τη Βενετία εκείνη την εποχή, εκτόξευσαν περίπου διακόσια (200) από αυτά τα μπαλόνια πάνω από την πόλη, το καθένα από τα οποία μετέφερε περίπου δώδεκα (12) κιλά εκρηκτική ύλη. Η συγκεκριμένη αποστολή αυτών των «πρώιμων ΣμηΕΑ» θα μπορούσε να χαρακτηριστεί ως αποτυχημένη, καθώς οι αλλαγές στην κατεύθυνση του ανέμου, οδήγησαν τα μπαλόνια εκτός πορείας με αποτέλεσμα ελάχιστα από αυτά να βρουν τον στόχο τους.



Εικόνα 1: Πρωτότυπο γυροπλάνο αδελφών Jacques and Louis Bréguet
Πηγή: Breguet Aviation / Wikimedia Commons

Ακολούθως, υπήρξαν αρκετές προσπάθειες ανάπτυξης της εν λόγω τεχνολογίας, με κάποιες από τις πιο σημαντικές να είναι αυτές των αδελφών Jacques and Louis Bréguet [2], οι οποίοι με την ανάπτυξη του πρωτότυπου γυροπλάνου, ουσιαστικά έθεσαν τις βάσεις για την υιοθέτηση της τεχνολογίας του ελικοπτέρου, καθώς και των κοινών εμπορικών ΣμηΕΑ, των πολυκοπτέρων.

Αρκετά αργότερα, το πρώτο αεροσκάφος σταθερής πτέρυγας, ικανό να επιχειρεί δίχως πιλότο, αναπτύχθηκε το 1916, αμέσως μετά την απαρχή του Α' Παγκοσμίου Πολέμου, με το όνομα του να μένει στην ιστορία ως Ruston Proctor Aerial Target [3]. Τα συγκεκριμένα στρατιωτικά ΣμηΕΑ αναπτύχθηκαν από τον Βρετανό μηχανικό Archibald Low και την ομάδα του και

χρησιμοποιούσαν ένα σύστημα ράδιο-καθοδήγησης. Το αεροσκάφος που ανέπτυξαν εκτοξεύτηκε για πρώτη φορά από το πίσω μέρος ενός φορτηγού χρησιμοποιώντας ειδικά σχεδιασμένο μηχανισμό με πεπιεσμένο αέρα. Παρόλο που η τεχνολογία που αναπτύχθηκε από τον Low ήταν αρκετά καινοτόμα για την εποχή, δίνοντάς του μάλιστα και το προσωνύμιο «ο πατέρας των συστημάτων ράδιο-καθοδήγησης», το έργο του δεν υιοθετήθηκε από τον βρετανικό στρατό μετά τον πόλεμο.

Εικόνα 2: Πρωτότυπο μοντέλο Kettering Bug
Πηγή: National Museum of the United States Air Force

Στα επακόλουθα χρόνια του Α' Παγκοσμίου Πολέμου, ο στρατός των Η.Π.Α. θέλησε να αναπτύξει μία «εναέρια τορπίλη» και ως εκ τούτου κατασκεύασε το Kettering Bug [4], το οποίο χρησιμοποιούσε γυροσκόπια και μπορούσε να εκτοξευθεί από μια φορητή πλατφόρμα μεταφοράς & εκτόξευσης. Ο τρόπος λειτουργείας του περιλάμβανε ένα ηλεκτρικό κύκλωμα, το οποίο έκλεινε μέσω του επίγειου σταθμού ελέγχου (μέσω ενός χειριστηρίου) όταν το αεροσκάφος είχε φτάσει σε ένα ικανοποιητικό για την αποστολή ύψος. Με το κλείσιμο του κυκλώματος, έκλεινε και ο κινητήρας του αεροσκάφους και απελευθερώνονταν τα φτερά, προκαλώντας την μετατροπή του αεροσκάφους σε «εναέρια τορπίλη» που βυθιζόταν προς το έδαφος φέροντας πάνω από ογδόντα (80) κιλά εκρηκτικής ύλης, ως φορτίο.

Εικόνα 3: Cusrtiss N2C Fledgling
Πηγή: National Naval Aviation Museum of the USA

Φτάνοντας, ιστορικά, μετά την εποχή του Α' Παγκοσμίου Πολέμου μέχρι και πριν τον Β' Παγκόσμιο πόλεμο, η τεχνολογία των ΣμηΕΑ εκ νέου νέες εξελίξεις και βελτιώσεις. Άξια αποτελεί η ενδελεχής ενασχόληση του Πολεμικού των Η.Π.Α. με τα ράδιο-ελεγχόμενα αεροσκάφη επί δεκαετία (1930-1940), η οποία και απέφερε την του Curtiss N2C-2 [5] το 1937. Παρόμοιες πρωτοβουλίες υλοποιήθηκαν από τους Βρετανούς, οι οποίοι το 1935 ανέπτυξαν το Queen Bee [6], ένα τηλεκατευθυνόμενο μη επανδρωμένο αεροσκάφος, το οποίο πιστεύεται ότι αποτέλεσε τον πρόδρομο της χρήσης του όρου «drone» για τα τηλεκατευθυνόμενα μη επανδρωμένα αεροσκάφη.

Εικόνα 4: DH.82 Queen Bee
Πηγή: Wikipedia, de Havilland Tiger Moth

γνώρισε αναφοράς Ναυτικού μία ανάπτυξη

Ένα ακόμα ΣμηΕΑ που αναπτύχθηκε από τους Βρετανούς είναι το Radioplane OQ-2 [7], το οποίο αποτελούσε ένα τηλεκατευθυνόμενο αεροσκάφος, με εφευρέτες τους Reginald Denny και Walter Righter, κατά την διάρκεια της δεκαετίας του 1930.

Παρόλο που προγενέστερα υπήρξαν όλα τα παραπάνω επιτεύγματα, η εφεύρεση ενός τηλεκατευθυνόμενου (ραδιοελεγχόμενου) αεροσκάφους που θα μπορούσε να διατηρεί την λειτουργικότητά του εκτός οπτικού πεδίου (Beyond line-of-sight / BLOS), πιστώθηκε στον Edward M. Sorensen, ο οποίος κατοχύρωσε, ως πατέντα [8], την εφεύρεσή του, στην οποία χρησιμοποιούσε έναν επίγειο σταθμό ελέγχου για να παρακολουθεί την θέση του αεροσκάφους. Πριν από αυτή την αξιοσημείωτη καινοτομία, όλα τα πρωτότυπα ραδιοελεγχόμενα ΣμηΕΑ μπορούσαν να επιχειρούν μόνο μέσα στο οπτικό πεδίο του «επίγειου» πιλότου.

Αναφορικά με την εξέλιξη της τεχνολογίας των ΣμηΕΑ, ένα από τα σημειωτέα γεγονότα που έλαβαν χώρα κατά την διάρκεια του Β' Παγκοσμίου Πολέμου, ήταν η εμφάνιση των V-1 Doodlebugs [9], τα οποία λειτουργούσαν με την χρήση Pulsejet, δηλαδή. με κινητήρα στον οποίο η καύση πραγματοποιείται με παλμούς. Το συγκεκριμένο αεροσκάφος αποτέλεσε τον πρόδρομο των πρώτων πυραύλων Κρουζ στον κόσμο.

Εικόνα 5: V-1 flying bomb Fieseler Fi 103 (Doodlebug)
Πηγή: Wikipedia, V-1 flying bomb

Μερικά χρόνια αργότερα και κατά την διάρκεια του πολέμου του Βιετνάμ, εμφανίστηκαν και χρησιμοποιηθήκαν για πρώτη φορά τα ΣμηΕΑ ως αναγνωριστικά αεροσκάφη. Από εκείνη την εποχή και μετά, τα ΣμηΕΑ άρχισαν να χρησιμοποιούνται για διάφορους, νέους ρόλους, όπως για παράδειγμα ως δόλωμα στη μάχη, είτε για την εκτόξευση πυραύλων εναντίον σταθερών στόχων, σύμφωνα με το Imperial War Museum του Λονδίνου.

Στα τέλη της δεκαετίας του 1950, το αμερικανικό κατασκοπευτικό αεροπλάνο, το επανδρωμένο SR-71 Blackbird, βρισκόταν ακόμη σε ανάπτυξη και οι κατασκοπευτικοί δορυφόροι επίσης δεν ήταν έτοιμοι για ανάπτυξη και πλήρη λειτουργία, ακόμη. Έτσι λοιπόν, η ανάγκη για τέτοια συστήματα μη επανδρωμένων αεροσκαφών έγινε ακόμη πιο εμφανής σε πολλά έθνη σε όλο τον κόσμο, τα οποία άρχισαν να εξερευνούν τη χρήση τους για διάφορες στρατιωτικές εφαρμογές. Ως εκ τούτου, τα νέα μοντέλα ΣμηΕΑ ενισχύθηκαν αρκετά, καθώς οι προσπάθειες επικεντρώθηκαν στη βελτίωση της αντοχής τους, αλλά και του ύψους στο οποίο θα μπορούσαν να λειτουργήσουν με ασφάλεια.

Την δεκαετία 1960-1970, και μετά την εφεύρεση των τρανζίστορ, εμφανίστηκαν τα πρώτα τηλεκατευθυνόμενα αερομοντέλα, τα οποία επέτρεπαν στους ενδιαφερόμενους να κατασκευάζουν και να πετούν τηλεκατευθυνόμενα αεροσκάφη, είτε σε εσωτερικούς είτε σε εξωτερικούς χώρους. Έτσι δημιουργήθηκε ένας μεγάλος αριθμός πολιτών, οι οποίοι ασχολήθηκαν ενδελεχώς με τον αερομοντελισμό, δημιουργώντας ένα νέο χόμπι και τελικά μια νέα βιομηχανία, η οποία επιτάχυνε αρκετά την ανάπτυξη της εμπορικής τεχνολογίας των τηλεκατευθυνόμενων αεροσκαφών.

Εικόνα 6: Pioneer RQ-2A UAV
Πηγή: National air and space museum of USA

Μέχρι το 1980, τα ΣμηΕΑ δεν θεωρούνταν αρκετά αξιόπιστα για την εκπλήρωση στρατιωτικών αποστολών, και σε συνδυασμό με το υψηλό τους κόστος δεν προτιμήθηκαν έναντι άλλων τεχνολογιών της εποχής, για περεταίρω επένδυση και βελτίωση. Αυτή, όμως, η αντίληψη άλλαξε άρδην, το 1982, όταν οι ισραηλινές δυνάμεις χρησιμοποίησαν μη επανδρωμένα αεροσκάφη για να κερδίσουν τη μάχη εκείνης της εποχής εναντίον της Συριακής Πολεμικής Αεροπορίας, με μηδαμινές απώλειες. Έκτοτε οι Η.Π.Α. ξεκίνησαν τις διαδικασίες για την ανάπτυξη και κατασκευή ενός φθηνού ΣμηΕΑ το οποίο θα υποστήριζε μαζικές στρατιωτικές επιχειρήσεις. Σε αυτή την κατεύθυνση, και έπειτα από μια σύμπραξη των Η.Π.Α. και του Ισραήλ το 1986 αναπτύχθηκε το RQ2 Pioneer [10], το οποίο αποτελούσε ένα μεσαίου μεγέθους αεροσκάφος αναγνώρισης.

Τα επόμενα χρόνια (1990-2010), αναπτύχθηκαν και κατασκευάστηκαν μικρό-εκδόσεις ΣμηΕΑ, καθώς και το Predator [11], το οποίο έγινε γνωστό μέσω της καταλυτικής συμμετοχής του στο Αφγανιστάν, κατά την διάρκεια των επιχειρήσεων αναζήτησης του Οσάμα Μπιν Λάντεν. Τα επόμενα χρόνια, αναπτύχθηκε, επίσης, μια σειρά από μικρού-μεγέθους μη επανδρωμένα

αεροσκάφη παρακολούθησης με σταθερή πτέρυγα, όπως τα Raven [12] και Puma [13]. Αξίζει να σημειωθεί επίσης, ότι το 2006 ήταν μια κομβική χρονιά στην ιστορία των ΣμηΕΑ, καθώς ήταν η πρώτη χρονιά που η FAA [14] εξέδωσε επίσημα την πρώτη εμπορική άδεια χρήσης.

Την σύγχρονη εποχή (2010-σήμερα), παρατηρήθηκε μια τεράστια ανάπτυξη στον τομέα και την τεχνολογία των ΣμηΕΑ, καθώς και στις εμπορικές εφαρμογές τους. Όπως απορρέει από τις προαναφερθείσες ιστορικές εξελίξεις, τα ΣμηΕΑ μέχρι περίπου τις αρχές του 2010, χρησιμοποιούνταν κυρίως για στρατιωτικούς σκοπούς ή για χόμπι (αερομοντελισμός). Από τότε, προτάθηκαν πολλές νέες χρήσεις για ΣμηΕΑ σε διάφορα πεδία και τομείς, όπως για παράδειγμα την χρήση τους, ως όχημα παράδοσης δεμάτων. Μοιραία, ήλθαν και οι νομοθετικές διατάξεις και κανονισμοί περί της σωστής και ασφαλούς χρήσης των ΣμηΕΑ, τόσο στην Αμερική (FAA), όσο και στην Ευρώπη (EASA) [15]. Από τεχνολογικής πλευράς, τα ΣμηΕΑ ακολούθησαν την άνθιση της τεχνολογίας στα πεδία των τηλεπικοινωνιών, μικροελεγκτών, ανάλυσης δεδομένων κτλ., και εμφανίστηκαν αρκετά ΣμηΕΑ με φορτίο που περιλαμβάνει, αλλά δεν περιορίζεται σε κάμερες, RADAR, LIDAR, κτλ. Περαιτέρω έρευνες επέτρεψαν τον έλεγχο ενός ΣμηΕΑ με 4 (quadcopter) ή περισσότερους ρότορες (multicopter) ρυθμίζοντας την ταχύτητα μεμονωμένων ρότορων. Η βελτίωση της ευστάθειας των αεροσκαφών με πολλαπλούς ρότορες άνοιξε νέες δυνατότητες χρήσης τους. Εν κατακλείδι, η ταχεία ανάπτυξη της τεχνολογίας αυτή την εποχή, επέτρεψε την περαιτέρω βελτίωση των μη επανδρωμένων αεροσκαφών τα οποία αφομοίωσαν μια σειρά από τεχνολογίες όπως, μικροελεγκτές, επιταχυνσιόμετρα, μπαταρία ιόντων λιθίου πολυμερούς (Li-Po), κτλ.

1.2 Η τεχνολογία των Συστημάτων μη Επανδρωμένων Αεροσκαφών

1.2.1 Γενικά

Εικόνα 7: ΣμηΕΑ περιστροφικής πτέρυγας -τύπου πολυκοπτέρου

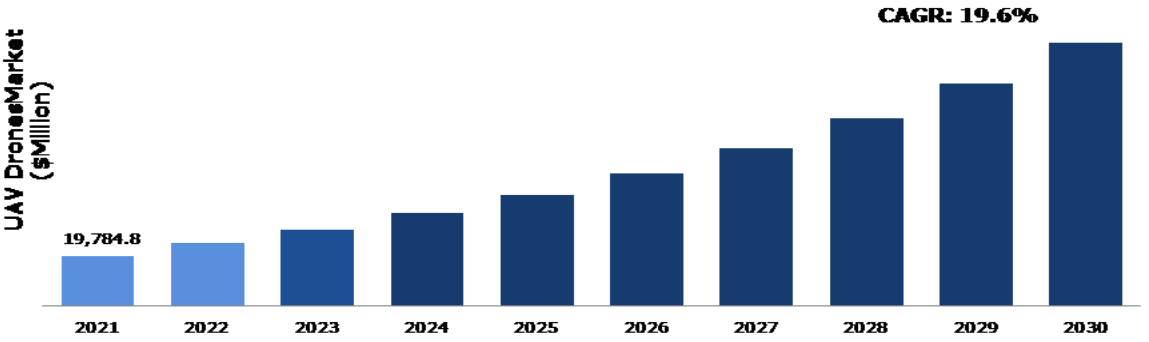
Εικόνα 8: ΣμηΕΑ σταθερής πτέρυγας

Την σημερινή εποχή, τα μη επανδρωμένα αεροσκάφη διατίθενται σε διάφορα σχήματα , που κυμαίνονται από μικρού μεγέθους, χειρός, έως μεγάλα αεροσκάφη τα σε πολλές περιπτώσεις έχουν παρόμοιο μέγεθος με τα επανδρωμένα. Η κατασκευή και οι αρχές λειτουργίας των ΣμηΕΑ εξαρτώνται σε μεγάλο βαθμό από την λειτουργία ή αποστολή που προσβλέπουν να εκτελέσουν όπως για παράδειγμα φωτογράφιση, βιντεοσκόπηση, χαρτογράφηση, αναγνώριση/παρακολούθηση στόχων, προστασία δημοσίων χώρων, κτλ.

Ως εκ τούτου, αξίζει να αναφερθεί πως τα τελευταία χρόνια, η αγορά και οι εφαρμογές των ΣμηΕΑ, πληθαίνουν καθώς πληθαίνουν και τα οφέλη από την χρήση τους. Με το ίδιο τρόπο έχει δομηθεί και η παγκόσμια αγορά των ΣμηΕΑ, δηλαδή με βάση τον τρόπο λειτουργίας τους, την εφαρμογή αλλά και τον τελικό χρήστη.

Με βάση την αρχή λειτουργίας, η παγκόσμια αγορά ΣμηΕΑ διαιρείται σε σταθερής πτέρυγας (fixed-wing), πολυκόπτερα (rotary-wing) και υβριδικά (hybrid), εκ της οποίας το μεγαλύτερο μερίδιο κατέχουν τα πολυκόπτερα. Οι

εκτιμήσεις των αναλυτών αναμένουν να φτάσει τα 872 δισεκατομμύρια δολάρια έως το 2030, φθάνοντας έναν σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR) που να αγγίζει το 54,5%. Οι εκτιμήσεις για την εμπορική χρήση του ΣμηΕΑ σταθερής πτέρυγας είναι ακόμα πιο ευοίωνες, εκτιμώντας ότι η αγορά αυτή θα φτάσει σε αξία τα 238 δισεκατομμυρίων δολάρια έως το 2030 με CAGR 59,3%. Η αγορά εμπορικών μη επανδρωμένων αεροσκαφών σταθερής πτέρυγας αναμένεται να σημειώσει σημαντική ανάπτυξη κατά την περίοδο πρόβλεψης λόγω της αυξανόμενης ζήτησης για εφαρμογές χαρτογράφησης και τοπογραφίας. Αξίζει να αναφερθεί πως στην αγορά των ΣμηΕΑ, η βιομηχανία που παρέχει τον μεγαλύτερο αριθμό ΣμηΕΑ είναι η DJI [16].



Εικόνα 9: Πρόβλεψη της αγοράς των ΣμηΕΑ μέχρι το 2030
Πηγή: Researchdive, UAV drones market

Με βάση την εφαρμογή και τον τελικό χρήστη, η παγκόσμια εμπορική αγορά των ΣμηΕΑ διαιρείται στους παρακάτω γενικούς τομείς: Κινηματογράφηση και Φωτογραφία, Επιθεώρηση και Συντήρηση, Χαρτογράφηση και Γεωγραφία, Γεωργία Ακριβείας, Επιτήρηση και Παρακολούθηση και άλλα, οι οποίοι θα αναλυθούν στην επόμενη ενότητα.

Τα Συστήματα μη Επανδρωμένων Αεροσκαφών, λοιπόν, αποτελούν έναν ταχέως αναπτυσσόμενο τομέα της αεροπορίας, με μεγάλες δυνατότητες ως προς την δημιουργία νέων θέσεων εργασίας και την τόνωση της οικονομίας στα κράτη μέλη της Ευρωπαϊκής Ένωσης, αλλά και του υπόλοιπου κόσμου. Καθώς η χρήση τους τείνει να γιγαντωθεί φτάνοντας σε συχνότητα την καθημερινή χρήση άλλων τεχνολογιών όπως π.χ. το αυτοκίνητο, είναι αναγκαίο να υπάρχουν διαδικασίες, κανονισμοί που θα πρέπει να τηρούνται τόσο για την προστασία του ΣμηΕΑ καθαυτού, όσο και για την ασφάλεια των χειριστών και των υλικών αγαθών και ανθρώπων που βρίσκονται στο «πεδίο λειτουργίας» του εκάστοτε ΣμηΕΑ. Γι' αυτόν ακριβώς τον λόγο η Ε.Ε. θέσπισε κανονισμό για την ασφαλή ένταξη των τηλεκατευθυνόμενων μη επανδρωμένων αεροσκαφών στον ευρωπαϊκό εναέριο χώρο [17]. Βάσει του κανονισμού 2019/945 [18] της Ευρωπαϊκής Επιτροπής, οι τεχνικές προδιαγραφές και οι κατηγορίες στις οποίες εμπίπτουν τα διάφορα ΣμηΕΑ από τις 31/12/2020 είναι οι C0, C1, C2, C3 και C4. Κάθε μία από αυτές φέρει διαφορετικά χαρακτηριστικά, τα οποία και περιγράφονται επακριβώς στην εν λόγω νομοθεσία. Παρατηρώντας αποκλειστικά την Μέγιστη Μάζα Απογείωσης (MTOM) στις παραπάνω κατηγορίες διαπιστώνεται πως τα ΣμηΕΑ:

- C0: έχουν MTOM κάτω των 250 g, συμπεριλαμβανομένου του ωφέλιμου φορτίου
- C1: έχουν MTOM κάτω των 900 g, συμπεριλαμβανομένου του ωφέλιμου φορτίου
- C2: έχουν MTOM κάτω των 4 kg, συμπεριλαμβανομένου του ωφέλιμου φορτίου
- C3: έχουν MTOM κάτω των 25 kg, συμπεριλαμβανομένου του ωφέλιμου φορτίου, και έχουν μέγιστη χαρακτηριστική διάσταση κάτω των 3 m
- C4: έχουν MTOM κάτω των 25 kg, συμπεριλαμβανομένου του ωφέλιμου φορτίου.

1.2.2 Πεδίο εφαρμογής

Τα τελευταία χρόνια η τεχνολογία των ΣμηΕΑ εξαπλώνεται ολοένα και περισσότερο σε διάφορες εφαρμογές της καθημερινότητας. Αν και αρχικά, όπως αναφέρθηκε και στην Ενότητα 1.1 τα

ΣμηΕΑ χρησιμοποιήθηκαν κυρίως για στρατιωτικές εφαρμογές, σήμερα βρίσκουν χρήση σε διάφορες πτυχές των ανθρώπινων δραστηριοτήτων και το εύρος των εφαρμογών τους αυξάνεται συνεχώς. Στην πραγματικότητα, υπάρχουν σχετικές προβλέψεις ότι τα ΣμηΕΑ μπορεί να αλλάξουν δραματικά τον τρόπο που εργαζόμαστε, όπως έκανε η τεχνολογία του Διαδικτύου και των «έξυπνων» κινητών τηλεφώνων. Οι πιο συνηθισμένες εφαρμογές ΣμηΕΑ παρατίθενται παρακάτω:

- **Έρευνα και διάσωση**: Τα ΣμηΕΑ δύναται να χρησιμοποιηθούν κατά τη διάρκεια οποιασδήποτε επιχείρησης πρόληψης, ανταπόκρισης και ανάκαμψης από φυσικές καταστροφές συμπεριλαμβανομένων και των επιχειρήσεων Έρευνας και Διάσωσης. Η συμβολή των ΣμηΕΑ είναι καθοριστική διότι παρέχουν υψηλής ποιότητας βίντεο και δεδομένα από αισθητήρες (π.χ. θερμοκρασία), χωρίς να κινδυνεύει η σωματική ακεραιότητα των πρώτων ανταποκριτών (πχ. Πυροσβέστες).
- **Επιθεώρηση και Συντήρηση**: Τα ΣμηΕΑ με την χρήση κατάλληλων αισθητήρων (π.χ. θερμική κάμερα), μπορούν να συνεισφέρουν σημαντικά σε επιθεωρήσεις ανεμογεννητριών, γεφυρών, εργοταξίων, γραμμών ηλεκτρικού ρεύματος, αγωγών κ.λπ., μειώνοντας με αυτόν τον τρόπο σημαντικά το κόστος των χειρωνακτικών επιθεωρήσεων.
- **Γεωργία Ακριβείας**: Στον τομέα της γεωργίας, μέσω των επιθεωρήσεων των χωραφιών και καλλιεργειών, τα ΣμηΕΑ συνεισφέρουν σημαντικά στην ακριβή αξιολόγηση της προόδου της καλλιέργειας και στην μεταφορά αλλά και στο ράντισμα των απαιτούμενων φυτοφαρμάκων, όπου αυτό απαιτείται.
- **Επιτήρηση και Παρακολούθηση**: Πλέον, σχεδόν όλα τα ΣμηΕΑ είναι εξοπλισμένα με κάμερα, εξ' αυτών τα περισσότερα επαγγελματικά ΣμηΕΑ διαθέτουν κάμερες ημέρας και θερμική, ως αναπόσπαστο μέρος του ωφέλιμού τους φορτίου. Αυτές οι κάμερες παρέχουν ζωντανές ροές βίντεο που βοηθούν τις αρχές επιβολής του νόμου (π.χ. Αστυνομία) στην έρευνα, επιτήρηση και παρακολούθηση περιοχών ενδιαφέροντος στις οποίες δεν υπάρχει σταθερό σύστημα επιτήρησης, όπως για παράδειγμα για την ασφάλεια συνόρων.
- **Γεωγραφική χαρτογράφηση**: Αναφορικά με την χαρτογράφηση περιοχών, τα ΣμηΕΑ φέροντας ως ωφέλιμο φορτίο, LIDAR, πολυφασματικές κάμερες, κ.λπ., επιτρέπουν τη συλλογή δεδομένων τα οποία είναι πιο ακριβή και ευκολότερα στη λήψη, συγκριτικά με τις παραδοσιακές μεθόδους χαρτογράφησης.
- **Μεταφορές φορτίων**: Ο συγκεκριμένος τομέας δεν είναι ακόμη σε πλήρη άνθιση, λόγω κυρίων των νομοθετικών απαιτήσεων και δικλείδων ασφαλείας που απαιτούνται για την υλοποίηση τέτοιων μεταφορών. Παρόλα αυτά, τα ΣμηΕΑ δύνανται να παραδώσουν πακέτα με ασφαλή και φιλικό προς το περιβάλλον τρόπο. Μια εφαρμογή στην οποία θα μπορούσε να προσφέρει άμεσα και καθοριστικά αποτελέσματα, είναι η παράδοση ιατρικών προμηθειών και πρώτων βοηθειών γρήγορα και εύκολα σε αγροτικές ή δυσπρόσιτες περιοχές.
- **Κινηματογράφηση και Αεροφωτογραφία**: Τα ΣμηΕΑ μπορούν να αντικαταστήσουν με ευκολία παραδοσιακά μέσα που χρησιμοποιούνταν μέχρι σήμερα για την κινηματογράφηση (συστήματα καμερών με ανυψωτικά μηχανήματα και βραχίονες) και για την αεροφωτογραφία (ελικόπτερα ή ειδικά αεροπλάνα) λόγω της ικανότητάς τους να αιωρούνται σε χαμηλότερα υψόμετρα και να προσφέρουν λήψεις μεγαλύτερης ακρίβειας.
- **Περιβαλλοντική Παρακολούθηση και Έρευνα**: Τα ΣμηΕΑ χρησιμοποιούνται, επίσης, για την παρακολούθηση απομακρυσμένων και μη ασφαλών περιοχών περιβαλλοντικού ενδιαφέροντος όπως για παράδειγμα, ηφαίστεια, περιοχές μολυσμένες με ακτινοβολία (π.χ. Τσέρνομπιλ), παρέχοντας σημαντικά δεδομένα για περαιτέρω περιβαλλοντική έρευνα.

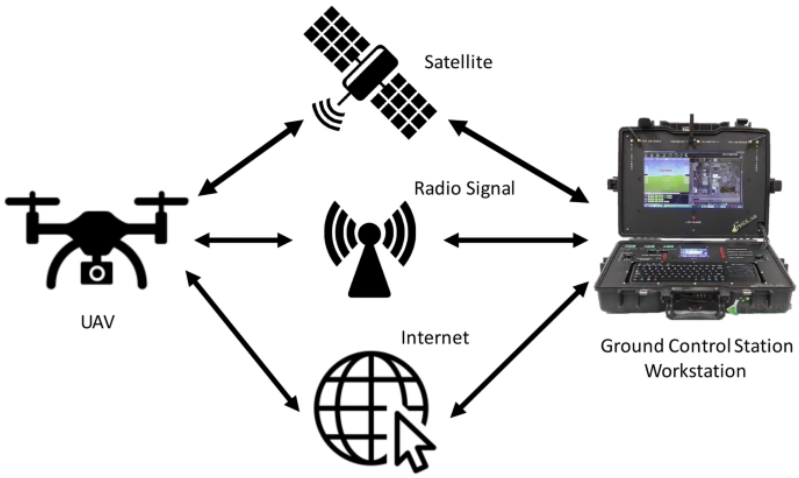
1.2.3 Αρχή λειτουργίας

Εξαιτίας της εκτεταμένης ποικιλίας των εφαρμογών τους, δεν υπάρχει ενιαία ταξινόμηση των ΣμηΕΑ, ανά τον κόσμο. Οι χειριστές ΣμηΕΑ στρατιωτικού τύπου χρησιμοποιούν τα δικά τους πρότυπα, ενώ οι υπόλοιποι χειριστές έχουν τις δικές τους διαρκώς μεταβαλλόμενες ταξινομήσεις. Παρά τις προφανείς διαφορές στις κατηγοριοποιήσεις τους, τόσο τα ΣμηΕΑ πολιτικού όσο και στρατιωτικού τύπου, είτε στην Ευρώπη, είτε στην Αμερική ταξινομούνται κυρίως κατά μέγεθος, και δευτερευόντως κατά τύπο και αντοχή. Παρόλα αυτά, έχοντας υπόψη τον Ευρωπαϊκό κανονισμό που παρουσιάστηκε στην Ενότητα 1.2.1, φαίνεται πως τουλάχιστον σε ευρωπαϊκό επίπεδο θα επιτευχθεί ο εναρμονισμός στις κατηγορίες.

Ανεξαρτήτως λοιπόν της κατηγοριοποίησης των ΣμηΕΑ και όπως αναφέρθηκε σε προηγούμενη ενότητα υπάρχουν τρεις βασικές κατηγορίες ΣμηΕΑ, σύμφωνα με την αρχή λειτουργίας τους, τα πολυκόπτερα, σταθερής πτέρυγας και εκείνα που διέπονται από τις δύο αρχές.

Τα μη επανδρωμένα οχήματα με περιστροφική πτέρυγα (πολυκόπτερα) δημιουργούν κάθετη ανύψωση περιστρέφοντας τα πτερύγια του ρότορα γύρω από έναν κεντρικό ιστό, πιέζοντας τον αέρα προς τα κάτω και ωθώντας το αεροσκάφος στον αέρα. Τα συγκεκριμένα ΣμηΕΑ με περιστροφική λεπίδα αποτελούνται από έναν έως οκτώ ρότορες που δημιουργούν την απαραίτητη ώθηση. Τα μη επανδρωμένα αεροσκάφη με σταθερή πτέρυγα διέπονται από τις ίδιες αρχές όπως τα επανδρωμένα αεροσκάφη, αναπτύσσοντας την δύναμη της άντωσης μέσω της ταχύτητας στον οριζόντιο άξονα, το οποίο συνήθως επιτυγχάνεται είτε μέσω διαδρόμου απογείωσης, είτε μέσω ειδικού εξοπλισμούς εκτόξευσης. Η υβριδική κατηγορία αφορά τα ΣμηΕΑ σταθερής πτέρυγας τα οποία περιλαμβάνουν την απογείωση/προσγείωση στον κάθετο άξονα μέσω περιστροφής (επιπρόσθετων) πτερυγίων (vertical take-off landing – VTOL).

Ανατρέχοντας στον όρο Σύστημα μη Επανδρωμένων Αεροσκαφών, αναφερόμαστε στο τηλεκατευθυνόμενο αεροσκάφος, στον επίγειο σταθμό ελέγχου αλλά και στο υποσύστημα επικοινωνίας. Μια τυπική διαμόρφωση λειτουργίας ενός συνήθους εμπορικού ΣμηΕΑ φαίνεται στην Εικόνα 10.



Εικόνα 10: Συνήθης διαμόρφωση για τηλεχειρισμό των ΣμηΕΑ
Πηγή: Aljehani, M., Inoue, M., Watanbe, A. et al. UAV communication system integrated into network traversal with mobility. SN Appl. Sci. 2, 1057 (2020). https://doi.org/10.1007/s42452-020-2749-5

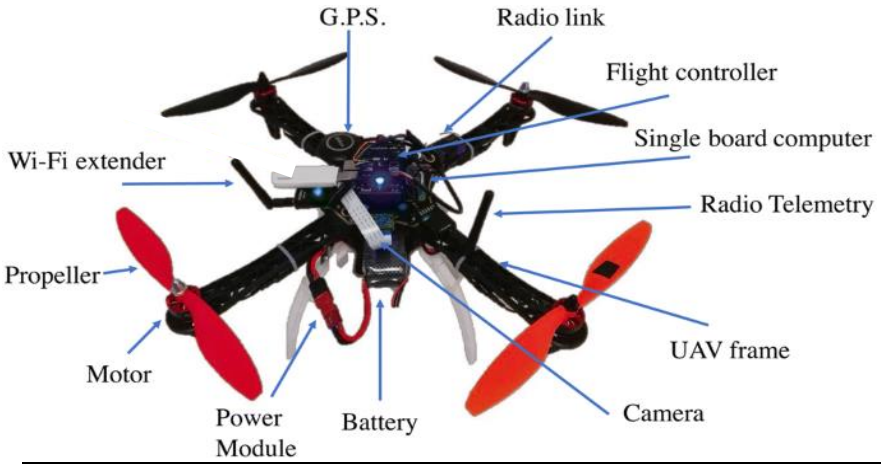
Τα ΣμηΕΑ μπορούν να λειτουργούν και να κατευθύνονται μέσω ελεγχόμενης λειτουργίας κατά την οποία το αεροσκάφος πλοηγείται από έναν εξειδικευμένο χειριστή ΣμηΕΑ μέσω χειριστηρίου, ή μέσω της αυτόνομης λειτουργίας, χρησιμοποιώντας σταθμό εδάφους ελέγχου (υπολογιστής με σχετικό λογισμικό ή/και εξοπλισμό πλοήγησης). Η πλοήγηση των ΣμηΕΑ και στις 2 περιπτώσεις μπορεί να βασίζεται σε μια σειρά από τεχνικές πλοήγησης όπως για παράδειγμα:

- «Παραδοσιακή» πλοήγηση: πλοήγηση με βάση οπτικά ορόσημα ή ειδικά σχεδιασμένα σημεία αναφοράς.

- Άστρο-πλοήγηση: πλοήγηση που βασίζεται σε γωνιακές μετρήσεις που λαμβάνονται μεταξύ ενός ουράνιου σώματος (ήλιος, σελήνη) και του ορατού ορίζοντα.
- Αδρανειακή πλοήγηση: ενσωματωμένο σύστημα πλοήγησης, inertial navigation system (INS), που συγχωνεύει δεδομένα από διάφορους αισθητήρες (ταχύμετρα, υψόμετρα, επιταχυνσιόμετρα, γυροσκόπια και μαγνητόμετρα) για να δώσει την τρέχουσα θέση σε σχέση με ένα γνωστό σημείο εκκίνησης
- Πλοήγηση με τη βοήθεια ραδιοσημάτων: σύστημα πλοήγησης που χρησιμοποιεί ραδιοσήματα από διάφορους σταθμούς (π.χ. ραντάρ εδάφους, δορυφορικά συστήματα) για την αξιολόγηση της τρέχουσας θέσης.

Τα περισσότερα εκ των εμπορικών ΣμηΕΑ υιοθετούν πλοήγηση που βασίζεται σε δορυφορικά συστήματα (π.χ. GPS, GLONASS, GALILEO, Beidou). Αξίζει να σημειωθεί πως οι συχνότητες που εκπέμπουν τα δορυφορικά συστήματα για την πλοήγηση των ΣμηΕΑ κυμαίνονται από 1176.45 MHz μέχρι και 1575.42 MHz. Επιπροσθέτως, η πλειοψηφία των εμπορικών ΣμηΕΑ που προορίζονται για πολιτική χρήση διαθέτουν έναν αριθμό συστημάτων επικοινωνίας που χρησιμοποιούνται για διάφορες εφαρμογές όπως για παράδειγμα το κανάλι ελέγχου με τον επίγειο σταθμό (μεταφορά τηλεμετρικών δεδομένων και εντολών), το κανάλι για την διασφάλιση των επικοινωνιών με άλλα ΣμηΕΑ και επανδρωμένα αεροσκάφη (όπως πχ ADS-B), το κανάλι για την μεταφορά βίντεο ή δεδομένων του αισθητήρα σε πραγματικό χρόνο. Τα εμπορικά ΣμηΕΑ συνήθως χρησιμοποιούν διαφορετικά κανάλια για την μεταφορά της τηλεμετρίας και την μεταφορά δεδομένων βίντεο. Στην Ευρώπη, οι συχνότητες που χρησιμοποιούνται για την μεταφορά τηλεμετρίας και εντολών είναι η ζώνη ραδιοφάσματος 2,4 -2,485 GHz και για την μεταφορά βίντεο είναι οι συχνότητες 900 MHz, 1,2 GHz, 2,4 GHz, 5,8 GHz.

Μια τυπική διαμόρφωση ΣμηΕΑ και όλων των εξαρτημάτων που συνήθως φέρουν, φαίνεται στην Εικόνα 11 παρακάτω και αποτελείται συνήθως από:



Εικόνα 11: Τυπική αρχιτεκτονική ΣμηΕΑ – κατηγορία πολυκόπτερο
Πηγή: Aljehani, M., Inoue, M., Watanbe, A. et al. UAV communication system integrated into network traversal with mobility. SN Appl. Sci. 2, 1057 (2020). https://doi.org/10.1007/s42452-020-2749-5

- Κινητήρας ή ρότορες και προπέλες
- Κυψέλη καυσίμου ή μπαταρία
- Σύστημα πλοήγησης
- Σύστημα αυτόματου πιλότου
- Μονάδα δορυφορικής πλοήγησης και η αντίστοιχη πομποδέκτη δορυφορικής πλοήγησης
- Κανάλι μεταφοράς τηλεμετρίας και ελέγχου
- Κανάλι μεταφοράς βίντεο

- Σύστημα φορτίου κάμερας (περιλαμβάνει κάμερα ημέρας ή/και νύχτας, συσκευή εγγραφής και αντίζυγο - gimbal)
- Αισθητήρες για την ασφαλή πτήση του ΣμηΕΑ όπως επιταχυνσιόμετρο, γυροσκόπιο, βαρόμετρο, κτλ.

Η μονάδα ισχύος ή αλλιώς Power Module (PM) που εμπεριέχει την/τις μπαταρία/μπαταρίες, παρέχει ισχύ τόσο στους κινητήρες/ρότορες όσο και στα εξαρτήματα ελέγχου πτήσης. Είναι σημαντικό να αναφερθεί ότι το PM περιλαμβάνει επίσης ένα εφεδρικό σύστημα μπαταρίας για αυξημένη αξιοπιστία και αντοχή του ΣμηΕΑ. Η μονάδα επικοινωνιών περιλαμβάνει πομπούς, δέκτες και ραδιομόντεμ σε διάφορες συχνότητες (κανάλια) για την μεταφορά, τηλεμετρίας, βίντεο, και για τον έλεγχο της κάμερας του ΣμηΕΑ. Η μονάδα πλοήγησης περιλαμβάνει το σύστημα αυτόματου πιλότου, την πυξίδα και τον δορυφορικό δέκτη GPS. Το σύστημα αυτόματου πιλότου ελέγχει όλη την μονάδα ελέγχου πτήσης που περιλαμβάνει το γκάζι (Throttle) και τα πηδάλια του αεροσκάφους (Rudder, Elevator, Aileron).

1.2.4 Αρχείο καταγραφής

Στους ηλεκτρονικούς υπολογιστές, ένα αρχείο καταγραφής (log file) είναι ένα αρχείο που καταγράφει είτε γεγονότα (events) που συμβαίνουν σε ένα λειτουργικό σύστημα ή άλλες εκδόσεις λογισμικού είτε μηνύματα μεταξύ διαφορετικών χρηστών λογισμικού επικοινωνίας. Η καταγραφή αυτών, αποτελεί την πράξη της τήρησης αρχείου καταγραφής. Για παράδειγμα ένα αρχείο καταγραφής συναλλαγών είναι ένα αρχείο των επικοινωνιών μεταξύ ενός συστήματος και των χρηστών αυτού του συστήματος, ή μια μέθοδος συλλογής δεδομένων που καταγράφει αυτόματα τον τύπο, το περιεχόμενο ή τον χρόνο των συναλλαγών που πραγματοποιούνται από ένα τερματικό με αυτό το σύστημα. Μια άλλη περίπτωση που τα αρχεία καταγραφής χρησιμοποιούνται ευρέως είναι τα λειτουργικά συστήματα και τα λογισμικά, που μέσω συστημάτων καταγραφής αυτοματοποιείται η διαδικασία της δημιουργίας, του φιλτραρίσματος και της καταγραφής των μηνυμάτων αυτών, εξοικονομώντας έτσι αρκετό χρόνο σε προγραμματιστές λογισμικού όταν πρέπει να διαπιστώσουν και επιλύσουν σφάλματα. Τα αρχεία καταγραφής πλέον χρησιμοποιούνται αρκετά, καθώς εμπερικλείονται σε κάθε «έξυπνη» ηλεκτρονική συσκευή, η οποία εκτελεί κάποια λειτουργία και για την οποία εφόσον δυσλειτουργεί θα πρέπει να εξεταστεί η λειτουργία της μέσω των αρχείων αυτών. Εκτός από την εύρεση δυσλειτουργιών, όμως, τα αρχεία καταγραφής χρησιμοποιούνται και ως πειστήρια μια ενέργειας, καθώς εμπεριέχουν πληροφορίες για τον χρήστη, την ενέργεια που έκανε καθώς και τον χρόνο. Όπως είναι λογικό λοιπόν, έτσι και στα ΣμηΕΑ υπάρχει το σύστημα που καταγράφει τα γεγονότα και συμβάντα της λειτουργίας του. Πιο συγκεκριμένα, αυτά τα αρχεία καταγραφής περιέχουν εξαιρετικά λεπτομερείς πληροφορίες σχετικά με την πτήση, οι οποίες περιλαμβάνουν τον σειριακό αριθμό και το μοντέλο του ΣμηΕΑ και των βασικών εξαρτημάτων, την διάρκεια ζωής της μπαταρίας του ΣμηΕΑ, τον εντοπισμό θέσης GPS, τη δραστηριότητα της κάμερας και άλλα, παρέχοντας ένα ζωτικής σημασίας αρχείο των δραστηριοτήτων πτήσης. Αυτά τα αρχεία καταγραφής πτήσεων είναι επίσης χρήσιμα για τη διάγνωση προβλημάτων με ΣμηΕΑ, σε περιπτώσεις ατυχημάτων. Τα αρχεία αυτά δεν είναι προσβάσιμα με τον ίδιο τρόπο για όλα τα εμπορικά ΣμηΕΑ, καθώς, επίσης, κάποια από αυτά είναι κωδικοποιημένα (π.χ. DJI logfiles) με αποτέλεσμα να γίνεται ακόμη πιο δύσκολη η ανάλυσή τους. Τέλος, θα μπορούσαμε να πούμε ότι το αρχείο καταγραφής των ΣμηΕΑ είναι κάτι αντίστοιχο με το «black box» των αεροσκαφών. Στην παρούσα διατριβή, τα αρχεία καταγραφής είναι όλα κωδικοποιημένα και προέρχονται από τον προμηθευτή ΣμηΕΑ «DJI».

1.3 Περιστατικά με Συστημάτων μη Επανδρωμένων Αεροσκαφών

Ως «παρενέργεια» της προόδου της τεχνολογίας και της κατακόρυφης αύξησης της χρήσης ΣμηΕΑ σε διάφορες εφαρμογές, υπήρξαν και περιστατικά ασφαλείας όπου σε αρκετές περιπτώσεις ΣμηΕΑ ενεπλάκησαν (εκούσια ή ακούσια), τα οποία έχουν καταγραφεί και αναλυθεί. Στην παρούσα ενότητα θα παρουσιαστούν ορισμένα από αυτά τα περιστατικά ασφαλείας, περιλαμβάνοντας ατυχήματα καθώς και εγκληματικές ενέργειες που εντοπίζονται στη βιβλιογραφία σχετικά με επιθέσεις σε δημόσιους χώρους, σε κρίσιμες υποδομές, κ.α.. Είναι

εύκολα κατανοητό πως ένα αντικείμενο που ίπταται σε μικρό υψόμετρο, μπορεί να προκαλέσει και ατυχήματα είτε από αστοχία του ιδίου (μπαταρία), είτε από κακή χρήση (αέρας, κτλ.). Επίσης, τα ΣμηΕΑ πρέπει να σημειωθεί πως μπορούν να φέρουν και άλλα «αυτοσχέδια» ωφέλιμα φορτία εκτός από τις κοινές κάμερες.

Η αμεσότητα, η ευκολία πρόσβασης στην τεχνολογία των ΣμηΕΑ, καθώς και οι δυνατότητες τους, τα καθιστούν ικανά να εκτελέσουν αρκετές αποστολές φθηνότερα, ευκολότερα και πολλές φορές «κρυφά» συγκριτικά με μικρά αεροσκάφη ή ελικόπτερα. Από την μία πλευρά, υπάρχουν περιστατικά ασφαλείας που οφείλονται στην αμέλεια του χειριστή ή την μη ορθή χρήση της τεχνολογίας. Από την άλλη, όμως, η εξάπλωση αυτής της φθηνής και άμεσα διαθέσιμης τεχνολογίας καθιστά την εκτέλεση εγκληματικών ή/και τρομοκρατικών ενεργειών εύκολη στην πραγματοποίηση και επίτευξη και δύσκολη στην αντιμετώπιση.

Λαμβάνοντας υπόψη ότι το κάθε ΣμηΕΑ είναι

- Εύκολα προσβάσιμο για όλους (εμπορικά)
- Εύκολο στην πλοήγηση και ικανό να διανύει μεγάλες αποστάσεις
- Ικανό να μεταφέρει αρκετά μεγάλο ωφέλιμο φορτίο σε σύγκριση με το μέγεθός και το βάρος του
- Ικανό να ξεπεράσει όλα τα μέτρα προστασίας ΄δυο (2) διαστάσεων που υπάρχουν ως σήμερα για την ασφάλεια χώρων ή υποδομών
- Δύσκολο να ανιχνευτεί και εξουδετερωθεί λόγω του μικρού οπτικού, θερμικού και ακουστικού αποτυπώματος που έχει
- Εύκολο να προσαρμοστούν εκτελώντας αυτοματοποιημένες πτήσεις ακριβείας ακόμα και χωρίς την χρήση των συντεταγμένων GPS μέσω αδρανειακών συστημάτων πλοήγησης,

κατηγοριοποιούμε τα περιστατικά ασφαλείας σε δύο (2) μεγάλες κατηγορίες: τα ατυχήματα που προκλήθηκαν από απρόσεκτους ή αμελείς χειριστές (Ενότητα 1.3.1) και τις εσκεμμένες κακόβουλες ενέργειες από έμπειρους χειριστές προκειμένου να διαπράξουν εγκληματικές ή ακόμα και τρομοκρατικές ενέργειες (Ενότητα 1.3.2).

1.3.1 Ατυχήματα με Συστημάτων μη Επανδρωμένων Αεροσκαφών

Τα συνήθη χαρακτηριστικά ενός απρόσεκτου ή αμελή χειριστή ΣμηΕΑ που παρατηρούνται σε ατυχήματα ΣμηΕΑ συνοψίζονται ως εξής:

- Δεν έχει καμία πρόθεση να διακόψει οποιαδήποτε λειτουργία ή να προκαλέσει αναστάτωση, ούτε φυσικά να προκαλέσει ζημιές σε υποδομές, στο περιβάλλον, σε άλλα αγαθά και δεν θέλει να βλάψει κανέναν άνθρωπο.
- Συνήθως τέτοιοι χειριστές δεν είναι γνώστες της νομοθεσίας που διέπει την χρήση των ΣμηΕΑ, είτε σε περίπτωση που την γνωρίζουν, την καταπατούν από δική τους αμέλεια, είτε επειδή υπήρξε κάποια δυσλειτουργία του ΣμηΕΑ και δεν γνώριζαν πως να αντιδράσουν ή τέλος ενδεχομένως να μην είχαν λάβει τα κατάλληλα μέτρα ασφαλείας.

Μερικά αντιπροσωπευτικά παραδείγματα τέτοιων ατυχημάτων είναι τα παρακάτω:

Το δημοφιλέστερο, λόγω των επιπτώσεων που είχε, περιστατικό απρόσεκτου χειριστή, είναι και η εμφάνιση ενός ΣμηΕΑ κοντά στο αεροδρόμιο του Heathrow [19], το οποίο προκάλεσε σοβαρή αναστάτωση στους επιβάτες αλλά και τους υπεύθυνους ασφαλείας του αεροδρομίου. Η έρευνα που ακολούθησε κατέληξε στην σύλληψη ενός άνδρα ο οποίος κατηγορήθηκε για πτήση χωρίς την έγκριση από τον πύργου ελέγχου. Παρόμοιο περιστατικό που δεν έχει λάβει την ίδια δημοσιότητα έχει συμβεί και στο αεροδρόμιο της Ρίγας [20], στην Λετονία όπου λόγω παρουσίας ΣμηΕΑ κοντά στον αεροδιάδρομο αναστάλθηκε η λειτουργία του αεροδρομίου. Στην Ελλάδα, διάφορα περιστατικά έχουν καταγραφεί κοντά στην Βουλή των Ελλήνων και το Μέγαρο Μαξίμου από τουρίστες ή ημεδαπούς που θέλησαν να τραβήξουν κάποιες φωτογραφίες κοντά σε αυτή την απαγορευμένη για ΣμηΕΑ ζώνη (no-fly zone), χωρίς να γνωρίζουν την νομοθεσία [21] [22].

1.3.2 Περιστατικά ασφαλείας με Συστημάτων μη Επανδρωμένων Αεροσκαφών

Η ικανότητα των ΣμηΕΑ να διεισδύουν χωρίς να γίνονται αντιληπτά από τις παραδοσιακές αντιαεροπορικές άμυνες και τα μέτρα ασφαλείας των υποδομών σε συνδυασμό με τις καθιερωμένες αντιλήψεις για το τι είναι η αεράμυνα ή τι συνιστά εύλογη εναέρια απειλή, αποτελεί μια συνεχώς αυξανόμενη ανησυχία, για τους κρατικούς φορείς και τους φορείς επιβολής του νόμου. Μερικά από τα περιστατικά εγκληματικών και τρομοκρατικών ενεργειών με την χρήση ΣμηΕΑ που πήραν δημοσιότητα παρουσιάζονται παρακάτω.

Τα χαρακτηριστικά ενός χειριστή ΣμηΕΑ που έχει ως στόχο την εκτέλεση εγκληματικών ή τρομοκρατικών ενεργειών συνοψίζονται ως εξής:

- Τέτοιου είδους χειριστές μπορεί να είναι ή να μην είναι γνώστες της νομοθεσίας που διέπει την χρήση των ΣμηΕΑ. Παρόλα αυτά λόγω της φύσης των ενεργειών που θέλουν να φέρουν εις πέρας είναι λογικό ότι θα παραβούν κάθε είδους κανονισμό και νόμο για να πετύχουν τον σκοπό τους.
- Στις περισσότερες των περιπτώσεων τέτοιοι χειριστές δεν δείχνουν να ενδιαφέρονται για τις όποιες συνέπειες που θα προκαλέσουν, αφού σκοπός τους είναι είτε να προκαλέσουν πολλαπλές ανθρώπινες ή υλικές απώλειες, είτε να εκτελέσουν τις εγκληματικές του ενέργειες με κάθε κόστος.

Χρήση ΣμηΕΑ για εγκληματικές ενέργειες

Εικόνα 12: Μεξικάνικα καρτέλ διακινούν ναρκωτικά με χρήση ΣμηΕΑ
Πηγή: AP Photo/Secretaria de Seguridad Pública Municipal de Tijuana

Το 2017, ένας συνοριοφύλακας στην Πολιτεία του Σαν Ντιέγκο, άκουσε τον ήχο από τις έλικες ενός ΣμηΕΑ το οποίο περνούσε τον φράκτη των συνόρων μεταξύ Η.Π.Α. και Μεξικού και ο οποίος επικοινώνησε αμέσως με τους συναδέλφους του, οι οποίοι στη συνέχεια βρήκαν και συνέλαβαν έναν άνδρα, που όπως αποδείχθηκε αργότερα, μετέφερε 13 κιλά ναρκωτικών ουσιών με χρήση του ΣμηΕΑ [23]. Ένα άλλο περιστατικό εγκληματικής ενέργειας με την χρήση ΣμηΕΑ συναντάται στο Ηνωμένο Βασίλειο, όπου ένας νεαρός συνελήφθη για πρώτη φορά για παράνομη διακίνηση υλικών, ναρκωτικών και όπλων μέσα σε φυλακές με την χρήση ΣμηΕΑ [24]. Ο εν λόγω χειριστής είχε φροντίσει να καλύψει τα φώτα του ΣμηΕΑ που χρησιμοποιούσε, για να μην γίνεται αντιληπτό και να μπορεί να διακινήσει καπνό και ναρκωτικά σε φυλακές της Αγγλίας. Παρόλα αυτά, οι αρχές τον εντόπισαν και τον συνέλαβαν. Στην Ελλάδα, παρόμοια περιστατικά είχαν καταγραφεί στις φυλακές της Λάρισας [25] και των Τρικάλων [26], από επίδοξους χειριστές που θέλησαν να περάσουν ναρκωτικά, λεφτά και κινητά τηλέφωνα σε έγκλειστους, οι οποίοι βέβαια και συνελήφθησαν.

Χρήση ΣμηΕΑ για τρομοκρατικές ενέργειες

Εικόνα 13: Η επίθεση με χρήση ΣμηΕΑ στις πετρελαϊκές εγκαταστάσεις της Σαουδικής Αραβίας
Πηγή: Ειδησεογραφικό πρακτορείο Reuters

Τα ΣμηΕΑ, εκτός των εγκληματικών ενεργειών που έχουν χρησιμοποιηθεί κατά καιρούς, έχουν καταγραφεί και ορισμένες περιπτώσεις τρομοκρατικών ενεργειών με την συμβολή τους. Χαρακτηριστικό παράδειγμα αποτελεί η απόπειρα ανθρωποκτονίας του προέδρου της Βενεζουέλας Μαδούρο [27]. Ο Μαδούρο μιλούσε σε στρατιωτική εκδήλωση στο Καράκας όταν

τουλάχιστον δύο (2) ΣμηΕΑ που έφεραν εκρηκτικά εξερράγησαν στον αέρα και δεκάδες μέτρα μακριά από την εκδήλωση. Ακόμη είναι χαρακτηριστικό παράδειγμα του πλήγματος που θα μπορούσαν να φέρουν τα ΣμηΕΑ σε περιπτώσεις κακόβουλης χρήσης είναι η επίθεση από σμήνος ΣμηΕΑ στις κρατικές πετρελαϊκές εγκαταστάσεις στην Abqaiq–Khurais της Σαουδικής Αραβίας [28]. Το 2019, ένα σμήνος ΣμηΕΑ φέροντας εκρηκτικά χρησιμοποιήθηκε για να επιτεθεί σε εγκαταστάσεις επεξεργασίας πετρελαίου στο Abqaiq, το οποίο είχε ως αποτέλεσμα να προκληθεί μεγάλη πυρκαγιά στη μονάδα επεξεργασίας. Οι ζημιές που προκλήθηκαν αναφορικά με την επισκευή αλλά και από την μείωση της παραγωγής του πετρελαίου ήταν αρκετά μεγάλες, σε σημείο που αποσταθεροποίησαν τις παγκόσμιες χρηματοπιστωτικές αγορές.

2. Ψηφιακή Εγκληματολογία

Η ανάπτυξη νέων τεχνολογιών εκτός από τα οφέλη αναφορικά με την βελτίωση του βιοτικού επιπέδου των ανθρώπων καθώς και την διευκόλυνση και ευκολία καθημερινών εργασιών, επικοινωνιών, κτλ., μπορεί να φέρει και νέες απειλές για την ασφάλεια της κοινωνίας. Η ανάπτυξη νέων τεχνολογιών μπορεί να συνεισφέρει στην εύρεση νέων τεχνικών και μεθόδων διάπραξης παράνομων ενεργειών για τους επίδοξους εγκληματίες, όπως αυτό αποτυπώθηκε και στο προηγούμενο κεφάλαιο με την χρήση ΣμηΕΑ. Η εξέλιξη, λοιπόν, που υπήρξε στον τομέα των ΣμηΕΑ κυρίως τα τελευταία είκοσι (20) έτη, οδήγησε στην ανάπτυξη και εμπορευματοποίηση των συστημάτων αυτών για διάφορες εφαρμογές, καθώς επίσης και στην εύκολη εύρεση επιμέρους μερών και εξαρτημάτων για την κατασκευή αυτοσχέδιων ΣμηΕΑ. Με αυτόν τον τρόπο η τεχνολογία αυτή έγινε προσιτή για αρκετούς νόμιμους, συμπεριλαμβανομένων των επαγγελματιών, αλλά και για παράνομους χρήστες.

Με τον όρο ψηφιακές συσκευές, αναφερόμαστε στα κινητά τηλέφωνα, στους ηλεκτρονικούς υπολογιστές, στα tablet και οποιαδήποτε άλλη ψηφιακή συσκευή που περιέχει μνήμη, όπως για παράδειγμα τα ΣμηΕΑ. Σε περιπτώσεις, λοιπόν, που γίνεται μη νόμιμη χρήση των παραπάνω ψηφιακών συσκευών έχουν οριστεί συγκεκριμένες διαδικασίες για την άντληση επίσημων αποδεικτικών στοιχείων για την χρήση τους ακόμα και σε ποινικές υποθέσεις. Τα αποδεικτικά στοιχεία αποτελούνται από οποιοδήποτε ψηφιακό αρχείο που έχει παραχθεί ή βρίσκεται στις ψηφιακές συσκευές του χρήστη. Η ανάκτηση αυτών των αρχείων ποικίλλει αναλόγως της ψηφιακής συσκευής όπως για παράδειγμα στον Η/Υ, στον οποίο, τα αποδεικτικά στοιχεία δύναται να βρεθούν από πηγές όπως το ηλεκτρονικό ταχυδρομείο, το ιστορικό περιήγησης, τα αρχεία που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή, κ.α. Για όλα αυτά τα ψηφιακά αποδεικτικά στοιχεία που αναφέρθηκαν χρησιμοποιείται ο όρος ψηφιακά πειστήρια [29].

Ένας σημαντικός παράγοντας μιας εγκληματολογικής έρευνας αφορά και τα αποδεικτικά αυτά αρχεία που πιθανότατα να οδηγήσουν στην απόδειξη ενοχής ή αθώωση του εκάστοτε εμπλεκόμενου χρήστη. Για την ανάκτηση των ψηφιακών πειστηρίων υπάρχουν διάφορες τεχνικές χωρίς αλλοίωση των στοιχείων και οι οποίες εξαρτώνται και πάλι από το είδος της υπό-έρευνας ψηφιακής συσκευής. Οι τεχνικές αυτές, προφανώς, βοηθάνε στον μέγιστο βαθμό τον κλάδο της εγκληματολογίας καθώς και την δουλειά των φορέων επιβολής του νόμου [30].

Η έρευνα για την ανάκτηση και συλλογή αποδεικτικών στοιχείων θα πρέπει να είναι ιδιαίτερα προσεκτική και τέτοια ώστε να μην είναι αμφισβητήσιμη, καθώς επρόκειτο να χρησιμοποιηθεί και να προσκομισθεί στο δικαστήριο για την επιβολή ποινών ή αθώωση κατηγορούμενων [31].

Παρόλα αυτά, παρόμοιες διαδικασίες εύρεσης πειστηρίων χρησιμοποιούνται και για άλλους σκοπούς, όπως για παράδειγμα ελέγχους και έρευνες στο εσωτερικό μίας εταιρείας ύστερα από κάποια κυβερνοεπίθεση ή απώλεια δεδομένων. Επίσης, με παρόμοιο τρόπο λειτουργούν και οι πραγματογνώμονες που καλούνται να φέρουν ψηφιακά πειστήρια για την εκάστοτε υπόθεση που αναλαμβάνουν, όπως επίσης η ανάλυση των ψηφιακών αυτών αρχείων λαμβάνει χώρα από προγραμματιστές και για σκοπούς βελτίωσης λογισμικού, επιδιορθώσεων μετά από δυσλειτουργίες, κτλ. Εν κατακλείδι, η ψηφιακή εγκληματολογία, οι αρχές της και η ανάλυση των ψηφιακών αρχείων ωφελεί κάθε είδους έρευνα και όχι μόνο την δικαστική [29].

2.1 Γενικά

Με τον όρο Ψηφιακή Εγκληματολογία (Digital Forensics) αναφερόμαστε στην επιστήμη που αποτελείται από την συλλογή και διατήρηση, την εξέταση, την ανάλυση και η αναφορά ψηφιακών δεδομένων με νομικά αποδεκτό τρόπο [32]. Τα δεδομένα αυτά ενδέχεται να βρίσκονται σε ψηφιακές συσκευές και υπάρχει η πιθανότητα συσχέτισης τους με κάποια παράνομη, εγκληματική ενέργεια. Αυτού του είδους η έρευνα ωστόσο δεν αποτελεί μόνο μέσο ανίχνευσης ενός εγκλήματος που έχει διαπραχθεί αλλά αποτελεί και μέσο πρόληψης. Ο όρος Ψηφιακή Εγκληματολογία αρχικά χρησιμοποιήθηκε για να περιγράψει την εγκληματολογική έρευνα αναφορικά με τους υπολογιστές (Computer Forensics), ωστόσο, με την πάροδο του

χρόνου και την εξέλιξη της τεχνολογία επεκτάθηκε για να συμπεριλάβει όλες τις ψηφιακές συσκευές που είναι ικανές να αποθηκεύσουν ψηφιακά δεδομένα [29] [33].

Η Ψηφιακή Εγκληματολογία και η έρευνα είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς. Αποτελεί έναν αποδοτικό τρόπο εύρεσης και συλλογής αποδεικτικών στοιχείων για υποθέσεις τόσο ποινικού όσο και αστικού χαρακτήρα. Οι ποινικές υποθέσεις σχετίζονται με πιθανή παραβίαση νόμων που ορίζονται από την νομοθεσία και διώκονται από το κράτος. Χαρακτηριστικά παραδείγματα τέτοιων αδικημάτων είναι η κλοπή ή δολοφονία. Αντιθέτως, οι υποθέσεις αστικού κώδικα ασχολούνται με την προστασία δικαιωμάτων κάθε είδους, περιουσίας ακόμα και με διαφορές μεταξύ εταιρειών.

2.2 Ψηφιακό Πειστήριο

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, τα ψηφιακά πειστήρια (Digital Evidence) διαδραματίζουν τον πιο σημαντικό ρόλο στην έκβαση του αποτελέσματος μιας έρευνας. Οι B. Carrier και E. Spafford, όρισαν τα ψηφιακά πειστήρια ως τις πληροφορίες που δύναται να υποστηρίξουν ή να διαψεύσουν μια υπόθεση [34]. Τέτοιου είδους πειστήρια μπορούν να συλλεχθούν από περιπτώσεις όπου εμπλέκονται ψηφιακές συσκευές που παράγουν ή αποθηκεύουν τα αντίστοιχα ψηφιακά δεδομένα. Με αυτόν τον τρόπο τα στοιχεία αυτά προσφέρουν μια ψηφιακή διάσταση σε μια εγκληματολογική έρευνα και ο ερευνητής ή πραγματογνώμονας που συμμετέχει στην συλλογή τους μπορεί να εξάγει χρήσιμα συμπεράσματα για την έκβαση της υπόθεσης, αναγνωρίζοντας σε μεγάλο βαθμό το προφίλ του ατόμου που είναι υπεύθυνο για την πραγματοποίηση ή μη παράνομων ενεργειών. Τα ψηφιακά πειστήρια είναι ιδιαίτερα ευπαθή δεδομένα τα οποία είναι εύκολο να παραποιηθούν ή και να καταστραφούν από απρόσεκτο χειρισμό. Για αυτό τον λόγο, υπάρχουν διαδικασίες και μέτρα προστασίας που πρέπει να λαμβάνονται υπόψη και να εφαρμόζονται, ούτως ώστε να διατηρηθεί ακέραια η αρχική τους κατάσταση για μεταγενέστερο επανέλεγχο, για πιστοποίηση του αποτελέσματος, κτλ. Οι τύποι πειστηρίων που ενδέχεται να εμφανιστούν ποικίλουν, αναλόγως της υπό-έρευνας ψηφιακής συσκευής. Ο Henseler [35] κατηγοριοποίησε τα υπολογιστικά συστήματα που περιέχουν τέτοιου είδους δεδομένα, ως εξής:

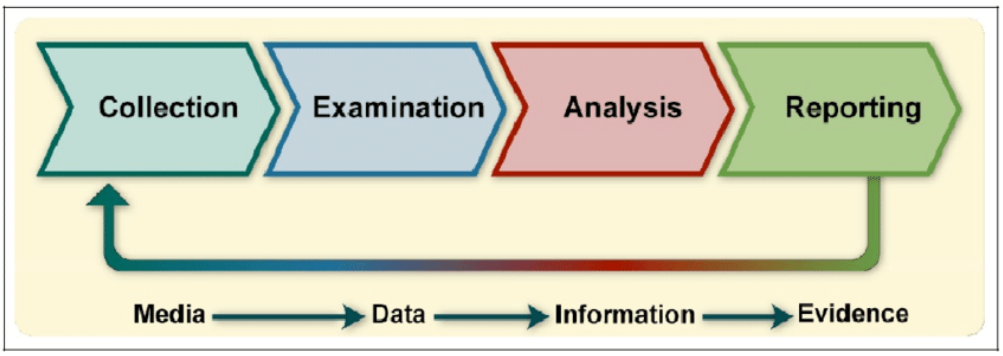
- Ανοιχτά υπολογιστικά συστήματα (Open computer systems): Στην κατηγορία αυτή περιλαμβάνονται όλοι οι κοινοί ηλεκτρονικοί υπολογιστές. Με την πολυεπίπεδη εξέλιξη της τεχνολογίας, βελτιώνονται σημαντικά και τα υπολογιστικά συστήματα καθώς και τα επιμέρους συστήματά τους, όπως για παράδειγμα η ραγδαία αύξηση του χώρου αποθήκευσης των σκληρών δίσκων λόγω της κατακόρυφης αύξησης της παραγόμενης ψηφιακής πληροφορίας και δεδομένων. Αυτό συνεπάγεται ότι σε μια έρευνα digital forensics είναι διαθέσιμη ακόμη περισσότερη πληροφορία που δυνητικά θα μπορούσε να χρησιμοποιηθεί ως ψηφιακό πειστήριο.
- Συστήματα Επικοινωνίας (Communication systems): Στην κατηγορία αυτή περιλαμβάνονται τα τηλεφωνικά συστήματα, τα ασύρματα δίκτυα επικοινωνίας και το διαδίκτυο. Ο εκάστοτε ερευνητής αναλύοντας δεδομένα από τέτοιου είδους συστήματα, είναι σε θέση να αντλήσει πληροφορίες για την ταυτότητα του αποστολέα ή/και του παραλήπτη, τον χρόνο που έγινε μια κλήση ή στάλθηκε ένα μήνυμα ή ακόμα και ένα ηλεκτρονικό ταχυδρομείο (email), κτλ.
- Ενσωματωμένα Υπολογιστικά Συστήματα (Embedded computer systems): Στην κατηγορία αυτή συγκαταλέγονται τα κινητά τηλέφωνα, tablet, έξυπνες κάρτες, ψηφιακές συσκευές με δυνατότητα εντοπισμού θέσης (GNSS) και οποιαδήποτε γενικά συσκευή ή σύστημα εμπεριέχει υπολογιστικό σύστημα και μπορεί να παράγει ή να προσφέρει πληροφορίες. Στην σύγχρονη εποχή, τέτοιες συσκευές και συστήματα είναι πλέον αρκετά μέσω της εξέλιξης της τεχνολογίας και ειδικά στον τομέα του Διαδικτύου των Πραγμάτων (Internet of Things - IoT). των Πραγμάτων και μπορούν να επικοινωνούν μεταξύ τους.

2.3 Διαδικασία Εγκληματολογικής έρευνας

Οι προσεγγίσεις και μεθοδολογίες που χρησιμοποιούνται από τους ερευνητές της Ψηφιακής Εγκληματολογίας ποικίλουν ανάλογα με την ψηφιακή συσκευή και συνάδουν με την εξέλιξη της τεχνολογίας. Βιβλιογραφικά, υπάρχουν αρκετά μοντέλα και μεθοδολογίες που έχουν προταθεί κατά καιρούς, καθώς οι παράγοντες που επηρεάζουν μια έρευνα είναι αρκετοί και έτσι ο εκάστοτε ερευνητής οφείλει να προσαρμόζει την έρευνά του ανάλογα με την περίπτωση. Ανεξαρτήτως όμως του αριθμού των προτεινόμενων μοντέλων και μεθοδολογιών, υπάρχουν κάποια «γενικά» βήματα και διαδικασίες που ακολουθούνται από όλες τις μεθοδολογίες με κάποιες, μικρές, ή ακόμα και μεγάλες παραλλαγές, προσθέτοντας συνήθως επιπρόσθετα βήματα.

Σύμφωνα με το National Institute of Standards and Technology (NIST), τα βήματα που πρέπει να εφαρμόζονται σε κάθε έρευνα Ψηφιακής Εγκληματολογίας είναι τα εξής:

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



Εικόνα 14: Το μοντέλο τεσσάρων βημάτων για την ψηφιακή εγκληματολογία από το NIST

2.3.1 Συλλογή Δεδομένων

Κατά το πρώτο στάδιο του μοντέλου του NIST, λαμβάνει χώρα η Συλλογή Δεδομένων (Data Collection), κατά την οποία ο ερευνητής καλείται να αναγνωρίσει τα υποσυστήματα και τις πηγές από τις οποίες μπορεί να αντλήσει πληροφορίες και δεδομένα. Τα υποσυστήματα αυτά και οι πηγές μπορεί να είναι αρκετές, το οποίο εξαρτάται από την κάθε περίπτωση, οπότε μια σωστή επιλογή των πηγών που θα προσφέρουν δεδομένα ερευνητικής αξίας, είναι απαραίτητη. Οι πιο κοινές πηγές τέτοιων δεδομένων περιλαμβάνουν ηλεκτρονικούς υπολογιστές, εξυπηρετητές, δίκτυα, κ.α.. Μέσω αυτών, ο ερευνητής θα μπορέσει να προσεγγίσει για να ελέγξει τυχόν δεδομένα και πληροφορίες, τον σκληρό δίσκο του συστήματος, τις κάρτες μνήμης, τις εξωτερικές θύρες USB, κτλ. Αναλόγως την εκάστοτε έρευνα, χρήσιμα δεδομένα μπορούν να βρεθούν σε κινητά τηλέφωνα, ψηφιακές κάμερες, αυτοκίνητα τελευταίας τεχνολογίας και σε όλες τις έξυπνες συσκευές που συγκαταλέγονται σε αυτές του Διαδικτύου των Πραγμάτων. Ο ερευνητής μέσα από την εμπειρία του πρέπει να εντοπίσει και κατηγοριοποιήσει σύμφωνα με την σημαντικότητα της πληροφορίας που φέρει, οποιαδήποτε συσκευή μπορεί να του προσφέρει κάποια σημαντική πληροφορία.

Στο παρών στάδιο της συλλογής δεδομένων, είναι πολύ σημαντικό να εντοπιστούν και να συλλεχθούν δεδομένα που μπορούν να αποθηκευτούν ακόμα και στην μνήμη RAM της συσκευής, στο δίκτυο, ή σε σημεία που σε ενδεχόμενο κλείσιμο ή επανεκκίνηση της συσκευής, τα δεδομένα αυτά θα χαθούν.

Πολλές φορές και λόγω της δυσκολίας πρόσβασης σε χρήσιμα για την έρευνα δεδομένα, όπως για παράδειγμα αρχεία καταγραφής από κάποιον πάροχο Διαδικτύου, είναι σύνηθες να λαμβάνονται κάποια προληπτικά μέτρα για να συλλέγονται δεδομένα που ενδεχομένως 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 ρυθμίζονται με τέτοιον τρόπο ώστε να καταγράφουν τις αλλαγές που μπορεί να προκύψουν στις ρυθμίσεις ασφαλείας του συστήματος. Βέβαια, τα μέτρα αυτά, θα πρέπει να σχεδιαστούν βασισμένα πρωτίστως στον σεβασμό προς την ιδιωτικότητα του εκάστοτε χρήστη.

Αφού, λοιπόν, ο ερευνητής εντοπίσει τις πιθανές πηγές δεδομένων, θα πρέπει στην συνέχεια να αποκτήσει τα δεδομένα που χρειάζεται ώστε να τα μελετήσει. Το NIST διαχωρίζει αυτήν την διεργασία σε τρεις μικρότερες διεργασίες, και πιο συγκεκριμένα:

- **Σχεδιασμός**: Ο Σχεδιασμός αφορά την κατηγοριοποίηση και διαχωρισμό των ψηφιακών μέσων και συστημάτων που ο ερευνητής έχει εντοπίσει. Για τον αρτιότερο διαχωρισμό των δεδομένων, ο ερευνητής καλείται να λάβει υπόψη παράγοντες που επηρεάζουν την σημαντικότητα και χρησιμότητα των δεδομένων που θα αντλήσει από κάθε πηγή, το οποίο σε μεγάλο βαθμό εξαρτάται από την φύση του συμβάντος καθώς και από την εμπειρία του εκάστοτε ερευνητή. Σημαντικός επίσης παράγοντας που πρέπει να συνυπολογιστεί σε αυτή την διεργασία για την κατηγοριοποίηση είναι και η ρευστότητα των δεδομένων, όπως στην περίπτωση της μνήμης RAM. Τα δεδομένα που είναι πιο ευάλωτα σε αλλαγές, είναι σύνηθες να συλλέγονται κατά απόλυτη προτεραιότητα. Τέλος, ένας ακόμα παράγοντας που συμβάλλει στην ορθή κατηγοριοποίηση των συλλεχθέντων δεδομένων είναι η προσπάθεια και ο χρόνος που απαιτείται για την συλλογή αυτών, καθώς και οι εξαρτήσεις από συμβαλλόμενα μέρη (π.χ. πάροχος Διαδικτύου), οι οποίες μπορούν να καθυστερήσουν αρκετά την διαδικασία.
- **Ανάκτηση Δεδομένων**: Η ανάκτηση των δεδομένων πρέπει να είναι τέτοια ώστε να διασφαλίζει την αρχική μορφή και ακεραιότητα τους. Για τον λόγο αυτό, ο συνήθης τρόπος που ακολουθείται είναι με την χρήση ειδικών εργαλείων της ψηφιακής εγκληματολογίας. Η διεργασία αυτή δύναται να πραγματοποιηθεί είτε τοπικά, είτε μέσω του δικτύου.
- **Επαλήθευση των Δεδομένων**: Η τελευταία διεργασία, μετά την ανάκτηση των δεδομένων, είναι η εξασφάλιση και η επαλήθευση της ακεραιότητάς τους. Η διεργασία αυτή πραγματοποιείται για δύο (2) λόγους, αρχικά, για την επαλήθευση ότι δεν έχει χαθεί ή παραποιηθεί κάποιο δεδομένο κατά την διάρκεια της ανάκτησής τους, καθώς, επίσης, και για νομικούς σκοπούς, αποδεικνύοντας και επιβεβαιώνοντας την ακεραιότητα των δεδομένων ούτως ώστε να μπορούν αυτά να χρησιμοποιηθούν για αποδεικτικά στοιχεία, εφόσον χρειαστεί. Και σε αυτή την διεργασία, η επαλήθευση πραγματοποιείται με ειδικά εργαλεία της ψηφιακής εγκληματολογίας, όπου μέσω συγκεκριμένων μεθόδων συγκρίνονται τα αρχικά στοιχεία με αυτά που ανάκτησε ο ερευνητής κατά την διάρκεια της έρευνας.

2.3.2 Εξέταση Δεδομένων

Το δεύτερο στάδιο της μεθόδου NIST περιλαμβάνει την Εξέταση (Examination). Σε αυτό το στάδιο λαμβάνει χώρα η αξιολόγηση των συλλεχθέντων δεδομένων, έτσι ώστε να εξαχθούν χρήσιμες πληροφορίες για αυτά. Ο όγκος των δεδομένων, συνήθως, είναι αρκετά μεγάλος και θεωρείται δύσκολο αλλά και χρονοβόρο να εξεταστούν και αξιολογηθούν τα δεδομένα αυτά χειροκίνητα. Όπως στις αντίστοιχες περιπτώσεις του σταδίου Ανάκτησης, τα εργαλεία της ψηφιακής εγκληματολογίας υποβοηθούν την έρευνα και τον ερευνητή για την ταχύτερη αξιολόγηση των δεδομένων. Σύμφωνα με τους Zareen, Waqar, & Aslam [36] ο τρόπος γρηγορότερης εξέτασης των δεδομένων μπορεί να επιτευχθεί ως εξής:

- Μέσω αναζήτησης με λέξεις κλειδιά που μπορούν να βρουν κείμενο ή κάποιο μοτίβο
- Με φιλτράρισμα ανά διαφορετικό τύπο δεδομένων όπως π.χ. κείμενο ,ήχος, εικόνα, βίντεο, κ.ο.κ.

Στις μέρες μας, με την ανάπτυξη των τεχνολογικών πεδίων των Μεγάλων Δεδομένων (Big Data) καθώς και με την συνεχόμενη ανάπτυξη της Τεχνητής Νοημοσύνης (Artificial Intelligence), γίνεται ακόμη πιο εύκολη η αξιολόγηση για τον ερευνητή, καθώς έχουν δοθεί αρκετές

προσπάθειες για την αυτοματοποιημένη εξαγωγή χρήσιμης πληροφορίες μέσα από τεράστιο όγκο δεδομένων.

2.3.3 Ανάλυση Δεδομένων

Το τρίτο στάδιο της μεθόδου NIST αφορά την Ανάλυση των Δεδομένων (Analysis). Αμέσως μετά την εξέταση των δεδομένων, επέρχεται η ανάλυσή τους, κατά την οποία ο εκάστοτε ερευνητής προσπαθεί να εξαγάγει κάποια χρήσιμα συμπεράσματα στηριζόμενος στις πληροφορίες που εξέτασε κατά την διάρκεια του δεύτερου σταδίου. Η ανάλυση περιλαμβάνει την συγκέντρωση σημαντικών πληροφοριών που πρέπει να λάβει υπόψη του, έτσι ώστε να μπορέσει να αναπαραστήσει από την αρχή την εξέλιξη του συμβάντος. Αυτό θα οδηγήσει στην αποτύπωση με χρονολογική σειρά, των ενεργειών που έγιναν, τους χρήστες που ενεπλάκησαν, την ευπάθεια που εκμεταλλεύτηκε, κτλ.

2.3.4 Αναφορά

Το τελευταίο στάδιο της μεθόδου NIST εμπεριέχει την Αναφορά (Reporting), κατά την οποία γίνεται η αναφορά των αποτελεσμάτων της έρευνας σε συνοπτική και ευανάγνωστη μορφή. Η αναφορά αυτή, περιλαμβάνει πληροφορίες για τα δεδομένα που έχει αποκτήσει ο ερευνητής συνοδευόμενα από την ημερομηνία, την ώρα, το μέρος που τα σύλλεξε, την μέθοδο και εργαλεία που χρησιμοποίησε για την συλλογή και ανάλυση τους, κ.ο.κ. Στις περισσότερες περιπτώσεις η αναφορά αυτή γίνεται γραπτώς και καταχωρείται στο αρχείο π.χ. της εταιρίας ή ακόμα μπορεί να συνοδεύει την δικογραφία για κάποια υπόθεση σαν αποδεικτικό στοιχείο. Σε περιπτώσεις που ένα γεγονός έχει παραπάνω από μία ερμηνείες, ο ερευνητής υποχρεούται να τις αναφέρει όλες στην αναφορά του, με την απαραίτητη λεπτομέρεια και ακρίβεια για την καθεμία από αυτές, χωρίς να παραλείπεται κάποια πληροφορία που ενδεχομένως να είναι σημαντική [37].

2.4 Κατηγορίες Ψηφιακής Εγκληματολογίας

Η επιστήμη της ψηφιακής εγκληματολογίας δεν περιορίζεται μόνο στην άντληση, ανάκτηση και ανάλυση των δεδομένων του ηλεκτρονικού υπολογιστή. Όπως αναφέρθηκε στην αρχή της Ενότητας, η τεχνολογική εξέλιξη καθώς και η εύκολη πρόσβαση στην τεχνολογία, αποτελεί προνόμιο όχι μόνο για την κοινωνία αλλά και για τους επίδοξους κακόβουλους δράστες που εκμεταλλεύονται τα τεχνολογικά επιτεύγματα για την πραγματοποίηση των δικών τους παράνομων ενεργειών. Λόγω της διαφορετικότητας των ψηφιακών συσκευών και συστημάτων που ενδέχεται να χρησιμοποιηθούν σε παράνομες ενέργειες όπως για παράδειγμα «έξυπνα» τηλέφωνα και tablets, Η/Υ, τελευταίας τεχνολογίας αυτοκίνητα, κ.α., είναι εύκολα κατανοητό πως η ψηφιακή εγκληματολογία και η διαδικασία αυτής δεν είναι ίδια για καθεμία από αυτές τις περιπτώσεις. Εξειδικευμένες διαδικασίες και μεθοδολογίες έχουν παρουσιαστεί για τα διάφορα αυτά συστήματα, με σκοπό την ευκολότερη πραγματοποίηση και τυποποίηση της εκάστοτε έρευνας. Μέχρι σήμερα, αναγνωρίζονται, λοιπόν, πέντε (5) διαφορετικοί τομείς ψηφιακής εγκληματολογίας, βάσει σημαντικότητας και συχνότητας ερευνών [29] [33]:

- **Ψηφιακή Εγκληματολογία υπολογιστών (Computer Forensics)** που αποτελεί ίσως τον πιο διαδεδομένο τομέα ψηφιακής εγκληματολογίας. Ασχολείται με ένα ευρύ φάσμα πληροφοριών περιλαμβάνοντας από τα αρχεία καταγραφής, όπως το ιστορικό περιήγησης στο διαδίκτυο, μέχρι τα αρχεία που βρίσκονται στον δίσκο ή στην μνήμη του υπολογιστή. Στόχος του τομέα αυτού είναι η ερμηνεία και ανάλυση της τρέχουσας κατάστασης στην οποία βρίσκεται ο Η/Υ, καθώς και η εύρεση ψηφιακών πειστηρίων [38].
- **Ψηφιακή Εγκληματολογία δικτύων (Network Forensics)**. Ασχολείται με την παρακολούθηση και ανάλυση της κίνησης του δικτύου. Το δίκτυο μπορεί να είναι είτε το τοπικό(local network) είτε το πιο διευρυμένο δίκτυο (wide-area network), είτε ακόμα και το διαδίκτυο (internet). Η ανάλυση σε αυτή την περίπτωση λαμβάνει χώρα μετά από

κάποια κυβερνοεπίθεση, για τον προσδιορισμό τυχόν ευπαθειών, για την έρευνα της κινητικότητας στο δίκτυο που ενδεχομένως παρεμποδίζει την παράδοση πακέτων, κ.ο.κ.

- **Ψηφιακή Εγκληματολογία κινητής τηλεφωνίας (Mobile Forensics)**, η οποία ασχολείται αποκλειστικά με τις συσκευές κινητής τηλεφωνίας. Η διαφορά του συγκεκριμένου τομέα σε σχέση με τα συστήματα που ανήκουν στην πρώτη κατηγορία είναι ότι μία συσκευή κινητού τηλεφώνου διαθέτει ενσωματωμένο σύστημα επικοινωνίας. Επομένως, η έρευνα του τομέα αυτού επικεντρώνεται κυρίως σε απλά δεδομένα, όπως τα δεδομένα κλήσεων ή γραπτών μηνυμάτων.
- **Ψηφιακή Εγκληματολογία ανάλυσης δεδομένων (Forensic Data Analysis)**. Ο συγκεκριμένος τομέας εξετάζει και αναλύει δεδομένα που σχετίζονται κυρίως με οικονομικές παραβάσεις και παράνομες ενέργειες. Σκοπός της έρευνας είναι η εύρεση αποδεικτικών στοιχείων που θα οδηγήσουν σε εμπεριστατωμένα συμπεράσματα αναφορικά με την επαίσχυντη αυτή πράξη, σύμφωνα με την αρχή του «follow-the-money». Τα δεδομένα προέρχονται συνήθως από συστήματα εφαρμογών.
- **Ψηφιακή Εγκληματολογία βάσεων δεδομένων (Database Forensics)**: Ο συγκεκριμένος τομέας αφορά την έρευνα και μελέτη βάσεων δεδομένων καθώς και των στοιχείων που εμπεριέχονται ή προκύπτουν από αυτές. Χαρακτηριστικότερο παράδειγμα μιας τέτοιας έρευνας είναι ο εντοπισμός συναλλαγών εντός ενός συστήματος βάσεων.

Καθένας από τους παραπάνω τομείς εξειδικεύεται σε ένα συγκεκριμένο κομμάτι της ψηφιακής εγκληματολογίας. Ωστόσο, στις περισσότερες περιπτώσεις, για την διενέργεια ολοκληρωμένης έρευνας μίας υπόθεσης θα χρησιμοποιηθούν περισσότεροι από έναν τομείς. Εκτός από τους παραπάνω τομείς ψηφιακής εγκληματολογίας, υπάρχουν και άλλοι «υπο-τομείς» που βασίζονται στις αρχές των πέντε (5) προαναφερθέντων, είτε συνδυάζουν, τεχνικές και μεθοδολογίες από αυτούς για να φέρουν εις πέρας την έρευνα [39]. Ένας από αυτούς είναι ο «νεοσύστατος» τομέας της Ψηφιακής Εγκληματολογίας ΣμηΕΑ (Drone Forensics) και ο οποίος είναι το αντικείμενο μελέτης της παρούσας διατριβής. Περισσότερες πληροφορίες για τα Drone Forensics ακολουθούν στην επόμενη ενότητα.

3. Drone forensics

3.1 Γενικά

Σε ενδεχόμενη εμπλοκή ενός ΣμηΕΑ σε ένα ατύχημα ή σε μια παράνομη ενέργεια είναι ενδεδειγμένο να πραγματοποιηθεί μια έρευνα ψηφιακής εγκληματολογίας [40], αμέσως μετά το συμβάν στα κατασχεθέντα ή/και με ζημιά ΣμηΕΑ [41]. Με αυτόν τον τρόπο καθίσταται εφικτό να καθοριστεί η διαδρομή που έχει διανύσει το ΣμηΕΑ, να αποτυπωθούν το σημείο και ο χρόνος εκκίνησης, το σημείο του χειριστή, το φορτίο, όπως επίσης και άλλες χρήσιμες πληροφορίες που θα οδηγήσουν στην αποκωδικοποίηση του συμβάντος.

Η ολοκληρωμένη διαδικασία Drone Forensics, όμως, δεν περιλαμβάνει μόνο την ανάλυση ψηφιακών πειστηρίων, αλλά και την αναζήτηση φυσικών πειστηρίων, όπως για παράδειγμα εύρεση DNA στην συσκευή. Αναφορικά με την ψηφιακή εγκληματολογία και για να κατανοηθεί πλήρως ο βαθμός δυσκολίας μιας τέτοιας έρευνας εν αντιθέσει με πολλές άλλες ψηφιακές συσκευές, είναι απαραίτητο να καταγραφούν οι συσχετιζόμενες συσκευές, αφού καθεμία από αυτές απαιτούν διαφορετικές μεθόδους υποστήριξης για την άντληση και ανάλυση των δεδομένων. Αυτές οι συσκευές ή πηγές δεδομένων θα μπορούσαν να είναι:

- Ο επίγειος σταθμός ελέγχου (Remote controller), ο οποίος χρησιμοποιείται από τον χειριστή για να ελέγξει το ΣμηΕΑ
- Κινητό τηλέφωνο ή tablet (Mobile/Tablet device), οι οποίες σε ορισμένα μοντέλα ΣμηΕΑ χρησιμοποιούνται για την μετάδοση του βίντεο και τηλεμετρίας που παρέχονται από το ΣμηΕΑ
- Γυαλιά προβολής πρώτου προσώπου (First Person View Googles), τα οποία ενδέχεται να χρησιμοποιηθούν για τον έλεγχο ενός ΣμηΕΑ αντί του επίγειου σταθμού ελέγχου, εφόσον το μοντέλο τα υποστηρίζει
- Κάρτες μνήμης (Memory Cards), οι οποίες αποτελούν αφαιρούμενα μέσα και χρησιμοποιούνται για τη διατήρηση φωτογραφιών και βίντεο που τραβήχτηκαν κατά την διάρκεια της πτήσης. Οι κάρτες μνήμης ενδέχεται επίσης να περιέχουν δεδομένα σχετικά με την διαδρομής της πτήσης, καθώς επίσης και γεωγραφικά χαρακτηριστικά των φωτογραφιών που τραβήχτηκαν.
- Αποθήκευση στο νέφος (Cloud Storage), το οποίο, αναλόγως το μοντέλο, ενδέχεται να μπορεί να χρησιμοποιήσει με σκοπό την αποθήκευση φωτογραφιών ή βίντεο μέσω υπηρεσιών αποθήκευσης στο νέφος, όπως για παράδειγμα το iCloud.

Αυτό καθιστά σαφές πως ενώ το ίδιο το ΣμηΕΑ αποτελεί την κύρια πηγή αποδεικτικών στοιχείων σε μια έρευνα, είναι εξίσου ζωτικής σημασίας οι δευτερεύουσες πηγές αποδεικτικών στοιχείων όπως το κινητό τηλέφωνο/tablet και οι κάρτες μνήμης οι οποίες θα πρέπει να διατηρούνται ασφαλείς για να συλλεχθεί και αναλυθεί η ολοκληρωμένη εικόνα του συμβάντος. Σε πολλές περιπτώσεις η πληροφορία που αποθηκεύεται στις συσχετιζόμενες συσκευές είναι η ίδια που υπάρχει και στο «blackbox» του ΣμηΕΑ, παρόλα αυτά, είναι σημαντικό να συλλεχθούν όσο το δυνατόν περισσότερες πληροφορίες για το περιστατικό πριν την ανάλυσή τους. Ορισμένα από αυτά τα αναγνωριστικά μπορεί να φαίνονται περιττά στην αρχή, αλλά καθώς εξελίσσεται η έρευνα μπορεί να αποδειχθούν αρκετά κρίσιμα.

Όπως όλες οι ψηφιακές συσκευές, έτσι λοιπόν και η χρήση ενός ΣμηΕΑ αναπόφευκτα αποφέρει αρκετά δεδομένα τα οποία αποθηκεύονται είτε στο ίδιο το ΣμηΕΑ είτε στις προαναφερθείσες συσχετιζόμενες συσκευές. Εν συντομία τα δεδομένα αυτά ενδέχεται να βρίσκονται (1) σε ενσωματωμένη στο ΣμηΕΑ συσκευή αποθήκευσης (on-board storage), (2) σε διάφορους αφαιρούμενους αποθηκευτικούς χώρους, οι οποίοι ενδεχομένως να βρίσκονται στο ίδιο το ΣμηΕΑ, είτε στον επίγειο σταθμό ελέγχου, είτε στο κινητό τηλέφωνο/tablet ή ακόμα και στο ωφέλιμο φορτίο που το ΣμηΕΑ φέρει, (3) στον ενσωματωμένο αποθηκευτικό χώρο των κινητών/tablet ή σε εφαρμογές αυτών που χρησιμοποιούνται κατά την πτήση, (4) στον εσωτερικό αποθηκευτικό χώρο ή την εφαρμογή που εκτελείται από τον επίγειο σταθμό ελέγχου,

(5) στον αποθηκευτικό χώρο νέφους, ακόμα και (6) σε πακέτα δικτύου όταν η επικοινωνία χειριστή και ΣμηΕΑ γίνεται με ασύρματα δίκτυα (π.χ. μέσω 5G). Μεγάλο μέρος των αρχείων αυτών πρόκειται για ιστορικά αρχεία καταγραφής χρήσης σχετιζόμενα με τις πτήσεις που έχουν πραγματοποιηθεί.

Επιπροσθέτως, είναι αναγκαίο για την διερεύνηση αυτή, να διευκρινιστούν και να διεκπεραιωθούν τυχόν ηθικά και νομικά ζητήματα που προκύπτουν, ούτως ώστε τα πειστήρια που προκύπτουν να γίνονται αποδεκτά από τη σκοπιά της νομιμότητας και του παραδεκτού των πληροφοριών εντός του δικαστικού συστήματος. Για να επιτευχθεί αυτό, θα πρέπει να νομοθετηθεί πλήρως ή ενημερωθεί το υπάρχων πλαίσιο που αφορά την χρήση ΣμηΕΑ για κακόβουλες ενέργειες, συμπεριλαμβάνοντας την ψηφιακή εγκληματολογία, την αλυσίδα ανάκτησης αποδεικτικών στοιχείων μέχρι την παρουσίασή τους στο δικαστήριο, καθώς επίσης και των αποδεκτών διαδικασιών έρευνας και των κατάλληλων κυρώσεων σε περιπτώσεις απόδοσης ευθύνης.

3.2 Διαδικασία Digital Drone Forensics

Σύμφωνα με τις οδηγίες που έχουν εκδοθεί από την Interpol [42], ο στόχος της διεξαγωγής ψηφιακής εγκληματολογίας σε ΣμηΕΑ και τον συσχετιζόμενο εξοπλισμό είναι ο εντοπισμός των διαδρομών πτήσης, των δεδομένων του χρήστη και των σχετικών εικόνων και βίντεο (ή αρχείων του αισθητήρα), που εμπεριέχονται στις συσκευές και θα βοηθήσουν στην κατανόηση του περιστατικού καθώς και την χρήση του.

Η φύση των υποθέσεων στις οποίες εμπλέκονται ψηφιακές συσκευές όπως τα ΣμηΕΑ δεν γνωρίζουν σύνορα και για τον λόγο αυτό τα ευρήματα που προέρχονται από ψηφιακά πειστήρια θα πρέπει να ακολουθούν ένα συγκεκριμένο τυποποιημένων διαδικασιών για να διασφαλίζεται ότι είναι αποδεκτά σε οποιοδήποτε δικαστήριο που ενδεχομένως κατατεθούν ως αποδεικτικά στοιχεία και όχι μόνο στο δικαστήριο μιας συγκεκριμένης χώρας.

Παρακάτω παρουσιάζονται τα βήματα της διαδικασίας που πρέπει να ακολουθηθεί από τον εκάστοτε ερευνητή προκειμένου να διαχειριστεί και να διατηρήσει την ακεραιότητα των δεδομένων που προκύπτουν από τα ΣμηΕΑ.

Όπως και στις υπόλοιπες υποθέσεις ψηφιακής εγκληματολογίας, που παρουσιάστηκαν στην Ενότητα 2, έτσι και για τα ΣμηΕΑ, υπάρχουν συνήθως τέσσερις φάσεις που ακολουθούνται για την ανάλυση των ψηφιακών δεδομένων: η συλλογή, η εξέταση, η ανάλυση και η αναφορά. Κα θ' όλη τη διάρκεια της διαδικασίας, η ακεραιότητά και η φύλαξη των δεδομένων πρέπει να διασφαλίζεται ανά πάσα στιγμή. Οι φάσεις εξέτασης και ανάλυσης μπορούν να επαναλαμβάνονται μέχρι η έρευνα να οδηγηθεί σε σαφή συμπεράσματα αναφορικά με την υπόθεση. Είναι προφανές, πως η πραγματοποίηση όλων των φάσεων δεν είναι απαραίτητη για όλες τις περιπτώσεις, καθώς σε ορισμένες από αυτές ενδέχεται να μπορεί να παραληφθεί η φάση της συλλογής προκειμένου να πραγματοποιηθεί αμέσως η φάση της εξέτασης. Ένα παράδειγμα τέτοιας περίπτωσης είναι όταν υπάρχουν μεγάλα σύνολα δεδομένων και, ως εκ τούτου, η διεξαγωγή συλλογής για κάθε στοιχείο αποδεικτικών στοιχείων μπορεί να μην είναι εφικτή.

Η παρούσα ενότητα αναφέρεται αποκλειστικά στην διαδικασία της συλλογής, εξέτασης και ανάλυσης ψηφιακών πειστηρίων και δεν εμπλέκεται στην ολοκληρωμένη διαδικασία Drone Forensics που προϋποθέτει μεταξύ άλλων και μελέτη για δακτυλικά αποτυπώματα κ.ο.κ. Για τον λόγο αυτόν τα Digital Drone Forensics αφορούν την απόκτηση, εξέταση, ανάλυση και αν αφορά δύο τύπων ψηφιακών συσκευών, τα ΣμηΕΑ και το χειριστήριο ή επίγειο σταθμό ελέγχου.

3.2.1 Στάδιο Συλλογής

Ομοίως με τους άλλους τομείς ψηφιακής εγκληματολογίας ,η συλλογή δεδομένων, είναι η διαδικασία εύρεσης των σημαντικών δεδομένων και πληροφοριών, καθώς προϋποθέτει επίσης την δημιουργία ενός πιστού αντιγράφου των ψηφιακών δεδομένων που θα αναλυθούν όπως αυτά εξήχθησαν από το ΣμηΕΑ, το χειριστήριο, το κινητό τηλέφωνο ή το laptop, με τη μορφή αρχείου καταγραφής ή αρχείων εικόνας (image files).

Η συλλογή θα πρέπει, και σε αυτή την περίπτωση, να γίνεται με σκοπό τη διατήρηση της ακεραιότητας των ψηφιακών δεδομένων. Πρωταρχικός στόχος, λοιπόν, είναι η δημιουργία πανομοιότυπου αντιγράφου των δεδομένων χωρίς να αλλάξει το περιεχόμενο τους. Καλή πρακτική είναι η δημιουργία δύο (2) τέτοιων αντιγράφων για την ευκολότερη διαδικασία αντιγραφής και εξέτασης και επεξεργασίας στο επόμενο στάδιο.

Η εξαγωγή των δεδομένων που εμπεριέχονται στα διάφορα εμπορικά ΣμηΕΑ απαιτεί συνήθως τη χρήση συγκεκριμένου λογισμικού, καλωδίων για την σύνδεση του εξοπλισμού με κάποιον Η/Υ για την μεταφορά δεδομένων, είτε απλά τοποθέτηση μιας κάρτας μνήμης στο Η/Υ που θα συλλέξει τα δεδομένα. Υπάρχουν αρκετές επιπρόσθετες και προηγμένες τεχνικές συλλογής δεδομένων οι οποίες και απαιτούν επιπρόσθετα εργαλεία, όπως η εξαγωγή του τσιπ σε περιπτώσεις που το ΣμηΕΑ έχει πάθει αρκετά μεγάλης έκτασης ζημιά. Είναι εμφανές ότι για την ανάγνωση και συλλογή ακατέργαστων δεδομένων από το τσιπ του ΣμηΕΑ, είναι απαραίτητη η χρήση εξειδικευμένων συσκευών και λογισμικού. Επίσης, κατά την συλλογή των δεδομένων από ΣμηΕΑ, ενδεχομένως να είναι απαραίτητη η χρήση συγκεκριμένου λογισμικού του κατασκευαστή σε περιπτώσεις που δεν είναι εφικτή η απόκτηση των δεδομένων με οποιονδήποτε άλλον τρόπο.

Τα εργαλεία εξαγωγής των δεδομένων ποικίλλουν και είναι πανομοιότυπα με αυτά που χρησιμοποιούνται σε άλλους τομείς Ψηφιακής Εγκληματολογίας, όπως για παράδειγμα το FTK Imager [43]. Τα περισσότερα εγκληματολογικά εργαλεία συλλογής δεδομένων έχουν οδηγό χρήσης που εξηγεί τη διαδικασία που πρέπει να ακολουθηθεί για μια επιτυχημένη εξαγωγή. Όμως, λόγω της φύσης των ΣμηΕΑ, τα τυπικά εγκληματολογικά εργαλεία είναι πιθανόν να μην υποστηρίζουν την εξαγωγή και ανάλυση δεδομένων. Για τον λόγο αυτό, συνήθως χρησιμοποιούνται αποκλειστικά εργαλεία των κατασκευαστών για την ελαχιστοποίηση του χρόνου απόκτησής τους. Τα δεδομένα που εξάγονται από τα ΣμηΕΑ, εξαιτίας της χρήσης αποκλειστικών εργαλείων του κατασκευαστή για την εξαγωγή δεδομένων, ενδεχομένως να εμφανίζονται σε ιδιόκτητη μορφή. Αυτές οι μορφές αρχείων πρέπει να μεταφερθούν σε εξειδικευμένα εργαλεία του κατασκευαστή ή άλλα που υπάρχουν διαθέσιμα στο Διαδίκτυο με σκοπό να αποκωδικοποιηθούν. Άλλες μη ιδιόκτητες μορφές περιλαμβάνουν αρχεία bin και ακατέργαστα αρχεία (raw).

Μια άλλη πλούσια πηγή ψηφιακών δεδομένων αποτελούν τα εφεδρικά αρχεία, η τηλεμετρία και τα διαγνωστικά αρχεία του ΣμηΕΑ. Ορισμένα ΣμηΕΑ δημιουργούν αντίγραφα ασφαλείας ή αντίγραφα σε άλλες συσκευές, όπως σε Η/Υ ή ακόμα και στο νέφος. Αυτά τα αντίγραφα ασφαλείας μπορούν να αποδειχθούν αρκετά χρήσιμα καθώς βοηθούν στην δημιουργία ενός χρονοδιαγράμματος των συμβάντων, και μπορούν επίσης να χρησιμοποιηθούν για την απόκτηση πρόσβασης σε ιστορικά δεδομένα τα οποία δεν βρίσκονται στο ΣμηΕΑ.

Αφού συλλεχθούν όλα τα σημαντικά για την έρευνα δεδομένα, ο ερευνητής πρέπει να επαληθεύσει την ακεραιότητά τους σε σχέση με τα πρωτότυπα. Πληροφορίες και δεδομένα όπως η ημερομηνία, η ώρα, οι γεωγραφικές συντεταγμένες και οι πληροφορίες του χρήστη και του συστήματος πρέπει να διασταυρώνονται από τον εξεταστή, καθώς μερικές φορές μετατρέπονται σε άλλη μορφή κατά τη διαδικασία εξαγωγής.

Το τελευταίο βήμα σε αυτό το στάδιο αφορά την καταγραφή των ενεργειών (ημερομηνία, ώρα, είδος ενέργειας, εργαλείο) από την πλευρά του ερευνητή σε κάθε βήμα που επιχειρεί για την συλλογή των δεδομένων ΣμηΕΑ έτσι ώστε να διασφαλίσει πως η διαδικασία είναι τεκμηριωμένη. Τυχόν σφάλματα ή ανωμαλίες που προκύπτουν κατά τη διαδικασία από τα εργαλεία που χρησιμοποιήθηκαν, πρέπει επίσης να καταγραφούν.

3.2.2 Στάδιο Εξέτασης

Ομοίως με τους υπόλοιπους τομείς ψηφιακής εγκληματολογίας, έτσι και στην περίπτωση των ΣμηΕΑ, η εξέταση των πρωτότυπων ψηφιακών δεδομένων θα πρέπει να αποφεύγεται, όπου αυτό καθίσταται δυνατόν. Ο ερευνητής οφείλει να εργάζεται στο αντίγραφο (αρχείο εικόνας) των ψηφιακών δεδομένων που έχει δημιουργήσει κατά το πρώτο στάδιο της εγκληματολογικής έρευνας. Υπάρχουν περιπτώσεις στις οποίες οι ερευνητές θα πρέπει να χρησιμοποιήσουν ένα απομονωμένο περιβάλλον για τη διεξαγωγή της εξέτασης. Σε τέτοιες περιπτώσεις χρησιμοποιείται η τεχνολογία της εικονικοποίησης, μέσω γνωστών λογισμικών όπως το

VirtualBox το Hyper-V κ.ο.κ. Η διαδικασία της εξέτασης στην τομέα των ΣμηΕΑ θα μπορούσε να είναι αρκετά χρονοβόρα διαδικασία έχοντας υπόψη τον όγκο των πληροφοριών που δύναται να εξαχθεί από το ίδιο το ΣμηΕΑ καθώς και τα συσχετιζόμενα συστήματα.

3.2.3 Στάδιο Ανάλυσης

Με τον ίδιο τρόπο που ένας εγκληματίας αφήνει πίσω του φυσικά ίχνη στον τόπο του εγκλήματος, έτσι και στην περίπτωση ενός ΣμηΕΑ που χρησιμοποιείται από έναν εγκληματία για να διαπράξει κάποια παράνομη πράξη θα αφήσει ψηφιακά στοιχεία σχετικά με τις τοποθεσίες και τις ενέργειές του που οδηγούν στην κατανόηση του συμβάντος και στην τελική αναφορά.

Τα δεδομένα που πρέπει να εξαχθούν και αναλυθούν από ένα ΣμηΕΑ ή συσχετιζόμενο σύστημά του εξαρτώνται σε μεγάλο βαθμό από τον τύπο της υπόθεσης. Έτσι, η ανάλυση δεν θα πρέπει να περιορίζεται αλλά μπορεί να επικεντρωθεί σε κάποιον από τους παρακάτω τύπους δεδομένων:

- Φωτογραφίες και βίντεο: στην περίπτωση αυτή ο ερευνητής θα χρειαστεί να αναλύσει όλες τις φωτογραφίες και τα βίντεο που έχει στην διάθεσή του για να καταγράψει τις ενέργειες του ΣμηΕΑ σύμφωνα με τα σημεία που η κάμερα φωτογραφίζει ή/και παρατηρεί. Με αυτόν τον τρόπο θα γίνει κατανοητός ο σκοπός της πτήσης. Σε αρκετές περιπτώσεις ενδεχομένως να χρειαστεί και η περαιτέρω ανάλυση των φωτογραφιών ή/και του βίντεο με χρήση εξειδικευμένων εργαλείων. Τέλος, τα μεταδεδομένα (metadata) θα βοηθήσουν ακόμη περισσότερο στην σύνδεση χρόνου, ενέργειας, γεωγραφικών δεδομένων και φωτογραφίας, κατά την διάρκεια όλης της πτήσης του ΣμηΕΑ.
- Αρχεία καταγραφής πτήσης: αποτελούν τα σημαντικότερα αρχεία για την έρευνα. Συνήθως περιέχουν στοιχεία όπως (1) Θέση GPS, (2) Ώρα και ημερομηνία, (3) Παραμέτρους της πτήσης (π.χ. ταχύτητα, υψόμετρο κ.ο.κ), (4) Κωδικούς σφαλμάτων κατά την πτήση, (5) Ενέργειες ή συσχετισμένα αρχεία μέσων (φωτογραφία ή βίντεο). Η ανάλυση των αρχείων καταγραφής της πτήσης μπορεί να φανεί αρκετά σημαντική αναφορικά με την αναζήτηση της πρόθεσης του χειριστή. Χαρακτηριστικό παράδειγμα θα μπορούσε να είναι η εύρεση της θέσης του ΣμηΕΑ σε απαγορευμένη ζώνη, το οποίο απεικονίζει την κακόβουλη πρόθεση του χειριστή να καταγράψει ενδεχομένως τον προστατευμένο αυτό χώρο. Συγκεκριμένα λογισμικά εγκληματολογικών ερευνών προσφέρουν ανάλυση των αρχείων καταγραφής πτήσης, με τα πιο αποδοτικά να είναι αυτά των κατασκευαστών αφού σε αρκετές περιπτώσεις τα αρχεία αυτά είναι κωδικοποιημένα. Τα λογισμικά των κατασκευαστών στις περισσότερες των περιπτώσεων δεν είναι διαθέσιμα για το ευρύ κοινό, έτσι ο ερευνητής οφείλει να μεταμορφώσει τα αρχεία αυτά σε μορφή κατανοητή και επεξεργάσιμη (π.χ. .csv) μέσω προγραμμάτων ανοιχτού λογισμικού.
- Λογισμικά: η ανάλυση του λογισμικού που χρησιμοποιήθηκε για την πτήση είναι επίσης μια από τις πηγές ψηφιακών δεδομένων. Αρχικά ο ερευνητής οφείλει να κατανοήσει πως λειτουργεί η εφαρμογή, που αποθηκεύει δεδομένα, κ.ο.κ., το οποίο θα το επιτύχει μόνον μέσω της εικονικοποίησης του λογισμικού και της διεξαγωγής διάφορων δοκιμών. Τα ευρήματα από αυτή την διαδικασία μπορούν να συνεισφέρουν στην κατανόηση της λειτουργικότητας και της συλλογής δεδομένων της εφαρμογής.
- Ενέργειες του χρήστη: οι ενέργειες του χρήστη αποθηκεύονται σε πολλά σημεία, είτε στην εσωτερική μνήμη του ΣμηΕΑ είτε σε κάποια από τις συσχετιζόμενες συσκευές (π.χ. χειριστήριο). Οι ενέργειες του χρήστη μπορεί να περιλαμβάνουν τον χρόνο εκκίνησης και απενεργοποίησης του ΣμηΕΑ, τις ρυθμίσεις του, συνδεδεμένοι λογαριασμοί χρήστη, Wi-Fi ή LTE συνδέσεις, κ.ο.κ. Τα συγκεκριμένα δεδομένα, εφόσον αναλυθούν μπορούν να προσφέρουν στον ερευνητή μια καλύτερη κατανόηση της συμπεριφοράς του χειριστή του ΣμηΕΑ.

3.2.4 Στάδιο Αναφοράς

Το στάδιο της αναφοράς απαιτείται σε όλους τους τομείς ψηφιακής εγκληματολογίας και στοχεύει στην συγκέντρωση όλων των ευρημάτων με τρόπο κατανοητό για τα ενδιαφερόμενα μέρη. Αμέσως μετά την ολοκλήρωση της ανάλυσης των δεδομένων, ο ερευνητής καλείται να καταγράψει γραπτώς τα ευρήματά του σε τυποποιημένες φόρμες ούτως ώστε να μπορούν να χρησιμοποιηθούν στο δικαστήριο εφόσον αυτό χρειαστεί. Είναι επίσης ευθύνη του ερευνητή να εξηγήσει και να απεικονίσει με κατανοητό τρόπο τις τεχνικές μεθόδους που χρησιμοποίησε για να εξάγει το αποτέλεσμα της μελέτης. Σε ορισμένες περιπτώσεις, όπου υπάρχει μεγάλος αριθμός πειστηρίων, χρησιμοποιούνται επίσης συγκεκριμένα λογισμικά που αντιστοιχίζουν τα πειστήρια με τα δεδομένα που εξήχθησαν από την έρευνα προς διευκόλυνση του εκάστοτε ερευνητή.

3.3 Διαθέσιμα Δεδομένα

Όπως προσδιορίζεται στην Ενότητα 3.2, υπάρχουν αρκετοί διαφορετικοί τύποι δεδομένων που επρόκειτο να προκύψουν από την συλλογή ψηφιακών στοιχείων, τα οποία αποθηκεύονται σε διαφορετικά μέσα, συμπεριλαμβανομένου του ίδιου του ΣμηΕΑ, των αφαιρούμενων μέσων αποθήκευσης, των φορητών συσκευών, κ.ο.κ. Έχει παρατηρηθεί ότι μερικές φορές υπάρχουν διαθέσιμα δεδομένα και στο χειριστήριο του ΣμηΕΑ. Εάν είναι απαραίτητο, ο ερευνητής θα πρέπει να προσπαθήσει να ανακτήσει δεδομένα και από αυτή την πηγή. Αυτά τα δεδομένα θα μπορούσαν να περιλαμβάνουν: τηλεμετρικά δεδομένα, δηλαδή στίγμα γεωγραφικών συντεταγμένων, ταχύτητα, υψόμετρο, κ.ο.κ., συνδεδεμένες συσκευές, όπως για παράδειγμα το χειριστήριο συμπεριλαμβανομένου του S/N της συσκευής, συνδεδεμένους λογαριασμούς χρήστη, όπως για παράδειγμα email του χρήστη το οποίο χρησιμοποιήθηκε για την δημιουργία λογαριασμού στον κατασκευαστή του ΣμηΕΑ.

Στην περίπτωση εξαγωγής και ανάλυσης δεδομένων από ΣμηΕΑ, υπάρχουν τέσσερα διαφορετικά επίπεδα, τα οποία περιγράφονται παρακάτω ξεκινώντας από το επίπεδο όπου μπορούν να εξαχθούν τα περισσότερα δεδομένα και κυμαίνονται μέχρι το επίπεδο όπου μπορούν να εξαχθούν τα λιγότερα δεδομένα.

1. **Φυσική Εξαγωγή** που αφορά την απόκτηση ακατέργαστων (raw) δυαδικών δεδομένων από την συσκευή. Αυτά τα ακατέργαστα δεδομένα πρέπει στη συνέχεια να αναλυθούν και να υποβληθούν σε επεξεργασία σε μεταγενέστερο στάδιο από εγκληματολογικό λογισμικό.
2. **Αποτύπωση συστήματος αρχείων** (File System Dump - FSD), με το οποίο είναι εφικτό να ανακτηθεί το σύστημα αρχείων της συσκευής και να ερμηνευθούν τα συλλεχθέντα δεδομένα κατά το στάδιο της ανάλυσης. Αυτό επιτρέπει στον ερευνητή να ανακτήσει, για παράδειγμα, βάσεις δεδομένων που περιέχουν διαγραμμένα δεδομένα τηλεματικής/
3. **Λογική Εξαγωγή**, η οποία περιλαμβάνει τη λήψη πληροφοριών από το ΣμηΕΑ. Αυτή η μέθοδος καθιστά διαθέσιμα μόνο ζωντανά δεδομένα στον εξεταστή. Τα περισσότερα λογισμικά εγκληματολογικών ερευνών, προσφέρουν αυτόν την δυνατότητα λογικής εξαγωγής εάν τα δεδομένα δεν περιέχονται σε αφαιρούμενο αποθηκευτικό μέσο. Το πρόβλημα με τις λογικές εξαγωγές είναι ότι δεν υπάρχει τρόπος επαλήθευσης των δεδομένων στο ίδιο το ΣμηΕΑ.
4. **Chip-Off**, η οποία αφορά ΣμηΕΑ που διαθέτουν ενσωματωμένη μνήμη ή είναι κατεστραμμένα. Η μέθοδος Chip-Off επιτρέπει επίσης την εξαγωγή ακατέργαστων (raw) δεδομένων από την συσκευή, όμως απαιτεί τη μόνιμη αφαίρεση του τσιπ μνήμης της συσκευής από την πλακέτα.

Συγκεντρωτικά, τα ψηφιακά συστήματα που αποθηκεύονται δεδομένα φωτογραφιών και βίντεο είναι η εσωτερική μνήμη καθώς και οι αφαιρούμενοι αποθηκευτικοί χώροι των ΣμηΕΑ και του χειριστηρίου του.

Τα ψηφιακά συστήματα που εμπεριέχουν αρχεία καταγραφής πτήσεις είναι η εσωτερική μνήμη καθώς και οι αφαιρούμενοι αποθηκευτικοί χώροι των ΣμηΕΑ, του χειριστηρίου του, καθώς και

των εφαρμογών που βρίσκονται στα κινητά τηλέφωνα/tablet. Η μορφή των εξαγόμενων αρχείων καταγραφής ποικίλει αναλόγως τον κατασκευαστή, το μοντέλο και την εφαρμογή που χρησιμοποιήθηκε για την πτήση. Τις περισσότερες περιπτώσεις συναντώνται αρχεία τις μορφής .bin (π.χ. από Ardupilot), .dat, .txt (π.χ. DJI). Ενδεικτικά παρουσιάζονται στον παρακάτω πίνακα οι κοινές τοποθεσίες των αρχείων καταγραφής πτήσης κάποιων από τα πιο κοινά ΣμηΕΑ στην αγορά.

Πίνακας 1: Θέσεις και τύπος αρχείων καταγραφής πτήσης για κοινά ΣμηΕΑ της αγοράς

Μοντέλο και μάρκα ΣμηΕΑ	Τοποθεσία δεδομένων	Τύπος αρχείου	Τυποποιημένο όνομα αρχείου	Κωδικοποίηση δεδομένων
DJI Phantom 4 Pro	Εσωτερική κάρτα μνήμης	.dat	FLYXXX, DJI_ASSISTANT_xxxxxx.DAT	Ναι
DJI Mavic 2	Εσωτερική κάρτα μνήμης	.dat	FLYXXX, DJI_ASSISTANT_xxxxxx.DAT	Ναι
Parrot ANAFI	Εξωτερική κάρτα μνήμης	.bin	Log.bin	Όχι
YNEEX Q500 4K	Εξωτερική κάρτα μνήμης	.csv	Telemetry	Όχι

3.4 Περιπτώσεις Μελέτης

Η χρησιμότητα της ανάλυσης των αρχείων καταγραφής πτήσης, δεν φαίνεται μόνο στη ψηφιακή εγκληματολογία που καλούνται να διεκπεραιώσουν οι φορείς επιβολής του νόμου αλλά και σε άλλους αλληλένδετους τομείς όπου χρειάζεται να αναλυθούν τα δεδομένα μιας πτήσης. Χαρακτηριστικό παράδειγμα αποτελεί ο πραγματογνώμων, ο οποίος αναλαμβάνει παρόμοιες υποθέσεις για να εναποθέσει το δικό του συμπέρασμα αναφορικά με μια υπόθεση. Η χρησιμότητα της ανάλυσης των αρχείων καταγραφής πτήσης από οποιοδήποτε ΣμηΕΑ φαίνεται ακόμα και σε προγραμματιστές ή απλούς χρήστες που έχουν σαν χόμπι την χρήση ΣμηΕΑ και οποίοι στοχεύουν στην ανεύρεση δυσλειτουργιών που εμφανίστηκαν κατά την διάρκεια κάποιας πτήσης τους. Είναι λοιπόν δεδομένο πως με την γρήγορη συλλογή και ανάλυση των δεδομένων, υπάρχει μια καλύτερη κατανόηση της κατάστασης που βρέθηκε το ΣμηΕΑ ή/και ο χειριστής. Με τον ίδιο τρόπο και αναγνωρίζοντας πιθανά σφάλματα του ΣμηΕΑ κατά την πτήση, όπως για παράδειγμα αυξομειώσεις των τιμών της τάσης ή θερμοκρασίας είναι εύκολο να αποφανθεί κάποιος, αν κάποιο ατύχημα ήταν απόρροια της λανθασμένης χρήσης του χειριστή ή σφάλματος που προήλθε από το ίδιο το ΣμηΕΑ. Έτσι, ο καθένας θα μπορούσε να πιστοποιήσει τα αποτελέσματα της ψηφιακής εγκληματολογίας που σε τέτοιες περιπτώσεις γίνεται μέσω των εξειδικευμένων εργαλείων των κατασκευαστών.

Κάποια από τα εμπορικά ΣμηΕΑ ή ακόμα και ιδιοκατασκευές, παράγουν αρχεία καταγραφής πτήσης σε εύκολα επεξεργάσιμη μορφή όπως για παράδειγμα το Parrot ANAFI που αναφέρθηκε στην προηγούμενη ενότητα ή όποια ιδιοκατασκευή χρησιμοποιεί Ardupilot για τον προγραμματισμό της πτήσης του. Παρόλα αυτά, μεγάλο μέρος της αγοράς των εμπορικών ΣμηΕΑ (πάνω από το 70% της αγοράς [44]) προέρχονται από την κατασκευαστική εταιρία DJI, η οποία προσφέρει τα δεδομένα πτήσης σε «κωδικοποιημένη» μορφή, με την δυνατότητα πλήρους ανάλυσής τους μόνο από τα δικά τους Forensics Tools. Με αφορμή την ανάγκη για γρήγορη και κατανοητή ανάλυση των αρχείων καταγραφής πτήσης όλων των ΣμηΕΑ από έναν μόνο αλγόριθμο, η παρούσα διατριβή βασίζεται πάνω στο GRYPHON [45], επεκτείνοντας τις δυνατότητές του για να μπορεί να αναλύσει αρχεία καταγραφής πτήσης που προέρχονται από ΣμηΕΑ της DJI. Στις επόμενες ενότητες παρουσιάζονται αναλυτικά η μεθοδολογία που ακολουθήθηκε καθώς και τα αποτελέσματα και συμπεράσματα.

4. Μεθοδολογία και Υλοποίηση

4.1 Μεθοδολογία

Στην παρούσα ενότητα παρουσιάζονται η μεθοδολογία ψηφιακή εγκληματολογίας που ακολουθήθηκε, καθώς επίσης και το use case που λάβαμε υπόψη για την εκπόνηση της μελέτης, και οι παραδοχές που έγιναν στο πλαίσιο της μεθοδολογίας.

Η μελέτη, λοιπόν, βασίζεται στην κοινή μεθοδολογία που χρησιμοποιείται σε περιπτώσεις digital forensics, υιοθετεί τα τέσσερα βασικά βήματα της συλλογής, εξέτασης, ανάλυσης και αναφοράς, και τα προσαρμόζει περαιτέρω μέσω της ακόλουθης σταδιακής διαδικασίας (Εικόνα 15): (1) Προετοιμασία για ψηφιακή εγκληματολογία, (2) Συλλογή και Εξέταση δεδομένων, (3) Ανάλυση δεδομένων και (4) Αναφορά.

Προετοιμασία για ψηφιακή εγκληματολογία

Στο παρών στάδιο, πραγματοποιούνται μια σειρά από ενέργειες προετοιμασίας και ελέγχου για την βαθύτερη κατανόηση του συμβάντος. Πριν ξεκινήσει μια έρευνα ψηφιακής εγκληματολογίας και αφού παραληφθεί το έκθεμα, είναι απαραίτητο να αναζητήσουμε σχετικό υλικό όπως π.χ. αναφορά, φωτογραφίες, κτλ. από την κατάσχεση του ΣμηΕΑ που θα βοηθήσουν στον οριοθέτηση των στόχων που θα έχει η μελέτη. Πριν από μια ψηφιακή εγκληματολογία, είναι πάντα απαραίτητη η υλοποίηση παραδοσιακών μεθόδων εγκληματολογίας για την ανεύρεση δακτυλικών αποτυπωμάτων, εύρεση DNA στην συσκευή, κ.ο.κ. τα οποία θα υποστηρίξουν την συνολική έκβαση της αναφοράς συμβάντος και σύνδεσης των γεγονότων. Στο στάδιο της προετοιμασίας, ο εκάστοτε ερευνητής θα πρέπει να κατανοήσει πλήρως τον ρόλο του ΣμηΕΑ στο συμβάν (π.χ. εμπλοκή σε ατύχημα με υλικές ζημιές, π.χ. μεταφορά εκρηκτικών υλών προς μια κρίσιμη υποδομή κ.ο.κ.), καθώς επίσης και να φωτογραφίσει το έκθεμα πριν από την όποια ενέργεια. Κλείνοντας, το παρών βήμα ο ερευνητής εξετάζει τη φυσική συσκευή (ΣμηΕΑ) για την καταγραφή εμφανών γενικών πληροφοριών, όπως για παράδειγμα μάρκα, μοντέλο, μοναδικός αριθμός ταυτοποίησης (S/N) αλλά και των ενδεχόμενων σημείων ενδιαφέροντος αναφορικά με την ψηφιακή εγκληματολογία, όπως εγκοπές που υποδεικνύουν χώρους αποθήκευσης δεδομένων (SD cards). Η διαδικασία αυτή γίνεται για να μη παραληφθούν δεδομένα κατά την έρευνα, όπως επίσης και για την σύγκριση της αρχικής αναφοράς της κατάσχεσης με τα αποτελέσματα μετά την ανάλυση.

Συλλογή και Εξέταση δεδομένων

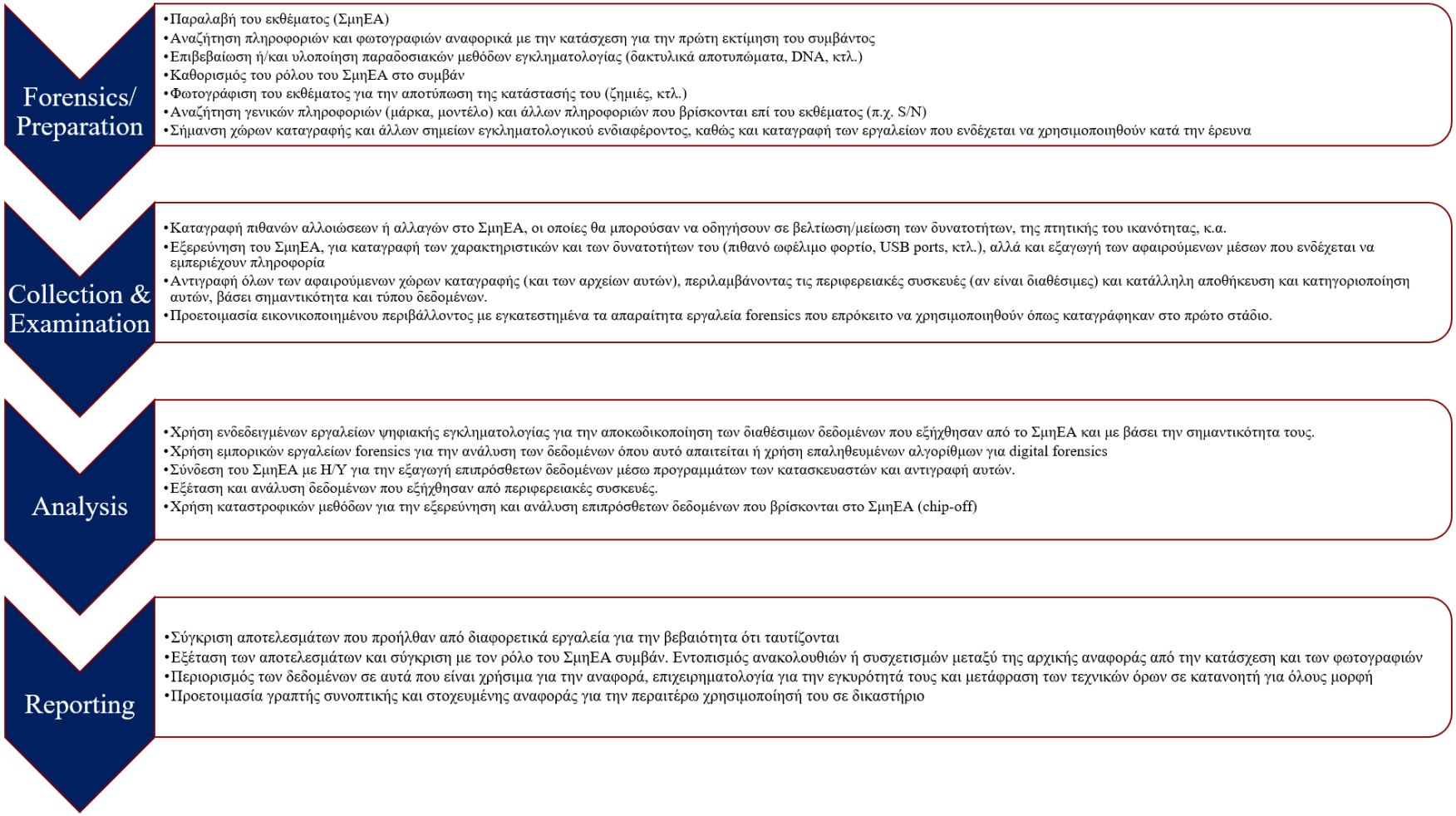
Το στάδιο αυτό ξεκινάει με την καταγραφή και καταχώρηση πιθανών αλλοιώσεων που έχει υποστεί το ΣμηΕΑ, οι οποίες ενδεχομένως να επηρεάζουν και τα δεδομένα που έχουν καταγραφεί. Οι αλλαγές που έχουν γίνει πάνω στο ΣμηΕΑ και το διαφοροποιούν από την αρχική του εκδοχή, ενδεχομένως να επιφέρουν βελτιώσεις ή μειώσεις των δυνατοτήτων του αλλά και της πτητικής του ικανότητας, εφόσον αυτές οι αλλαγές δεν έχουν εγκριθεί από τον φορέα πιστοποίησης (Υ.Π.Α.). Η καταγραφή των αλλαγών, εφόσον αυτές υπάρχουν, λειτουργούν ως ένδειξη για τον ρόλο του ΣμηΕΑ στο συμβάν και συμπληρώνουν την ψηφιακή εγκληματολογία. Στην συνέχεια, ο ερευνητής οφείλει να καταγράψει όλα τα εμφανή χαρακτηριστικά από τα περιφερειακά μέρη του ΣμηΕΑ, όπως για παράδειγμα το ωφέλιμο φορτίο και το χειριστήριο, καθώς επίσης να εξάγει όλες τις αφαιρούμενες μονάδες αποθηκευτικού χώρου. Πριν την ανάλυση των δεδομένων, ο ερευνητής οφείλει να δημιουργήσει τα κατάλληλα αντίγραφα όλων των δεδομένων που έχουν συλλεχθεί και να τα κατηγοριοποιήσει βάσει της εμπειρίας του με βάση την σημαντικότητά τους. Το βήμα αυτό είναι αρκετά σημαντικό για την εξοικονόμηση χρόνου, καθώς επίσης και για την «χαρτογράφηση» των δεδομένων και την καλύτερη ανάλυσή τους. Τέλος, βάσει της εμπειρίας του, καθώς και των διαθέσιμων εργαλείων forensics, ο ερευνητής θα πρέπει να καταγράψει τα εργαλεία που θα χρησιμοποιήσει κατά την έρευνα για να αποκωδικοποιήσει και αναλύσει τα δεδομένα ενδιαφέροντος, όπως επίσης θα πρέπει να ετοιμάσει το εικονικοποιημένο περιβάλλον για την διεξαγωγή της όλης έρευνας.

Ανάλυση δεδομένων

Το παρών στάδιο περιλαμβάνει την επιλογή των καταλληλότερων για την έρευνα εργαλείων forensics, επιλέγοντας από την υπάρχουσα λίστα και σύμφωνα με τα δεδομένα που πρέπει να αναλυθούν. Τα εργαλεία αυτά χρησιμοποιούνται αρχικά για την αποκωδικοποίηση και αρχική ανάλυση (decoding & parsing) των κωδικοποιημένων δεδομένων και στην συνέχεια για την ανάλυσή τους και εξαγωγή συμπερασμάτων, αναλυτικών γραφημάτων, αναπαραστάσεων του συμβάντος, κ.ο.κ. Η χρήση αξιόπιστων εργαλείων είτε open source είτε εμπορικών ενδείκνυται για την κατοχύρωση της ακεραιότητας των παραγόμενων αποτελεσμάτων. Η ανάλυση των διαθέσιμων δεδομένων λαμβάνει χώρα ξεκινώντας βάσει σημαντικότητας των δεδομένων και μέχρι το σημείο εύρεσης ικανοποιητικών πειστηρίων για την ερεύνα. Στην συνέχεια και εφόσον δεν υπάρχουν χρήσιμα εξαγόμενα, η έρευνα μπορεί να συνεχιστεί με την εξαγωγή και ανάλυση επιπρόσθετων δεδομένων που μπορούν να αντληθούν: (α) τις περιφερειακές συσκευές (χειριστήριο, tablet, κινητό, κ.ο.κ.), στις οποίες εφαρμόζονται παραδοσιακές μέθοδοι ψηφιακής εγκληματολογίας, (β) μέσω της διασύνδεσης του ΣμηΕΑ με Η/Υ και την χρήση ειδικών προγραμμάτων των κατασκευαστών που δίνουν την δυνατότητα εξαγωγής λεπτομερών δεδομένων, στην περιπτώσεις όπου αυτό καθίσταται εφικτό, (γ) μέσω της χρήσης καταστροφικών μεθόδων για την εξαγωγή «κρυμμένων» δεδομένων, όπως για παράδειγμα μέσω της μεθόδου chip-off. Η ανάλυση περιλαμβάνει ακόμα και την απτή αναπαράσταση του συμβάντος μέσω των συντεταγμένων GPS, και η εξαγωγή σχετικών γεγονότων (events) σε χρονική σειρά και γραφημάτων με δεδομένα σημασίας.

Αναφορά

Στο τελευταίο στάδιο της έρευνας, ο εκάστοτε ερευνητής οφείλει να συγκρίνει τα αποτελέσματα που εξήχθησαν από διαφορετικά εργαλεία για να πιστοποιήσει την εγκυρότητά τους, εφόσον χρησιμοποιήθηκαν διαφορετικά εργαλεία κατά την ανάλυση. Τυχόν διαφορές σε αποτελέσματα, οδηγούν στην επανάληψη του προηγούμενου σταδίου. Εν συνεχεία, εξετάζονται προσεκτικά τα αποτελέσματα και συνδέονται και συγκρίνονται με τον ρόλο του ΣμηΕΑ στο συμβάν, όπως αυτό είχε κατοχυρωθεί κατά το πρώτο στάδιο. Στο βήμα αυτό είναι απαραίτητη η εξαγωγή συσχετίσεων με τα γεγονότα του συμβάντος με χρονική σειρά, καθώς επίσης η ενοποίηση των γεγονότων, των γραφημάτων και αναπαραστάσεων που εξήχθησαν στο προηγούμενο στάδιο. Τέλος, για την συγγραφή της αναφοράς, ο ερευνητής πρέπει (α) να εστιάσει και συμπεριλάβει μόνο τα δεδομένα που είναι χρήσιμα για την έρευνα και όχι όλα τα ευρήματά του, (β) να επιχειρηματολογήσει με αποδείξεις για την εγκυρότητα των αποτελεσμάτων που παρουσιάζει ώστε να μην δέχονται αμφισβήτησης, και τέλος (γ) να μεταφέρει κατάλληλα και να αποφύγει αναφορές σε τεχνικούς όρους με σκοπό η αναφορά του να είναι κατανοητή από ανθρώπους με διαφορετική ειδίκευση. Η γραπτή, αυτή αναφορά θα πρέπει να τηρεί όλα τα παραπάνω και είναι όσο πιο περιεκτική και στοχευμένη γίνεται, χωρίς να εμπεριέχει περιττές λεπτομέρειες.



Εικόνα 15: Μεθοδολογία Drone Digital Forensics

4.1.1 Use case

Σε αυτήν την ενότητα, παρουσιάζεται μια ενδεικτική περίπτωση μελέτης που περιλαμβάνει τον σκοπό και στόχους την παρούσας μελέτης και την σύνδεση αυτής με την μεθοδολογία. Η παρούσα περίπτωση μελέτης αφορά ένα ΣμηΕΑ DJI Phantom 4 Pro., το οποίο υποθέτουμε πως έχει εμπλακεί σε ατύχημα, κατά το οποίο προκλήθηκαν υλικές ζημιές σε διερχόμενο από τον δρόμο όχημα. Η μελέτη ανατίθεται σε πραγματογνώμονα για να διαπιστώσει κατά πόσον έγινε κάποιος λάθος χειρισμός του χειριστή ή το ατύχημα προκλήθηκε από βλάβη του ΣμηΕΑ.

Με βάση την διαδικτυακή έρευνα, προσδιορίζονται τα σημεία δεδομένων ενδιαφέροντος που προκύπτουν από το ΣμηΕΑ DJI Phantom 4 Pro [46], το οποίο και διαθέτει αφαιρούμενη κάρτα μνήμης στην κάμερα και θύρα USB για περαιτέρω σύνδεση με Η/Υ και εξαγωγή δεδομένων, ενώ δεν εμπεριέχει εσωτερική κάρτα μνήμης. Η κάρτα μνήμης της κάμερας αποθηκεύει συνήθως πολυμέσα (εικόνες και βίντεο), ενώ μέσω του DJI Assistant της κατασκευάστριας εταιρίας είναι δυνατή η εξαγωγή των αποθηκευμένων αρχείων καταγραφής πτήσης.

Συνοπτικά τα χαρακτηριστικά του ΣμηΕΑ, πριν περιέλθει σε ψηφιακή ανάλυση αποτυπώνονται παρακάτω:

ΣμηΕΑ

- Μοντέλο: GL300E
- Θερμοκρασία λειτουργίας: 0-40 oC (από DJI manual)
- Μέγιστη διάρκεια πτήσης: περίπου 30 λεπτά (από DJI manual)
- Δορυφορικά συστήματα θέσης: GPS/GLONASS (από DJI manual)

Μπαταρίες

- Μοντέλο: Intelligent Flight Battery* (PH4-5870mAh-15.2V)
- Τύπος: LiPO 4S
- Χωρητικότητα: 5870 mAh
- Τάση: 15,2 V
- Θερμοκρασία λειτουργίας: 5-40 oC (από DJI manual)

Ωφέλιμο φορτίο

- Κάμερα ημέρας

4.1.2 Παραδοχές

Η παρούσα μελέτη λαμβάνει υπόψη κάποιες παραδοχές που εισήχθησαν στην μεθοδολογία για την ορθολογική εκπόνησή της στα πλαίσια του εφικτού και οι οποίες κατοχυρώθηκαν πριν την υλοποίηση και την εκπόνηση των αποτελεσμάτων της μελέτης. Οι παραδοχές αυτές έχουν καταγραφεί και παρουσιάζονται παρακάτω.

(1) Η διατριβή, λαμβάνοντας υπόψη τα αποτελέσματα προηγούμενης έρευνας που αφορά ανάλυση αρχείου καταγραφής από ΣμηΕΑ συμβατά με το Ardupilot, εστιάζει στην ανάλυση του ίδιου τύπου αρχείων από ΣμηΕΑ προερχόμενα από την κατασκευάστρια εταιρεία DJI, η οποία καταλαμβάνει την πλειοψηφία της παγκόσμιας αγοράς σε πωλήσεις εμπορικών ΣμηΕΑ.

(2) Λόγω της ιδιαιτερότητας των δεδομένων και αφού ανατρέξαμε σε δεδομένα ανοιχτής πρόσβασης (open-access) που έχουν δημιουργηθεί ακριβώς για αυτόν τον σκοπό - έρευνα και μελέτη-, όπως παρουσιάστηκε στην ενότητα 4.1.1, η μεθοδολογία αφορά αποκλειστικά την ψηφιακή εγκληματολογία, υποθέτοντας ότι οι τυπικές διαδικασίες που ακολουθούνται σε τέτοιες περιπτώσεις έχουν διασφαλιστεί και ταυτόχρονα με αυτές και η ακεραιότητα των δεδομένων.

(3) Λόγω της πολυπλοκότητας των δεδομένων και συγχρόνως την ιδιαιτερότητα που παρουσιάζουν, όπου σε αρκετές περιπτώσεις ενδέχεται να υπάρχουν προσωπικά δεδομένα ή/και κάποια αναγνωριστικά, όπως π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου, αναγνωριστικά δικτύου SSID, κ.ο.κ., η παρούσα έρευνα περιορίστηκε στην μελέτη και ανάλυση αρχείων καταγραφής πτήσης (flight data logs) και τα όποια προσωπικά στοιχεία αφαιρέθηκαν από τη μελέτη.

(4) Λαμβάνοντας υπόψη ότι τα αρχεία καταγραφής της DJI είναι κρυπτογραφημένα, καθώς επίσης και τα υπάρχοντα εργαλεία drone forensics «ανοιχτού κώδικα» και κατόπιν μελέτης των δυνατοτήτων αυτών, η παρούσα μελέτη εκμεταλλεύεται τον αναλυτή (parser) DatCon, ο οποίος έχει την δυνατότητα μετατροπής των παραγόμενων DJI αρχείων πτήσης .dat σε αρχεία .csv τα οποία εξετάζονται και αναλύονται περαιτέρω. Λόγω των περιορισμένων δυνατοτήτων των υπολοίπων εργαλείων για την ανάλυση (parsing) των αρχείων καταγραφής πτήσης από DJI ΣμηΕΑ, δεν χρησιμοποιήθηκε κάποιο άλλο εργαλείο.

(5) Κατά την ανάλυση (parsing) των αρχείων καταγραφής πτήσης, υποθέτουμε πως η όλη διαδικασία είναι επιτυχής και τα δεδομένα μεταφέρονται σε αρχείο τύπου .csv ακέραια.

(6) Τα γραφήματα συναρτήσει του χρόνου που παρουσιάζονται στην παρούσα μελέτη αφορούν τον έλεγχο ανωμαλιών που ενδεχομένως παρουσιάζονται στις μπαταρίες (voltage, temperature) κατά την διάρκεια της πτήσης, υποθέτοντας ότι είναι μια παράμετρος που θα εξεταστεί σε περιπτώσεις ατυχημάτων. Οποιαδήποτε άλλη στήλη ενδιαφέροντος, δύναται να παρουσιαστεί σε γράφημα, ακολουθώντας την ίδια προσέγγιση.

(7) Η υλοποίηση του αλγορίθμου έγινε σε εικονικοποιημένο περιβάλλον, με λειτουργικό σύστημα Linux – Ubuntu 20.4 και τις συσχετιζόμενες εξαρτήσεις/πακέτα να είναι τα εξής: python3, anaconda3, libgtk3, libgeos 3.8, libgeos -dev. Εκτός αυτού, απαραίτητη είναι η εγκατάσταση του DatCon 4.0.4 καθώς επίσης και η ύπαρξη του Gryphon στο εικονικοποιημένο περιβάλλον.

(8) Η υλοποίηση του αλγορίθμου έγινε σε γλώσσα Python με τις απαιτήσεις σε βιβλιοθήκες και πακέτα που καταγράφονται παρακάτω: MAVproxy, opencv-python, GitPython, termcolor, pymavlink ≥ 2.2.8, pyserial ≥ 3.0, attrdict, wxPython, matplotlib, basemap

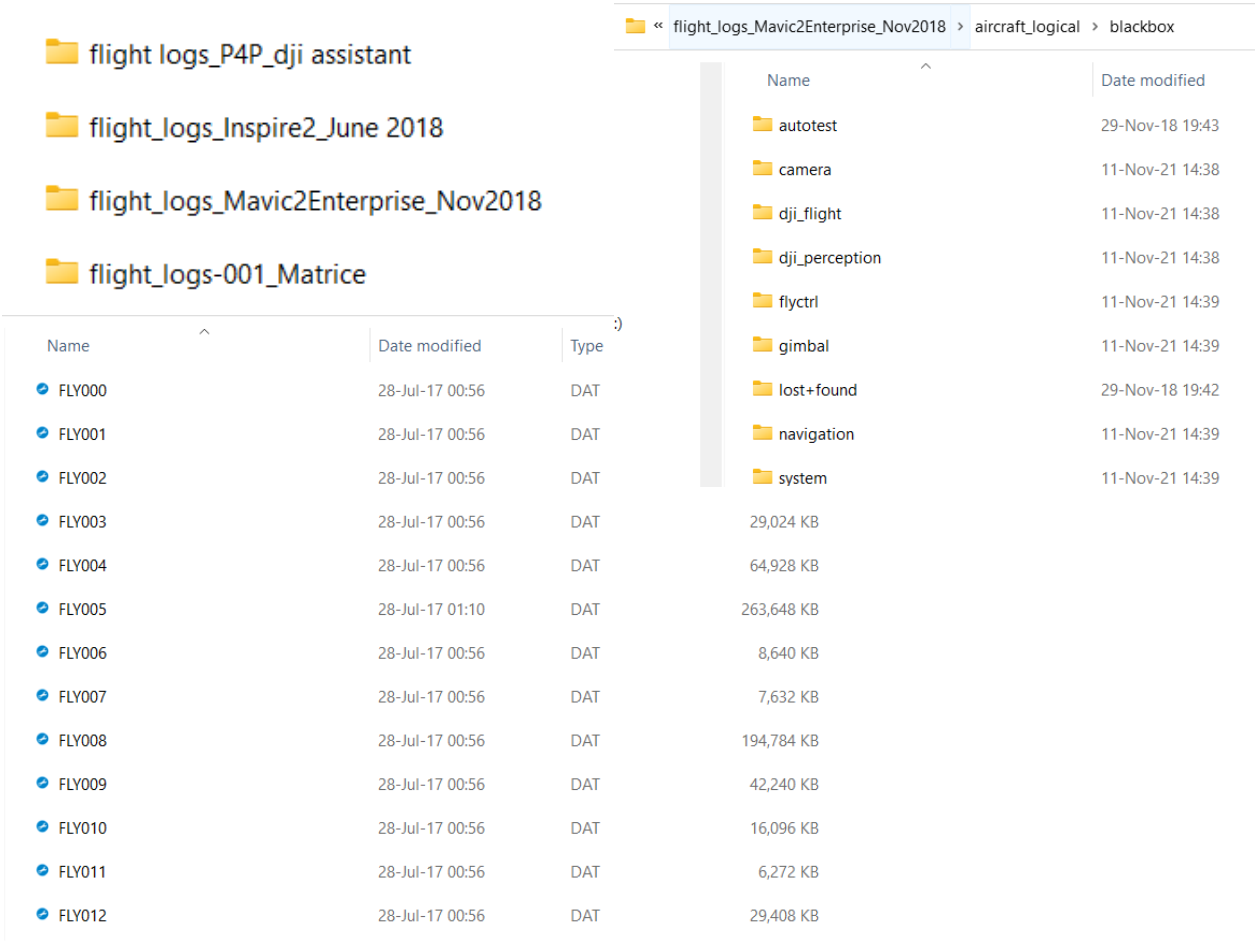
4.2 Υλοποίηση

Η εγκληματολογική μεθοδολογία που υλοποιήθηκε με βάση την περίπτωση μελέτης, δύναται να χρησιμοποιηθεί για να καθοδηγήσει την εγκληματολογική έρευνα και άλλων ΣμηΕΑ και συγκεκριμένα αυτών που είναι συμβατά με το Ardupilot, και των ΣμηΕΑ DJI και μοντέλα Inspire 1, Inspire 2, Mavic 2 Pro, Mavic 2 Enterprise, DJI Phantom 3, DJI Phantom 4, Matrice M200, Matrice M210.

Καθώς δεν χρησιμοποιήθηκε φυσική συσκευή για την πραγματοποίηση της συλλογής και ανάλυσης των δεδομένων, παραλείπονται οι απαιτήσεις του **πρώτου σταδίου** (Προετοιμασία), καθώς, δεν υπήρχαν καταγεγραμμένες πληροφορίες σχετικά με λεπτομέρειες κατάσχεσης ή άλλη μη ψηφιακή εγκληματολογική έρευνα (π.χ. DNA, δακτυλικά αποτυπώματα). Επίσης, δεν μας απασχόλησε η συλλογή αντικειμένων, η σύγκριση με τις αναφορές κατάσχεσης, κτλ. για να υποστηρίξουμε τα αποδεικτικά στοιχεία σε αυτήν την μελέτη. Ως εκ τούτου, προήλθε και η παράλειψη σχετικών βημάτων. Επιπροσθέτως και λόγω της ιδιαιτερότητας των δεδομένων, χρησιμοποιήθηκαν datasets από το Drone Forensics Program το οποίο παρέχει δωρεάν datasets για την υποστήριξη και βοήθεια των αρχών επιβολής του νόμου και κρατικών φορέων σχετικά με τις διαδικασίες ψηφιακής εγκληματολογίας σε ΣμηΕΑ. Το πρόγραμμα αυτό υλοποιήθηκε από την VTO Inc. of Broomfield [47], που εδρεύει στο Κολοράντο των Η.Π.Α.

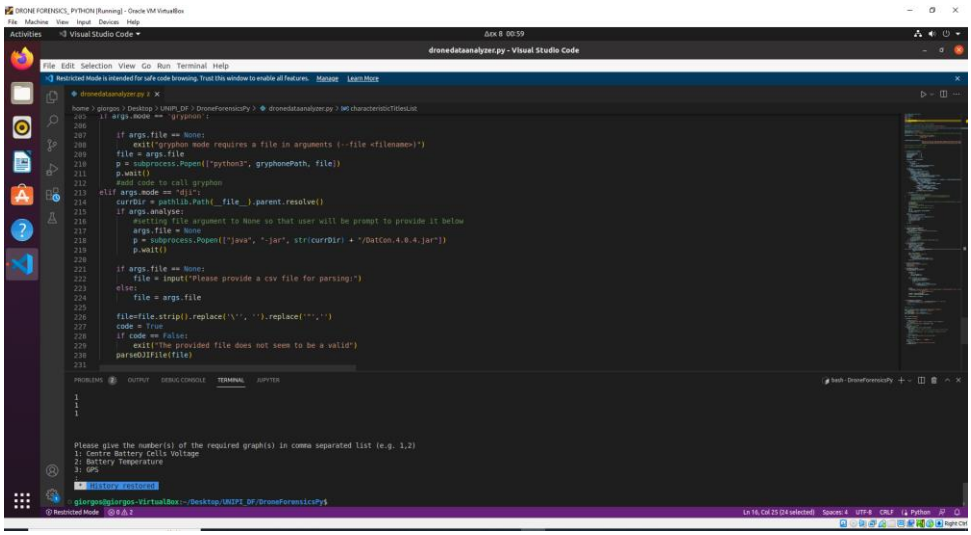
Κατά το **δεύτερο στάδιο** της μεθοδολογίας (συλλογή και εξέταση), δεν διαπιστώθηκαν αλλοιώσεις ή αλλαγές, συγκριτικά με το εμπορικό ΣμηΕΑ. Επιπροσθέτως, μετά από διαδικτυακή έρευνα διαπιστώθηκαν (βλ. 4.1.1.) τα χαρακτηριστικά του ΣμηΕΑ τα οποία θα μπορούσαν να αποδειχθούν χρήσιμα στην εξέλιξη της έρευνας. Στην συνέχεια έγινε η πολλαπλή καταγραφή

των datasets καθώς επίσης η κατάλληλη αποθήκευση σε φακέλους και υποφακέλους, αλλά και η κατηγοριοποίησή τους, όπως φαίνεται στις παρακάτω εικόνες:



Εικόνα 16:Αποθήκευση και κατηγοριοποίηση των δεδομένων σε φακέλους

Στην συνέχεια, έγινε η προετοιμασία του κατάλληλου εικονικοποιημένου περιβάλλοντος (Linux Ubuntu 20.4), με την εγκατάσταση των εργαλείων που θα χρησιμοποιηθούν πέραν του παρόντος αλγορίθμου.



Εικόνα 17: Εικονικοποιημένο περιβάλλον Linux Ubuntu 20.4, με εγκατεστημένα εργαλεία Digital Forensics

Μετά από διαδικτυακή έρευνα διαπιστώθηκε πως τα εργαλεία ψηφιακής εγκληματολογίας που έχουν την δυνατότητα να αναλύσουν αρχεία καταγραφής από ΣμηΕΑ δεν είναι πολλά και ούτε αρκετά διαδεδομένα. Υπάρχουν διάφορα εμπορικά εργαλεία και άλλα ανοιχτού κώδικα τα οποία εστιάζουν στην ανάλυση δεδομένων που προέρχονται από ΣμηΕΑ, καθώς πλέον η ανάγκη για τέτοιες αναλύσεις είναι επιτακτική. Δυστυχώς όμως, λόγω των συνεχόμενων ενημερώσεων των λογισμικών των διάφορων ΣμηΕΑ, την εμφάνιση νέων μοντέλων σε πολύ μικρό χρονικό διάστημα, όπως επίσης και λόγω της έλλειψης τυποποίησης ως προς την δημιουργία τέτοιων αρχείων, η ικανότητα και χρησιμότητα αυτών των εργαλείων ενδέχεται να αλλάζει από μήνα σε μήνα. Τα συγκεκριμένα εργαλεία αναφέρουν την λίστα συμβατότητας με τα μοντέλα που υποστηρίζουν για ανάλυση, καθώς και τους τύπους δεδομένων που μπορούν να εξάγουν από τα υποστηριζόμενα ΣμηΕΑ. Στον παρακάτω πίνακα φαίνονται τα διάφορα εργαλεία που μπορούν να χρησιμοποιηθούν για ανάλυση αρχείων καταγραφής πτήσης, καθώς και αυτά που επελέγησαν να χρησιμοποιηθούν στο πλαίσιο της συγκεκριμένης μελέτης.

Πίνακας 2: Εργαλεία Digital Drone Forensics

Όνομα εργαλείου	Τύπος	Μοντέλα υποστηριζόμενων ΣμηΕΑ	Τύπος υποστηριζόμενων αρχείων	Εργαλεία που χρησιμοποιήθηκαν	Περισσότερες πληροφορίες
Cellebrite UFED	Εμπορικό	Άγνωστο	Άγνωστο		Link
MSAB/URSA XRY Drone	Εμπορικό	DJI ΣμηΕΑ, Άγνωστα μοντέλα	.dat, .bin, .txt, .csv, .kml		Link
Oxygen Forensics	Εμπορικό	Parrot all, DJI Phantom 3, DJI Phantom 4, DJI Inspire 1, Mavic, and DJI Inspire 2	.dat, .bin, .txt, .csv, .kml		Link
DatCon parser & CsvView	Ανοιχτού Κώδικα	DJI Phantom 3, DJI Inspire 1, DJI Mavic Pro, and DJI Phantom 4, DJI Phantom 4 Pro, DJI Inspire 2, DJI Matrice M100, DJI M600	.dat, .txt, .csv, .kml	DatCOn	Link

DRone Open source Parser (DROP)	Ανοιχτού Κώδικα	DJI Phantom 3	.dat, .csv		Link
GRYPHON	Ανοιχτού Κώδικα	ΣμηΕΑ συμβατά με Ardupilot	.bin	GRYPHON	Link
Google Earth Pro	Εμπορικό/ Free	Όλα τα ΣμηΕΑ	.kml		Link
Αλγόριθμος Drone Forensics	Ανοιχτού Κώδικα	ΣμηΕΑ συμβατά με Ardupilot, πληθώρα DJI μοντέλων	dat, .txt, .csv, .bin	Αλγόριθμος Drone Forensics	Παράρτημα Α

Στα παραπάνω εργαλεία δεν συμπεριελήφθησαν άλλα εργαλεία ψηφιακής εγκληματολογίας, τα οποία ενδεχομένως να είναι χρήσιμα στην όλη διαδικασία της έρευνας, όχι όμως στην ανάλυση των δεδομένων καταγραφής πτήσης, όπως για παράδειγμα το FTK Imager που χρησιμοποιείται για να εξάγει και να δημιουργήσει εικονικά αντίγραφα των δεδομένων που βρέθηκαν σε εσωτερικό ή εξωτερικό χώρο αποθήκευσης.

Τα δύο (2) εργαλεία που χρησιμοποιήθηκαν στο πλαίσιο της έρευνας είναι το GRYPHON για την ανάλυση των αρχείων καταγραφής πτήσης ΣμηΕΑ συμβατών με Ardupilot αλλά και το DatCon το οποίο χρησιμοποιήθηκε για την αποκρυπτογράφηση (decoding) και την αρχική ανάλυση (parsing) των δεδομένων για την περαιτέρω ανάλυσή τους από τον προτεινόμενο αλγόριθμο ανάλυσης ανοιχτού κώδικα (Drone Forensics), το οποίο και δημιουργήθηκε για την υποστήριξη των ερευνητών σε τέτοιες έρευνες καλύπτοντας την πληθώρα των ΣμηΕΑ.

Στο **τρίτο στάδιο** πραγματοποιήθηκε η ανάλυση των δεδομένων με την χρήση του αλγορίθμου ανάλυσης ανοιχτού κώδικα (Drone Forensics), ο οποίος υποστηρίζεται από τα DatCon και Gryphon. Τα δεδομένα καταγραφής πτήσης από διάφορα ΣμηΕΑ χρησιμοποιήθηκαν για να εξεταστούν και να αξιοποιηθεί ο αλγόριθμος. Επίσης, η εξέταση περιφερειακών συσκευών καθώς και καταστροφικοί μέθοδοι άντλησης δεδομένων (chip-off) δεν εξετάστηκαν και ως εκ τούτου τα αντίστοιχα βήματα παρακάμφθηκαν.

Αναφορικά με τον αλγόριθμο ανάλυσης ανοιχτού κώδικα (Drone Forensics), ο πηγαίος κώδικας (Παράρτημα Α), υλοποιήθηκε βάσει των παραδοχών που περιγράφηκαν σε προηγούμενη ενότητα, έχοντας την δυνατότητα να αναλύσει δεδομένα διαφορετικού τύπου και μορφής μέσω δύο (2) διακριτών modes: Gryphon και DJI (python3 dronedataanalyzer.py --mode=<mode> --file <filename>). Για την ενεργοποίηση των εκάστοτε modes χρησιμοποιήθηκαν οι παρακάτω εντολές:

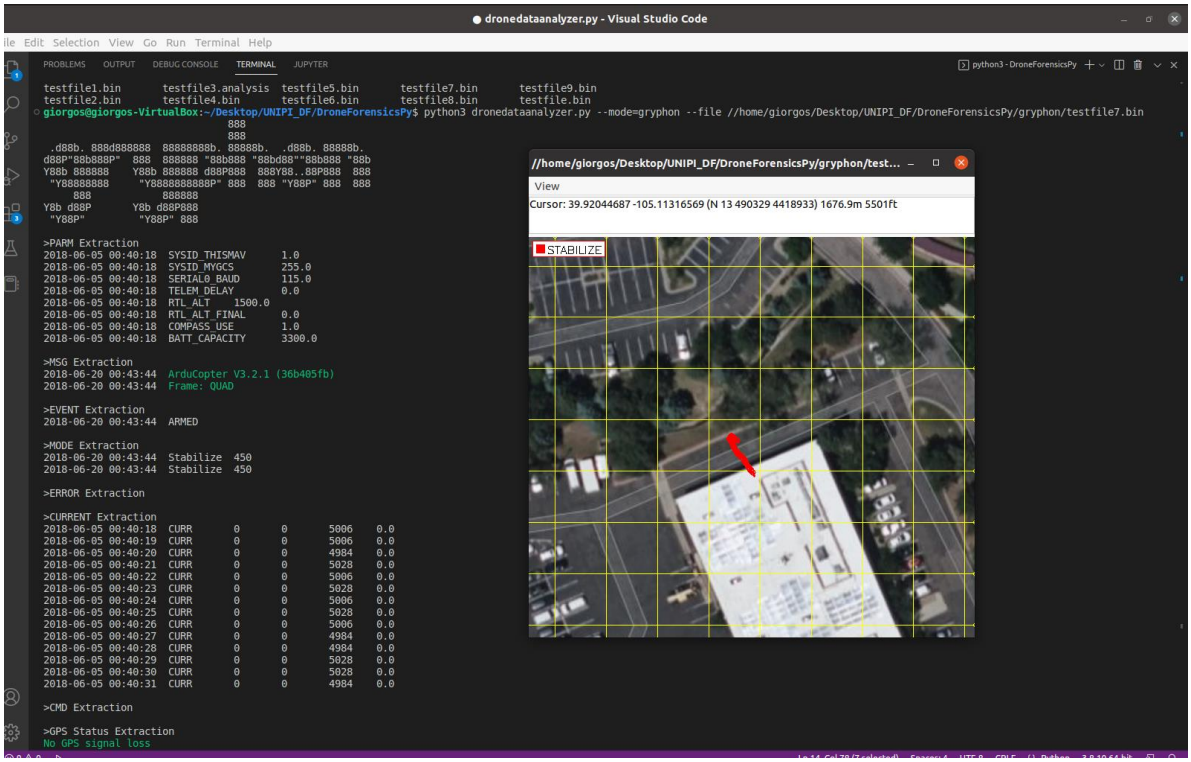
- **Gryphon**: python3 dronedataanalyzer.py --mode=gryphon --file <filename>
- **DJI**: python3 dronedataanalyzer.py --mode=dji –analyse

Τα αποτελέσματα της ανάλυσης παρουσιάζονται στην Ενότητα 5.

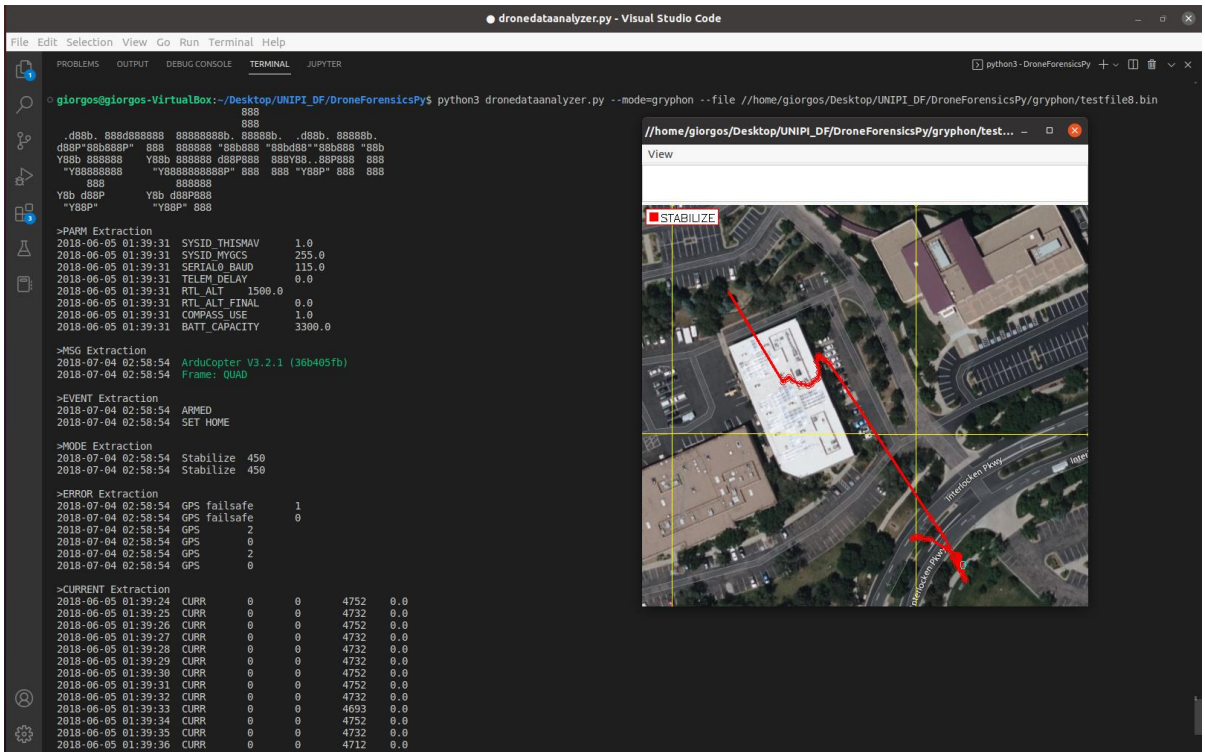
Τέλος, το **τελευταίο στάδιο** της μεθοδολογίας (Αναφορά), και λόγω του ότι χρησιμοποιήθηκε μόνο το παρών εργαλείο για την ανάλυση δεν χρειάστηκε επικύρωση των αποτελεσμάτων από διαφορετικά εργαλεία. Τα υπόλοιπα βήματα, παραλήφθηκαν λόγω της άμεσης σύνδεσής τους με το πρώτο στάδιο, ως προς την σύγκριση των αποτελεσμάτων και την εξακρίβωση των γεγονότων μέσω των αποτελεσμάτων των Digital Forensics.

5. Αποτελέσματα

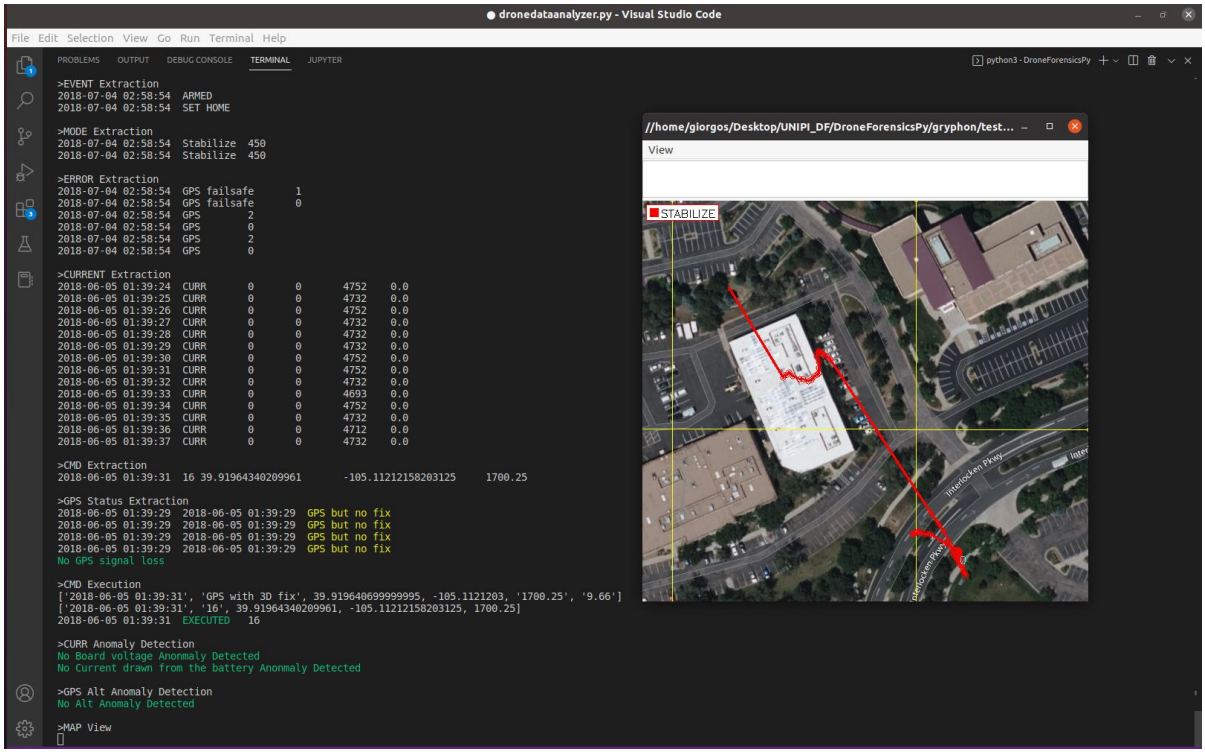
Στην παρούσα ενότητα παρουσιάζονται κάποια ενδεικτικά αποτελέσματα του αλγορίθμου σε δύο (2) περιπτώσεις, (α) όταν το αρχείο καταγραφής πτήσης προέρχεται από ΣμηΕΑ συμβατό με Ardupilot, το οποίο αναλύεται από το mode -gryphon, και (β) όταν το αρχείο καταγραφής πτήσης προέρχεται από ΣμηΕΑ DJI, το οποίο αναλύεται μέσω του mode -dji. Αναφορικά με το DJI analyer, τα αρχεία καταγραφής πτήσεις που εξετάστηκαν ήταν της μορφής <date>xxxx_FLYXXX.DAT, DJIFlightRecord_<date>.TXT FLYXXX.DAT αλλά και DJI_ASSISTANT_xxxxxx.DAT, το οποίο πρόκειται για συμπιεσμένο αρχείο που εμπεριέχει πολλά αρχεία της μορφής FLYXXX.DAT και προέρχονται από το πρόγραμμα της DJI, «DJI Assistant». Δεδομένου ότι η μελέτη αφορά για την αξιολόγηση της διαδικασίας των Digital Drone Forensics, μέσω της συλλογής και ανάλυσης των δεδομένων καταγραφής πτήσης που εξήχθησαν, τυχόν προσωπικά δεδομένα ή αναγνωριστικά που σχετίζονται με το ΣμηΕΑ και εξήχθησαν από τα αρχεία καταγραφής πτήσεων, δεν παρουσιάζονται.



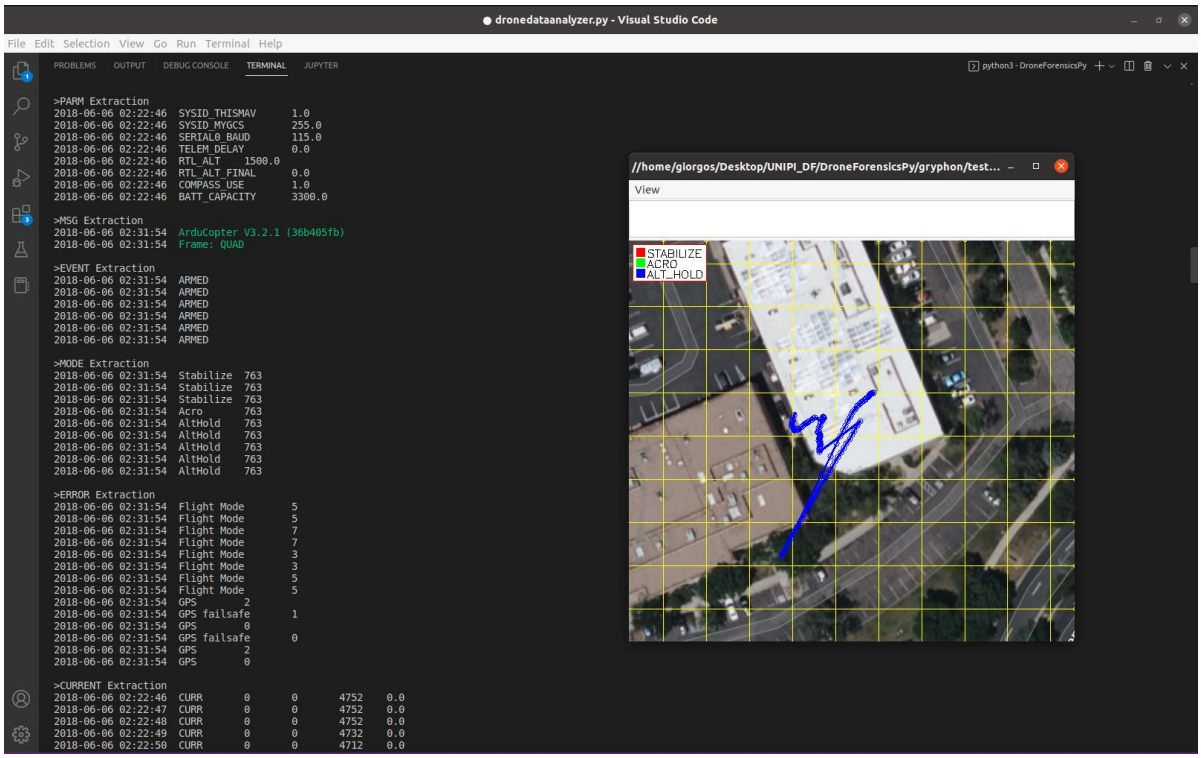
Εικόνα 18: Gryphon results (testfile 1)



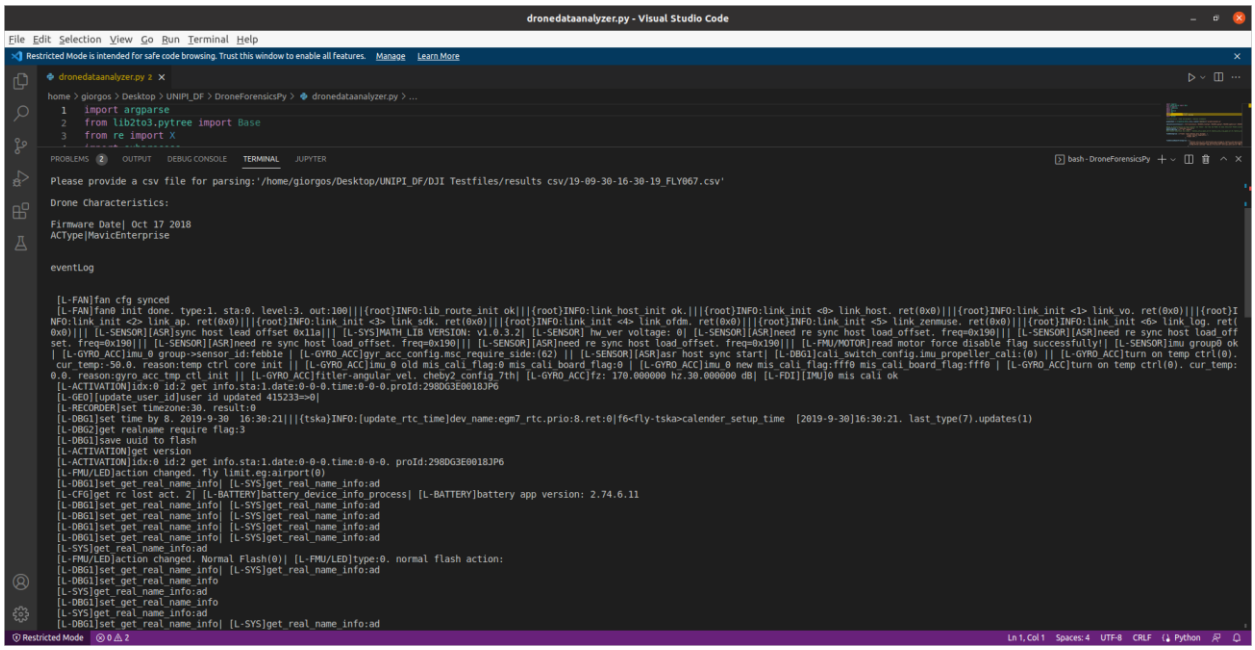
Εικόνα 19: Gryphon results (testfile 2-1)



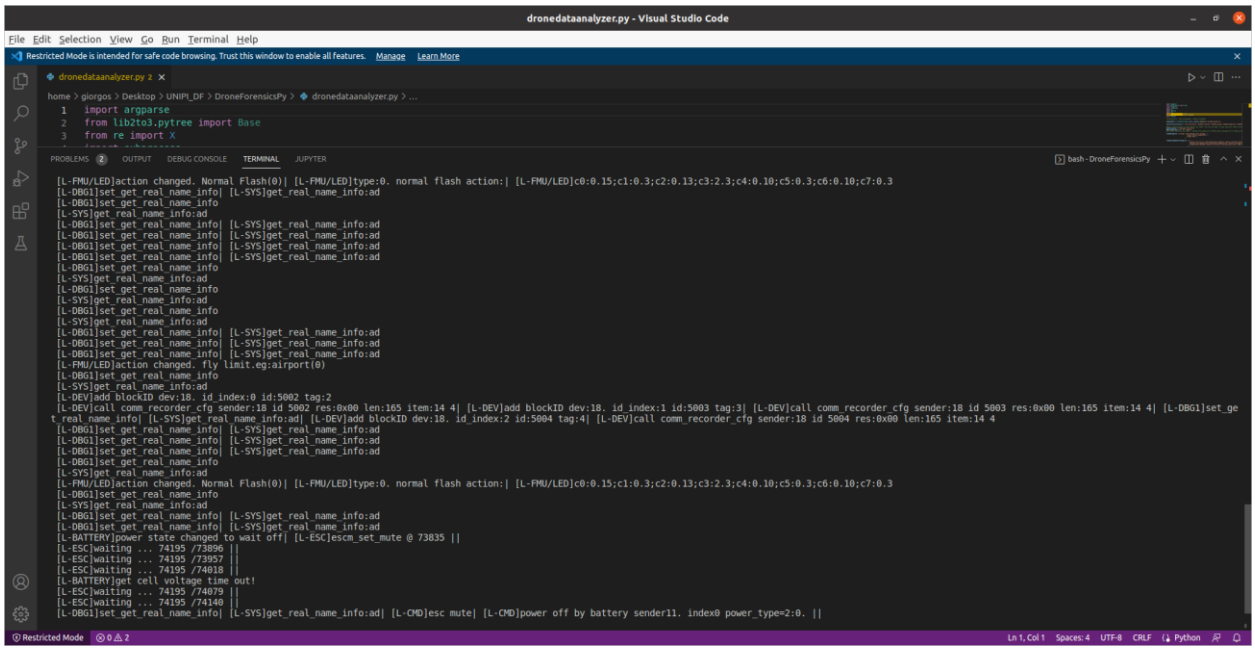
Εικόνα 20: Gryphon results (testfile 2-2)



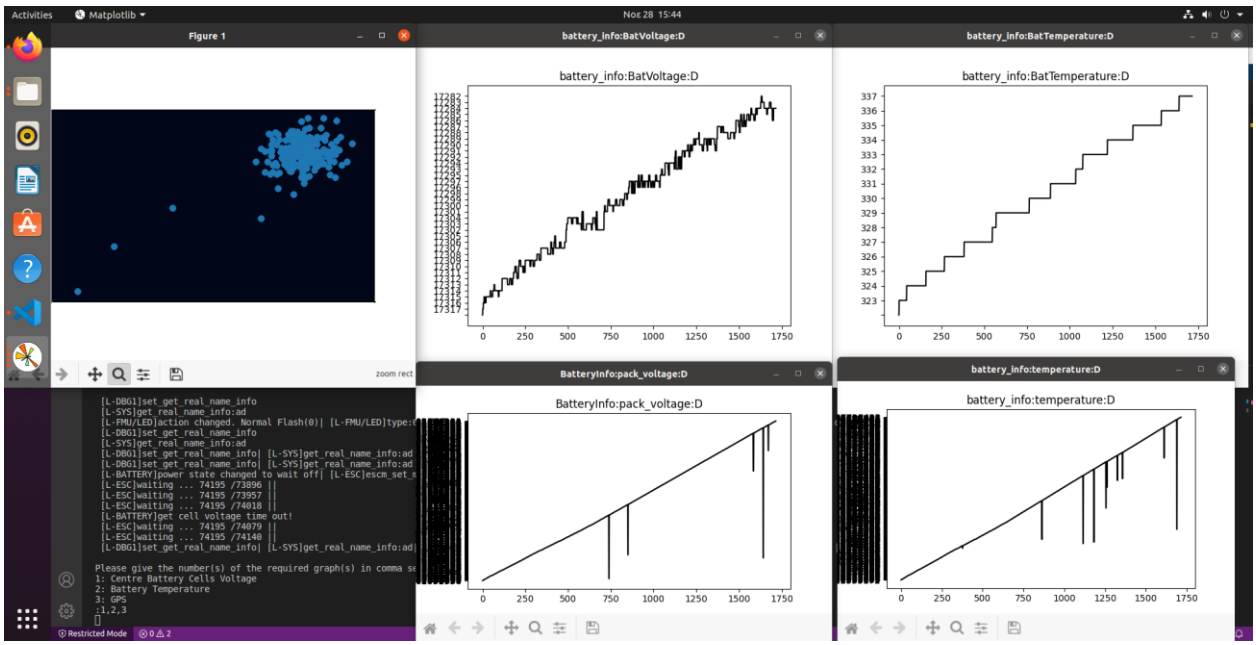
Εικόνα 21: Gryphon results (testfile 3)



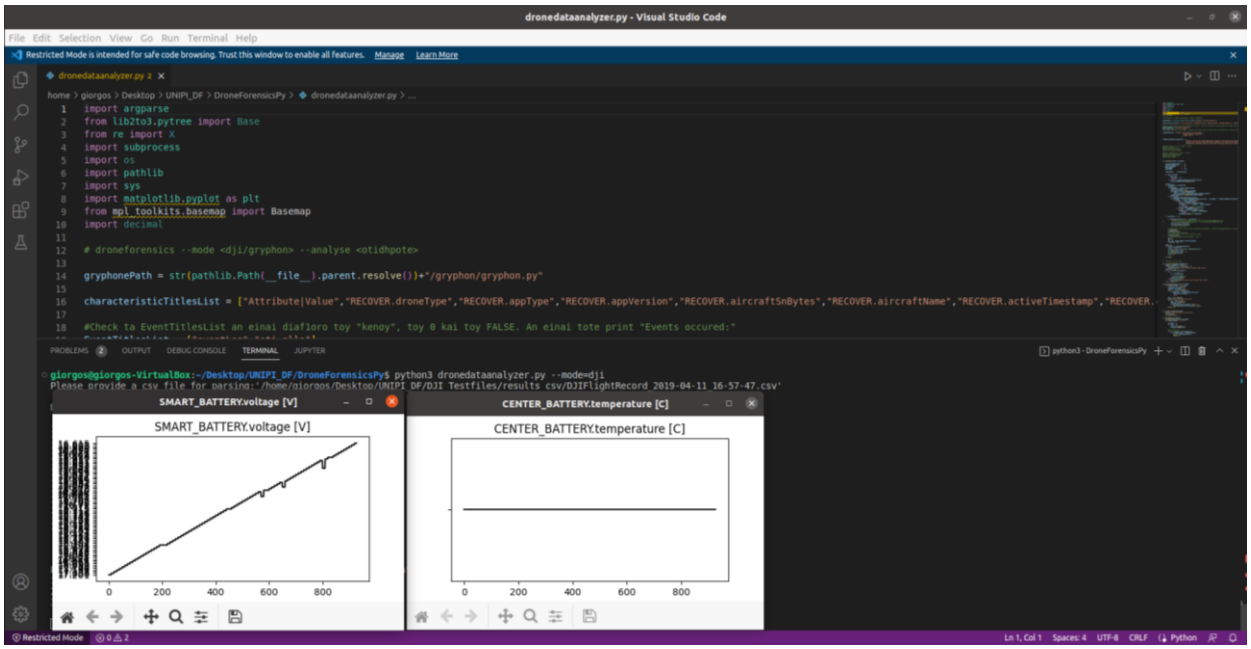
Εικόνα 22: DJI Mavic Enterprise - Drone Characteristics/Event Log/Graphs (testfile 4-1)



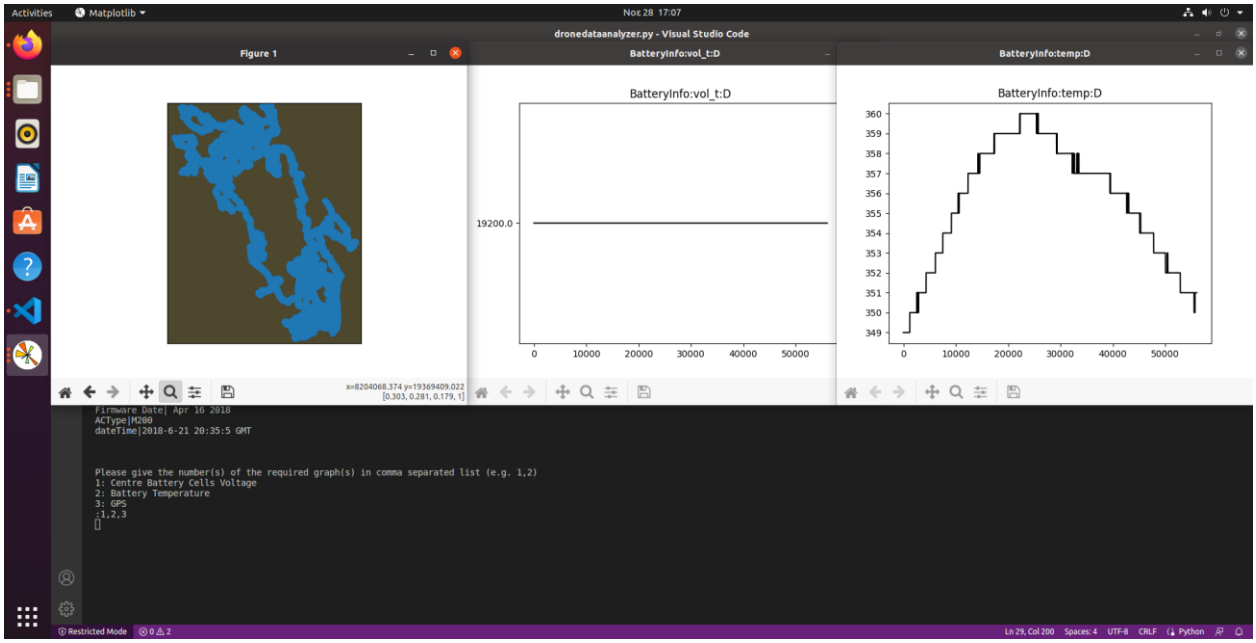
Εικόνα 23: DJI Mavic Enterprise - Drone Characteristics/Event Log/Graphs (testfile 4-2)



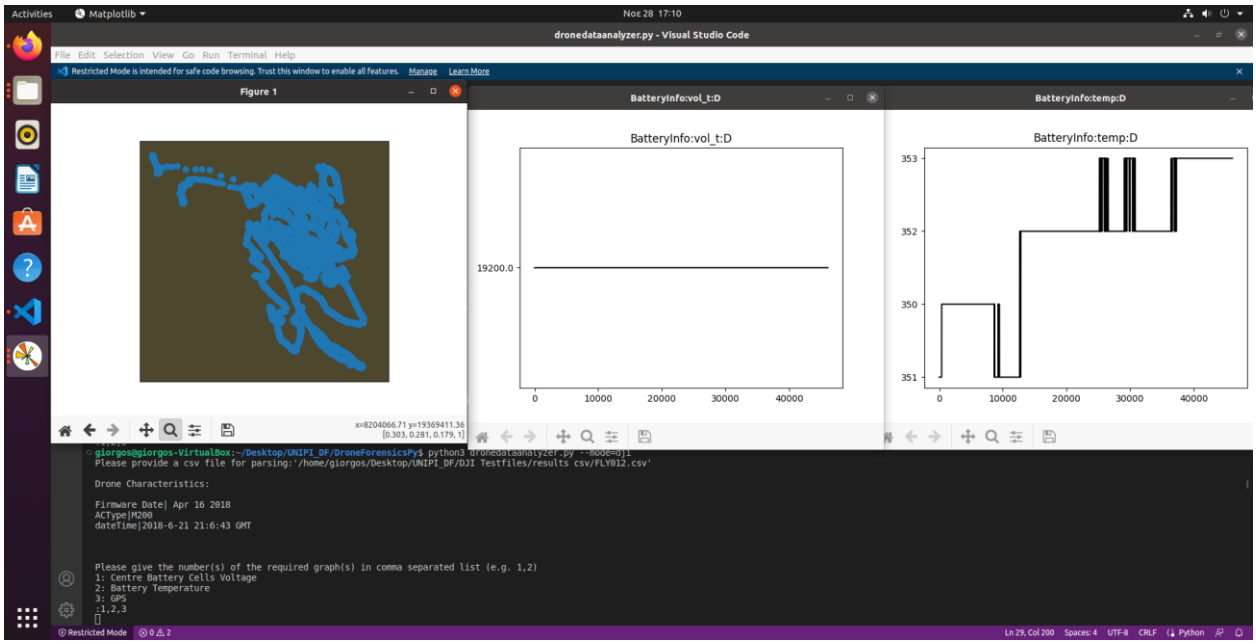
Εικόνα 24: DJI Mavic Enterprise - Drone Characteristics/Event Log/Graphs (testfile 4-3)



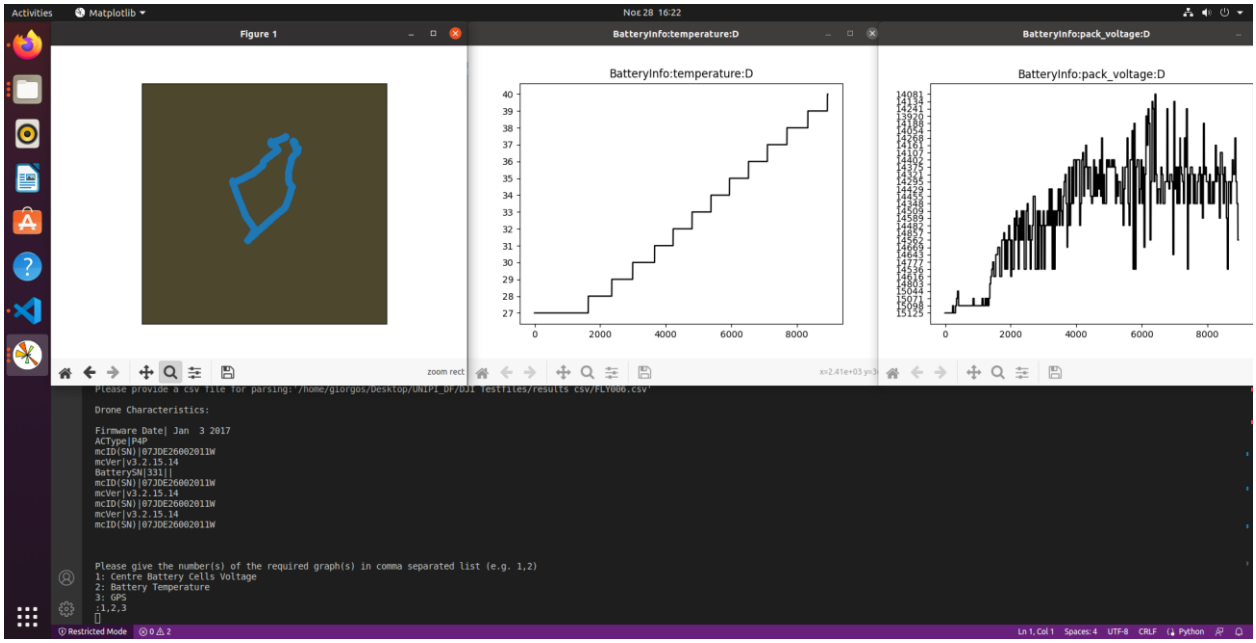
Εικόνα 25: DJI Mavic 2 - Drone Characteristics//Graphs (testfile 5)



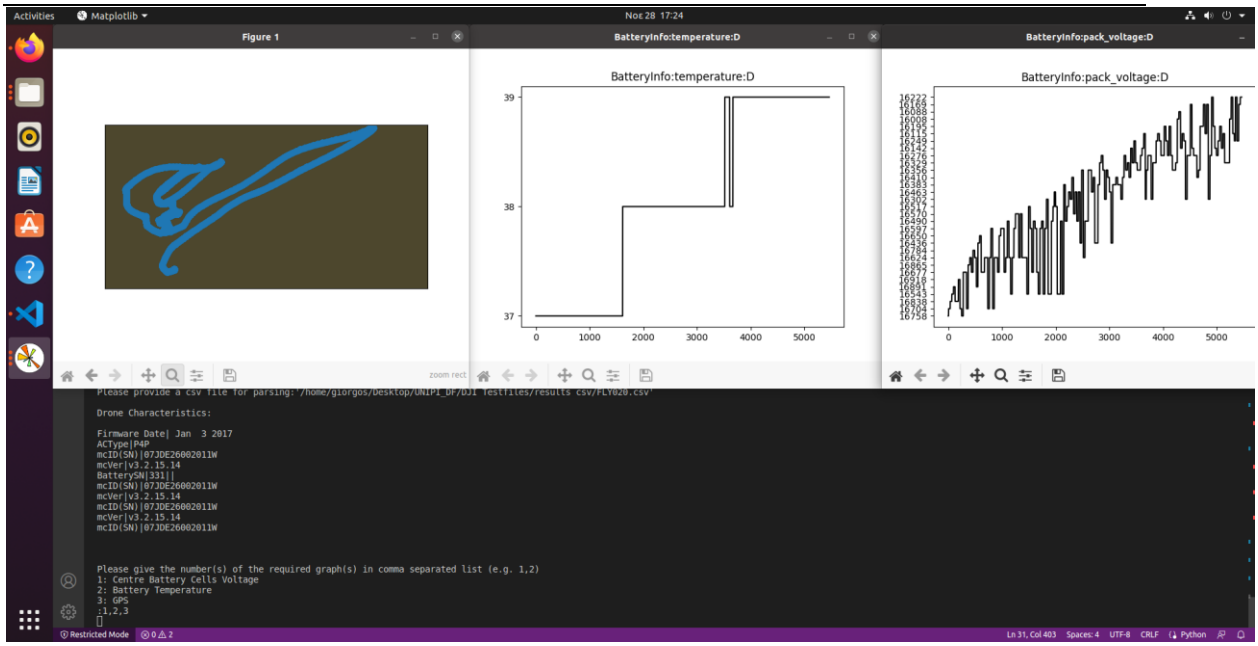
Εικόνα 26: DJI Matrice 200 - Drone Characteristics//Graphs (testfile 6)



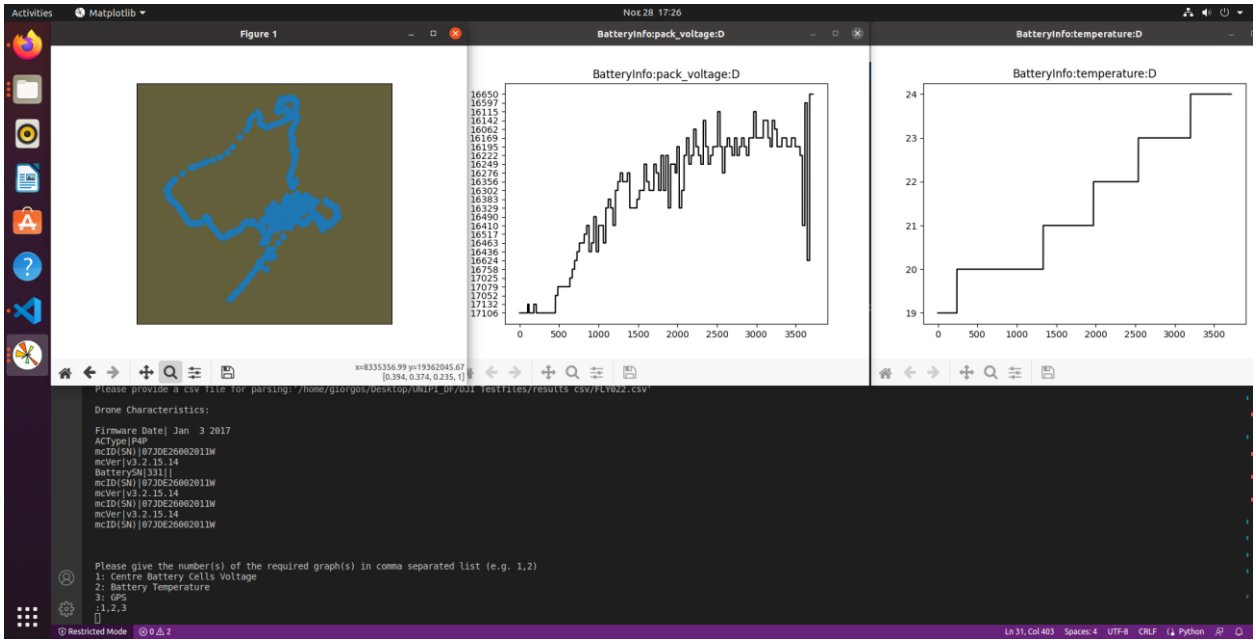
Εικόνα 27: DJI Matrice 200 - Drone Characteristics//Graphs (testfile 7)



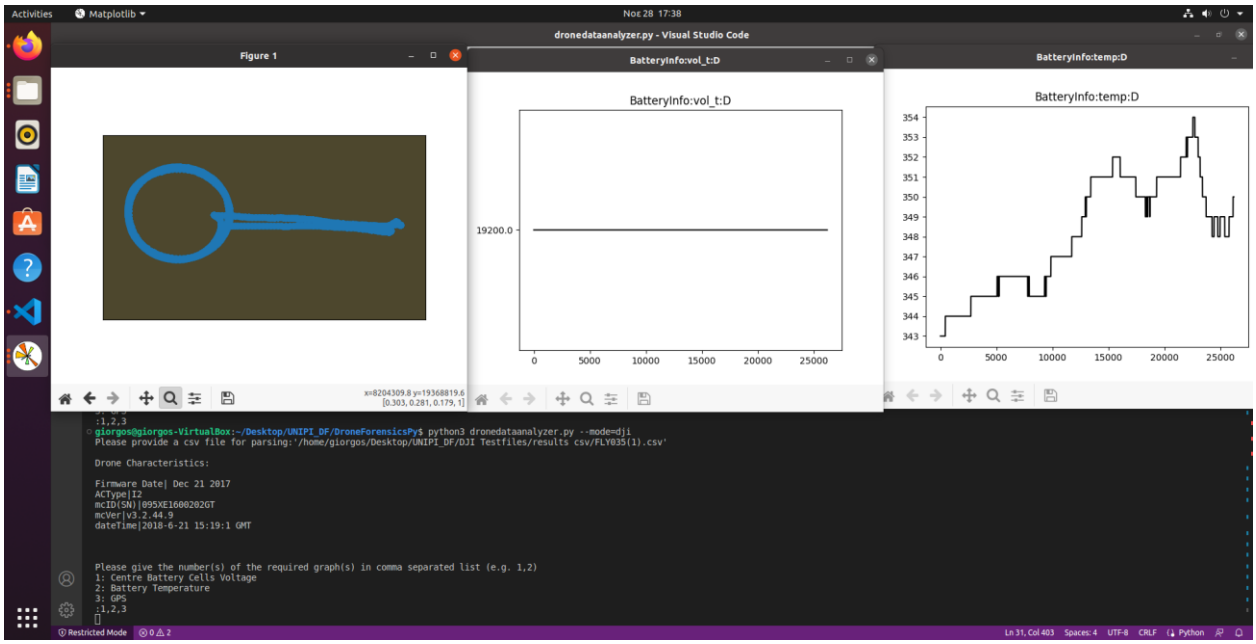
Εικόνα 28: DJI Phantom 4 Pro - Drone Characteristics//Graphs (testfile 8)



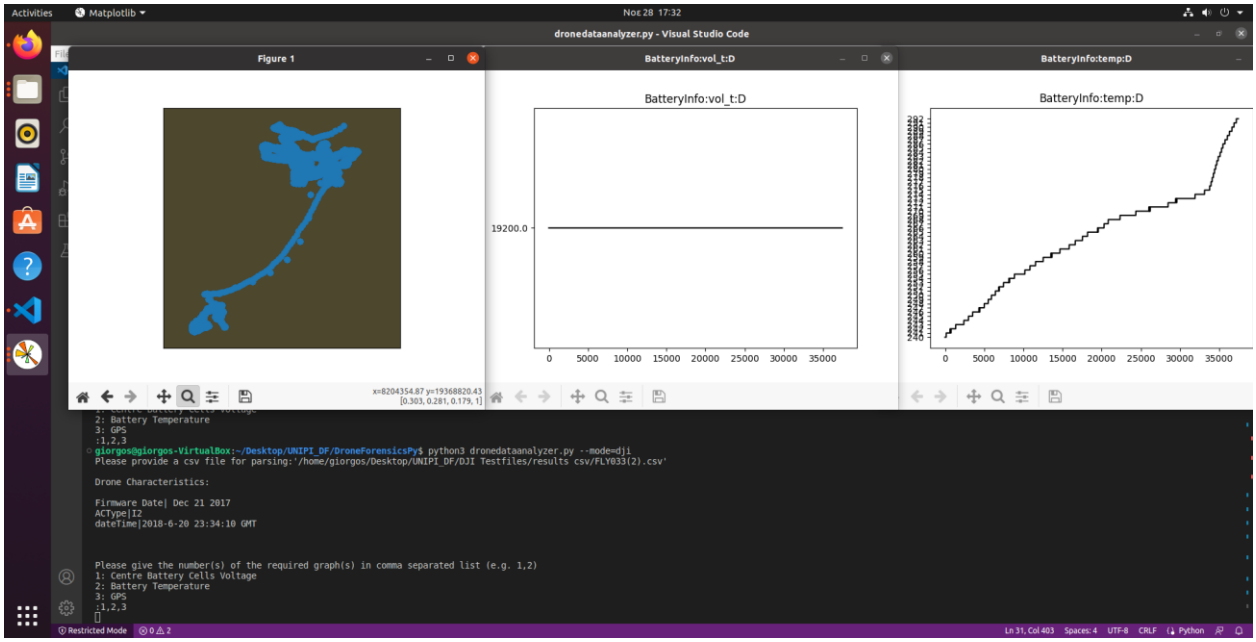
Εικόνα 29: DJI Phantom 4 Pro - Drone Characteristics//Graphs (testfile 9)



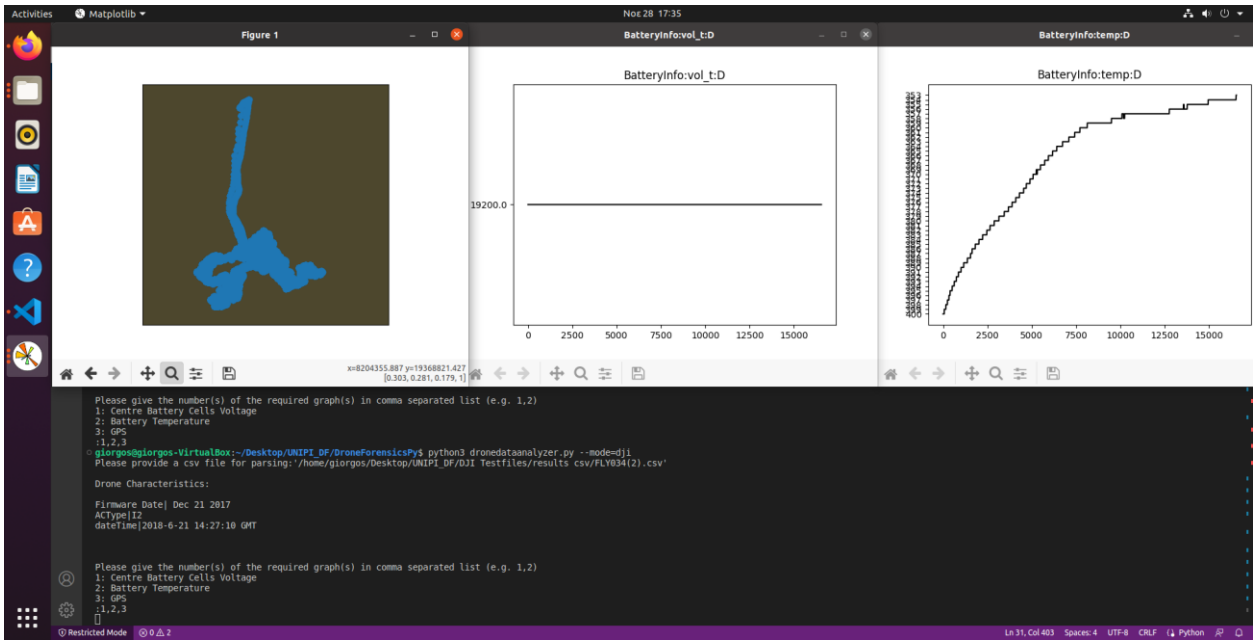
Εικόνα 30: DJI Phantom 4 Pro - Drone Characteristics//Graphs (testfile 10)



Εικόνα 31: DJI Inspire 2 - Drone Characteristics//Graphs (testfile 11)



Εικόνα 32: DJI Inspire 2 - Drone Characteristics//Graphs (testfile 12)



Εικόνα 33: DJI Inspire 2 - Drone Characteristics//Graphs (testfile 13)

6. Συμπεράσματα και Μελλοντική Έρευνα

6.1 Συμπεράσματα

Τα ΣμηΕΑ αναμένεται να επηρεάσουν ακόμη περισσότερο τις μελλοντικές ψηφιακές εγκληματολογικές έρευνες, καθώς τέτοιες συσκευές γίνονται ολοένα και πιο εξελιγμένες αλλά και πιο διαδεδομένες στο ευρύ κοινό. Σε αυτό το έγγραφο, παρουσιάσαμε μια διαδικασία ψηφιακής εγκληματολογίας για τα αρχεία καταγραφής πτήσης που παράγονται από τα ΣμηΕΑ, εστιάζοντας σε εκείνα που είναι συμβατά με το Ardupilot, καθώς και σε ΣμηΕΑ DJI, τα οποία καλύπτουν το μεγαλύτερο μέρος της αγοράς. Πέραν από την προτεινόμενη διαδικασία, ένας αλγόριθμος ικανός να εξετάσει και αναλύσει διαφόρων ειδών και τύπων δεδομένα, αναπτύχθηκε εκμεταλλευόμενος σχετικά εργαλεία Digital Drone Forensics ανοιχτού κώδικα, με σκοπό να προσφέρει γρήγορη και εύκολη ανάλυση των δεδομένων οποιουδήποτε ΣμηΕΑ. Η μεθοδολογία που χρησιμοποιήθηκε βασίστηκε στις προτεινόμενες οδηγίες που δημοσιεύθηκαν από την Interpol, και η οποία θα μπορούσε να τυποποιηθεί για να είναι κοινώς αποδεκτή και μη αμφισβητήσιμη από τα δικαστήρια της εκάστοτε χώρας. Η περίπτωση μελέτης στην οποία στηρίχτηκε η μελέτη ήταν ένα ατύχημα που προκλήθηκε με την χρήση ΣμηΕΑ της DJI και μοντέλου DJI Phantom Pro 4, παρόλα αυτά τα αποτελέσματα αυτής δεν περιορίζονται μόνο στο συγκεκριμένο μοντέλο. Οι αναλύσεις των δεδομένων στηρίζονται σε μεγάλο βαθμό στην ακεραιότητα και αποδοτικότητα των προγραμμάτων αρχικής ανάλυσης (parsing), καθώς συγκεντρώνουν, αναλύουν και παρουσιάζουν την πληροφορία που προέρχεται από τους διάφορους parsers. Η ανάπτυξη και η χρήση του αλγορίθμου αυτού που έχει ως στόχο την ανάλυση αρχείων καταγραφής πτήσης διαφόρων ΣμηΕΑ, μπορεί να θεωρηθεί ως ένα πρώτο βήμα προς την ανάπτυξη ενός πρωτότυπου εργαλείου ψηφιακής εγκληματολογίας το οποίο θα δύναται να εξετάσει και αναλύσει συγκεντρωτικά όλα τα δεδομένα που προέρχονται από τα διάφορα εμπορικά ΣμηΕΑ. Περιορισμοί, προκλήσεις και κενά σε νομοθετικό και τεχνολογικό πλαίσιο περιγράφονται στο παρόν έγγραφο το οποίο και δίνει αποτελέσματα, πληροφορίες και απόψεις με σκοπό τις αλλαγές, βελτιώσεις και περαιτέρω έρευνες στα ΣμηΕΑ, τις διαδικασίες ψηφιακής εγκληματολογίας των ΣμηΕΑ, καθώς και την εναρμόνιση και τυποποίηση των διαδικασιών που ακολουθούνται από τις κατασκευάστριες εταιρίες. Προς αυτή την κατεύθυνση, και με την χρήση βέλτιστων πρακτικών από όλα τα ενδιαφερόμενα μέρη, θα μπορέσει να επιτευχθεί η ανάπτυξη και βελτίωση τέτοιων χρήσιμων εργαλείων ψηφιακής εγκληματολογίας.

6.2 Περιορισμοί

Όπως αναφέρθηκε στην αρχή αυτής της μελέτης, η συγκεκριμένη έρευνα επικεντρώθηκε μόνο στην ανάλυση αρχείων καταγραφής πτήσης προερχόμενα από διαφορετικά μοντέλα DJI, όπως τα Inspire 1, Inspire 2, Mavic 2 Pro, Mavic 2 Enterprise, DJI Phantom 3, DJI Phantom 4, Matrice M200, Matrice M210. Είναι, λοιπόν, κατανοητό ότι επιπρόσθετα μοντέλα της εταιρίας δεν συμπεριελήφθησαν στην έρευνα. Επιπροσθέτως, πρέπει να σημειωθεί πως η συγκεκριμένη εργασία δεν περιλαμβάνει την πλήρη εγκληματολογική μελέτη για τα ΣμηΕΑ, καθώς επίσης δεν αφορά όλα τα εμπορικά ΣμηΕΑ, παρόλα αυτά αποτελεί ένα εργαλείο που συνδράμει στην ανάλυση δεδομένων πτήσεων από ένα ευρύ φάσμα ΣμηΕΑ. Η DJI καθώς και τα ΣμηΕΑ συμβατά με Ardupilot κατέχουν πάνω από το 80% της παγκόσμιας αγοράς αναφορικά με τις πωλήσεις ΣμηΕΑ, αιτιολογώντας, έτσι, την ανάγκη για να επικεντρωθούμε σε αυτού του τύπου τα ΣμηΕΑ. Επιπλέον, με βάση τον όγκο της έρευνας και του χρόνου που απαιτείται για τη διεξαγωγή μιας ενδελεχούς ψηφιακής εγκληματολογικής ανάλυσης, δεν ρεαλιστικό να καλυφθεί το σύνολο των εμπορικών ΣμηΕΑ. Αλλαγές που θα εφαρμοστούν σε νέες εκδόσεις των υπαρχόντων ΣμηΕΑ (DJI) ή ακόμα και σε νέα μοντέλα, ενδεχομένως να επηρεάσουν την λειτουργικότητα και χρηστικότητα του αλγορίθμου.

Όσον αφορά τον προτεινόμενο αλγόριθμο, ο μεγαλύτερος περιορισμός είναι ότι τα αρχεία DAT και TXT προέρχονται από κατασκευάστριες εταιρίες και είναι συνεχώς μεταβαλλόμενα. Η

καταγραφή των στηλών που εμπεριέχουν αυτά τα δεδομένα έγινε σε περιορισμένο dataset , το οποίο ενδεχομένως να μην καλύπτει όλο το φάσμα των πιθανών δεδομένων που μπορεί να εξαχθούν από αρχεία DAT.

Επιπροσθέτως, αξίζει να σημειωθεί πως ο αναλυτής (parser) «DatCon» που χρησιμοποιήθηκε, προσφέρει ένα επίπεδο πρώτης ανάλυσης και ταξινόμησης των δεδομένων που βρίσκονται σε ένα αρχείο καταγραφής, της οποίας αποτέλεσμα εμπεριέχεται σε ένα αρχείο τύπου .csv. Παρόλο που υπάρχει η δυνατότητα ανάλυσης όλων των αρχείων που προέρχονται από ΣμηΕΑ DJI, παρουσιάζεται διαφορετικότητα στις παραγόμενες από το DatCon στήλες, το οποίο ενδέχεται να προέρχεται από τον τύπο, το μοντέλο, το firmware version, κ.ο.κ. του εκάστοτε ΣμηΕΑ. Τέλος, δεν εξετάζεται η ακεραιότητα των εξαγόμενων δεδομένων από τον parser DatCon, το οποίο και διασφαλίζει την εγκυρότητα των αποτελεσμάτων.

6.3 Μελλοντική Έρευνα

Η παρούσα μελέτη περιορίζεται στην χρησιμοποίηση εργαλείων που είναι διαθέσιμα στο ευρύ κοινό. Παρόλα αυτά, περιορισμένος αριθμός αυτών είναι πραγματικά αποδοτικά και ακόμα λιγότερα είναι εφικτό να αποκωδικοποιήσουν τα δεδομένα ενδιαφέροντος (parsers). Ένα πεδίο μελλοντικής έρευνας θα μπορούσε να αφορά την ανάπτυξη και εξέλιξη των parsers που είναι αυτή τη στιγμή διαθέσιμοι με στόχο την καθολική δυνατότητα parsing όλων των εμπορικών ΣμηΕΑ (drone-agnostic parsers). Σε αυτή την περίπτωση, η μελλοντική έρευνα θα μπορούσε να βοηθηθεί αρκετά εφόσον οι κατασκευαστές τυποποιούσαν μέσω ενός και μόνο πρότυπου την καταγραφή των δεδομένων πτήσης.

Καθώς, η παρούσα διατριβή εξετάζει μόνο τα αρχεία καταγραφής πτήσης που εξήχθησαν από το ΣμηΕΑ θα μπορούσαν μελλοντικά να αναλυθούν και τα συμπληρωματικά δεδομένα τα οποία προέρχονται από περιφερειακές ή άλλες συσκευές/πηγές, όπως για παράδειγμα κινητό/tablet, χειριστήριο, εσωτερική μνήμη, κ.ο.κ.

Ενδιαφέρον παρουσιάζει και η διασύνδεση όλων των αναλύσεων και αποτελεσμάτων από τα δεδομένα σε κάποιον δυσδιάστατο ή τρισδιάστατο χάρτη αναπαράστασης του συμβάντος με ταυτόχρονη εισαγωγή και σύνδεση δεδομένων ενδιαφέροντος (φωτογραφία, events, κλτ.) συναρτήσει του χρόνου. Μια τέτοια μελλοντική έρευνα θα βοηθούσε αρκετά τους ερευνητές και θα εξοικονομούσε αρκετό χρόνο από την όλη διαδικασία.

Τέλος, οι τρόποι με τους οποίους επιτυγχάνεται μια μέθοδος Anti-forensics αναφορικά με τα παραγόμενα δεδομένα των ΣμηΕΑ είναι ακόμα ένα πιθανό θέμα ερευνητικού ενδιαφέροντος. Πρέπει να κατανοηθεί πλήρως το πεδίο και ο τύπος των δραστηριοτήτων που ενδέχεται να χρησιμοποιηθεί ένα ΣμηΕΑ για την τέλεση εγκληματικών ενεργειών, καθώς επίσης και οι ενέργειες που γίνονται για την αντιμετώπιση των εγκληματολογικών ερευνών. Μάλιστα το παραπάνω αποτελεί ένα από τα πιο συχνά αναφερόμενα προβλήματα σε Digital Forensics [39].

6.4 Προκλήσεις

Στον τομέα των ΣμηΕΑ, υπάρχει μια πληθώρα από προκλήσεις που θα πρέπει να ληφθούν υπόψη για ενδεχόμενη μελλοντική έρευνα, καθώς επίσης και από τους φορείς και οργανισμούς που ασχολούνται με εγκληματολογικές έρευνες, κανονισμούς και τυποποιήσεις στον τομέα.

Αρχικά, όπως έχει γίνει σαφές από την παρούσα μελέτη, η τεχνολογία των ΣμηΕΑ αλλά και συναφών τεχνολογιών (π.χ. 5G, 6G, κτλ.) είναι ταχέως αναπτυσσόμενοι, και επηρεάζουν άμεσα τον τρόπο κατασκευής τους, τις επικοινωνίες, την πλοήγησή τους, κ.ο.κ. Έτσι λοιπόν, γίνεται κατανοητό το μέγεθος της πρόκλησης αναφορικά με την διεξαγωγή μιας έρευνας ψηφιακής εγκληματολογίας σε ΣμηΕΑ και στις συσχετιζόμενες σε αυτό συσκευές. Ο πρωτεύον στόχος σε μια τέτοια έρευνα είναι να εντοπιστούν οι διαδρομές πτήσης, οι πιθανές δυσλειτουργίες, οι συγκρούσεις και τα σχετικά μέσα (εικόνες και βίντεο) που περιέχονται στις συσκευές του συστήματος [48]. Τα στοιχεία αυτά θα διευκολύνουν τον ερευνητή να κατανοήσει την αποστολή του ΣμηΕΑ και να εξάγει ασφαλή συμπεράσματα, σύμφωνα με τα ευρήματα που προέρχονται από τα ηλεκτρονικά αποδεικτικά στοιχεία και για τα οποία θα πρέπει να ακολουθούνται

τυποποιημένες διαδικασίες και βήματα για να διασφαλίζεται ότι η έρευνα και τα αποτελέσματα αυτής δεν αμφισβητούνται σε δικαστήριο.

Ο ερευνητής κατά την διάρκεια συλλογής και ανάλυσης δεδομένων θα πρέπει επίσης να λάβει υπόψη τα δεδομένα που ενδέχεται να βρίσκονται αποθηκευμένα στο νέφος (π.χ. στοιχεία σε διακομιστή άλλης χώρας) και για το οποίο η ψηφιακή εγκληματολογία αντιμετωπίζει αρκετές προκλήσεις. Χαρακτηριστικό παράδειγμα τέτοιων δυσκολιών αποτελεί η χορήγηση άδειας για την συλλογή δεδομένων από τον εκάστοτε πάροχο cloud, το οποίο δεν επιτυγχάνεται πάντα.

Τέλος, η παρουσία πολλαπλών ψηφιακών συσκευών συσχετιζόμενων με το ΣμηΕΑ και λόγω της διαφορετικότητάς τους (κάμερες, σταθμός ελέγχου, tablet/κινητό τηλέφωνο), απαιτεί ένα αρκετά υψηλό επίπεδο τεχνογνωσίας από τους ερευνητές που καλούνται να διεξάγουν την ψηφιακή εγκληματολογία ενός ΣμηΕΑ στο σύνολό του, καθώς κάθε συσκευή απαιτεί διαφορετικές τεχνικές απόκτησης και εξέτασης, αλλά και την κατάλληλη εξειδίκευση.

Μια επιπρόσθετη πρόκληση που έχει να αντιμετωπίσει ο εκάστοτε ερευνητής καθώς και η κοινότητα των Drone Forensics, είναι το ίδιο το ΣμηΕΑ, ως συσκευή [48]. Το ΣμηΕΑ πρόκειται για ένα κυβερνο-φυσικό σύστημα, γεγονός που εισάγει αρκετές παραμέτρους στην εγκληματολογική έρευνα. Οι διάφοροι αισθητήρες που ένα ΣμηΕΑ φέρει, ενδέχεται να έχουν σημαντικές διαφορές μεταξύ τους λόγω βαθμονόμησης ή ακρίβειας όπως στην περίπτωση του αισθητήρα πλοήγησης GPS, συγκρίνοντας έναν απλό πομποδέκτη GPS με έναν τύπου Real-Time Kinematic (RTK), ο οποίος δίνει ακρίβεια εκατοστού. Σε περιπτώσεις, λοιπόν, ολικής καταστροφής του ΣμηΕΑ, ο ερευνητής μπορεί να συλλέξει τα δεδομένα της θέσης του, όπως αυτή αναφέρεται από το σταθμό ελέγχου, και όχι από το RTK του ίδιου του ΣμηΕΑ, επομένως τα ψηφιακά πειστήρια δεν μπορούν να αξιολογηθούν με ακρίβεια.

Παρόλα αυτά, η ακρίβεια του αισθητήρα δεν είναι το μόνο πρόβλημα όσον αφορά τα συστήματα δορυφορικής πλοήγησης. Τα ΣμηΕΑ, όπως όλα τα ψηφιακά συστήματα, έχουν τρωτότητες, οι οποίες μεταξύ άλλων περιλαμβάνουν και την αλλοίωση/αντικατάσταση του σήματος δορυφορικής πλοήγησης (GPS spoofing), το οποίο και οδηγεί στην αμφισβήτηση της εγκυρότητας και ακεραιότητας του κατά τη διάρκεια μιας έρευνας.

Όπως αναφέρθηκε επανειλημμένως, το ΣμηΕΑ αποτελείται από αρκετές συσκευές και υποσυστήματα, τα οποία δεν είναι πάντα διαθέσιμα σε οποιαδήποτε εγκληματολογική έρευνα. Χαρακτηριστικό παράδειγμα αποτελούν, τα ΣμηΕΑ που κατασχέθηκαν γιατί πετούσαν πάνω από ζώνες απαγόρευσης πτήσεων όπως είναι οι φυλακές. Στην συγκεκριμένη περίπτωση, η πρόσβαση στο ΣμηΕΑ θα μπορούσε να είναι εφικτή, όχι όμως και στον επίγειο σταθμό ελέγχου, ο οποίος ενδέχεται να μην βρεθεί κατά την έρευνα. Μια άλλη περίπτωση που μπορεί κάποιος ερευνητής να συναντήσει είναι να έχει πάθει ολική καταστροφή το ΣμηΕΑ, ή να μην έχει ανακτηθεί, έτσι θα έχει διαθέσιμη μόνο την συσκευή σταθμού ελέγχου προς ανάλυση. Ως εκ τούτου, δεν υπάρχει πλήρης πρόσβαση σε όλες τις πιθανές πηγές αποδεικτικών στοιχείων. Επιπροσθέτως, μια ακόμη μεγάλη πρόκληση είναι να καθοριστούν οι αξιόπιστες πηγές συλλογής δεδομένων, στις περιπτώσεις που τα δεδομένα από δύο πήγες προκύπτουν να είναι αντικρουόμενα. Δεδομένου ότι αρκετά από τα εμπορικά ΣμηΕΑ δεν αποθηκεύουν τις εντολές και τα αρχεία σε κρυπτογραφημένη μορφή, μπορεί κανείς να «παράγει» τα αρχεία καταγραφής σε οποιαδήποτε από τις δύο συσκευές, ακολουθώντας την ίδια προσέγγιση όπως στο GPS spoofing. Αντιθέτως, στα ΣμηΕΑ που χρησιμοποιείται κρυπτογράφηση στην συσκευή, ενδέχεται το κλειδί να μην είναι πάντα διαθέσιμο για την εξαγωγή των δεδομένων, επομένως η συλλογή τους από εργαλεία Digital Forensics ενδέχεται να είναι «μερική» ή αδύνατη.

Τέλος, η ποικιλομορφία των διαθέσιμων συσκευών ΣμηΕΑ, πρέπει επίσης να ληφθεί υπόψη. Σε αντίθεση με άλλες ψηφιακές συσκευές που έχει χρειαστεί εγκληματολογική μελέτη, τα ΣμηΕΑ πέραν του μεγάλου ποσοστού που κατέχει η κατασκευάστρια εταιρεία DJI στην αγορά, το υπόλοιπο μερίδιο της αγοράς είναι σημαντικά κατακερματισμένο σε διάφορους κατασκευαστές. Επομένως, λόγω της ύπαρξης πολλών διαφορετικών ΣμηΕΑ εμφανίζεται και η ανάγκη για δημιουργία πολλαπλών εργαλείων εγκληματολογίας, είτε ενός που να μπορεί να μπορεί να εξετάζει διαφορετικά ΣμηΕΑ ανεξαρτήτως κατασκευαστή. Αυτό, όπως αναφέρθηκε προηγουμένως, προϋποθέτει την τυποποίηση των εξαγόμενων από το ΣμηΕΑ δεδομένων για όλους τους κατασκευαστές.

Βιβλιογραφία

[1] «Weapons and Warfare,» [Ηλεκτρονικό]. Available: https://weaponsandwarfare.com/2019/06/17/1845-austria-drops-balloon-bombs-on-venice/.

[2] «Britannica,» [Ηλεκτρονικό]. Available: https://www.britannica.com/biography/Louis-Charles-Breguet.

[3] «War History Online,» [Ηλεκτρονικό]. Available: https://www.warhistoryonline.com/military-vehicle-news/short-history-drones-part-1.html?chrome=1.

[4] «National Military Museum USAF,» [Ηλεκτρονικό]. Available: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/198095/kettering-aerial-torpedo-bug/.

[5] «National Military Museum of USA Navy,» [Ηλεκτρονικό]. Available: https://www.history.navy.mil/content/history/museums/nnam/explore/collections/aircraft/n/n2c-fledgling.html.

[6] «National Military Museum USAF,» [Ηλεκτρονικό]. Available: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196292/radioplane-oq-2a/.

[7] «de Havilland Tiger Moth,» Wikipedia, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/De_Havilland_Tiger_Moth#Training.

[8] «Google Patents,» Google, [Ηλεκτρονικό]. Available: https://patents.google.com/patent/US2490844.

[9] «Imperial War Museums,» [Ηλεκτρονικό]. Available: https://www.iwm.org.uk/history/the-terrifying-german-revenge-weapons-of-the-second-world-war.

[10] «National Air and Space Museum of USA,» [Ηλεκτρονικό]. Available: https://airandspace.si.edu/collection-objects/pioneer-rq-2a-uav/nasm_A20000794000.

[11] «Airforce Technology,» [Ηλεκτρονικό]. Available: https://www.airforce-technology.com/projects/predator-uav/.

[12] «Army Technology,» [Ηλεκτρονικό]. Available: https://www.army-technology.com/projects/rq-11-raven/.

[13] «Military Analyser Military Magazine,» [Ηλεκτρονικό]. Available: https://militaryanalizer.com/uav-rq-20-puma/.

[14] «Federal Aviation Administration,» [Ηλεκτρονικό]. Available: https://www.faa.gov/.

[15] «European Union Aviation Safety Agency,» [Ηλεκτρονικό]. Available: https://www.easa.europa.eu/en.

[16] «DJI,» [Ηλεκτρονικό]. Available: https://www.dji.com/gr.

[17] «European Council,» [Ηλεκτρονικό]. Available: https://www.consilium.europa.eu/el/policies/drones/.

[18] «Commission Delegated Regulation (EU) 2019/945,» [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0945&from=EN.

[19] «BBC News,» [Ηλεκτρονικό]. Available: https://www.bbc.com/news/uk-46803713.

[20] «Baltics News,» [Ηλεκτρονικό]. Available: https://baltics.news/2021/11/25/due-to-drones-air-traffic-at-riga-airport-has-been-temporarily-suspended-today-inspection-started/.

[21] «iefimerida news,» [Ηλεκτρονικό]. Available: https://www.iefimerida.gr/news/240004/synagermos-exaitias-drone-sti-voyli-synelifthi-enas-32hronos.

[22] «Kathimerini,» [Ηλεκτρονικό]. Available: https://www.kathimerini.gr/society/561128713/aspida-kata-drones-pano-apo-ti-voyli/.

[23] «Rotor & Wing International,» [Ηλεκτρονικό]. Available: https://www.rotorandwing.com/2019/01/10/u-s-dea-border-wall-no-drone-drug-smuggling-likely-increase/.

[24] «The Guardian,» [Ηλεκτρονικό]. Available: https://www.theguardian.com/uk-news/2016/jul/21/man-jailed-for-using-drone-to-fly-drugs-into-prisons.

[25] «CNN Greece,» [Ηλεκτρονικό]. Available: https://www.cnn.gr/ellada/story/44865/delivery-narkotikon-me-drone-stis-fylakes-larisas.

[26] «Trikala Voice,» [Ηλεκτρονικό]. Available: https://www.trikalavoice.gr/

[27] «BBC News,» [Ηλεκτρονικό]. Available: https://www.bbc.com/news/world-latin-america-45073385.

[28] «Abqaiq–Khurais attack,» Wikipedia, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Abqaiq%E2%80%93Khurais_attack.

[29] E. Casey, «Digital evidence and computer crime: Forensic science, computers, and the internet,» *Elselvier,* αρ. 3, 2011.

[30] I.Resendez, P.Martinez, J. Abraham, «An introduction to Digital Forensics,» *Research Gate,* 2014.

[31] N. Balon, R.Stovall, T. Scaria, «Computer Intrusion Forensics Research Paper,» *CIS ,* αρ. 544.

[32] S. Kumar, I. Vayansky, «Phising-Challenges and Solutions,» *Computer Fraud & Security,* 2018.

[33] M.N.O. Sadiku, M. Tembely, S.M. Musa, «Digital Forensics,» *International Journal of Advanced Research in Computer Science and Software Engineering,* 2017.

[34] B. Carrier and E. Spafford, «Getting Physical with the Digital Investigation Process,» *International Journal of Digital Evidence,* τόμ. 2, αρ. 2, pp. 1-21, 2003.

[35] J. Henseler, « Computer crime and computer forensics,» *The encyclopedia of forensic science,* 2000.

[36] Zareen, M. S., Waqar, A., & Aslam, B., «Digital forensics: Latest challenges and response,» *Information Assurance (NCIA), 2nd National Conference, IEEE,* 2013.

[37] Kent, K., Chevalier, S., Grance, T., & Dang, H, «Guide to integrating forensic techniques into incident response,» *NIST Special Publication,* pp. 80-86, 2006.

[38] A. Yasinsac, R.F. Erbacher, D.G. Marks, M.M. Pollitt, P.M. Sommer, «Computer forensics education,» *IEEE Security & Privacy,* τόμ. 9, 2003.

[39] Casino, Fran, et al., «Research trends, challenges, and emerging topics in digital forensics: A review of reviews,» *IEEE Access,* 2022.

[40] Mekala, S.H., Baig, Z., «Digital Forensics for Drone Data – Intelligent Clustering Using Self Organising Maps. In: Doss, R., Piramuthu, S., Zhou, W. (eds),» *Future Network Systems and Security. FNSS 2019. Communications in Computer and Information Science, Springer,* τόμ. 1113, 2019.

[41] F. Salamh, U. Karabiyik, M. Rogers and E. Matson, «A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges.,» *Drones 2021,* τόμ.

5, αρ. 42.

[42] «Interpol DFL,» [Ηλεκτρονικό]. Available: https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf.

[43] «FTK Imager,» Exterro, [Ηλεκτρονικό]. Available: https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,(FTK%C2%AE)%20is%20warranted..

[44] «DJI,» Wikipedia, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/DJI.

[45] Mantas, Evangelos & Patsakis, Constantinos, *GRYPHON: Drone Forensics in Dataflash and Telemetry Logs,* 2019.

[46] «Phantom 4 Pro User Manual,» DJI, [Ηλεκτρονικό]. Available: https://dl.djicdn.com/downloads/phantom_4_pro/20170125/user+manual/Phantom+4+Pro+Pro+Plus+User+Manual+v1.2.pdf.

[47] «Drone Forensics,» VTOLabs, [Ηλεκτρονικό]. Available: https://www.vtolabs.com/drone-forensics.

[48] Mantas, Evangelos & Patsakis, Constantinos, «Who watches the new watchmen? The challenges for drone digital forensics investigations,» Array, τόμ. 14, αρ. 100135, 2022.

Παράρτημα Α – Πηγαίος Κώδικας

```
import argparse
from lib2to3.pytree import Base
from re import X
import subprocess
import os
import pathlib
import sys
import matplotlib.pyplot as plt
from mpl_toolkits.basemap import Basemap
import decimal

# droneforensics --mode <dji/gryphon> --analyse <otidhpote>

gryphonePath = str(pathlib.Path(__file__).parent.resolve())+"/gryphon/gryphon.py"

characteristicTitlesList =
["Attribute|Value","RECOVER.aircraftName","RECOVER.aircraftSnBytes","RECOVER.droneTy
pe","RECOVER.appType","RECOVER.appVersion","RECOVER.aircraftSnBytes","RECOVER.ai
rcraftName","RECOVER.activeTimestamp","RECOVER.cameraSn","RECOVER.rcSn","RECOV
ER.batterySn","RECOVER.gimbalType","FIRMWARE.version","DETAILS.photoNum","DETAILS
.videoTime
[s]","DETAILS.aircraftName","DETAILS.aircraftSnBytes","DETAILS.cameraSn","DETAILS.rcSn"
,"DETAILS.appVersion","DETAILS.batterySn","CAMERA_INFO.sdCardInsertState"]

#Check Events, other than blank,0,FALSE. If yes, "Events occurred:"
EventTitlesList = ["eventLog"]
EventListDiscard = ["", "0", "FALSE"]

flyXXXCategories = ["Graph1: Centre Battery Cells Voltage", \
                    "Graph2: Battery Temperature", \
                    "Graph3: GPS", \
                   ]

flyXXXColumnNamesForCategories = [ \

["battery_info:vol_t:D","BatteryInfo:pack_voltage:D","battery_info:pack_voltage:D","SMART_BA
TTERY.voltage [V]","battery_info:BatVoltage:D", "BatteryInfo:vol_t:D"], \
```

```
["battery_info:temperature:D","BatteryInfo:temperature:D","battery_info:temp:D","CENTER_BAT
TERY.temperature [C]","battery_info:BatTemperature:D","BatteryInfo:temp:D"], \

[["IMU_ATTI(0):Latitude","IMU_EX_1:rtk_lati1:D","ahrs_data:ahrs_lati:D","GPS:Lat","ahrs_data:
ns_lati:D","DETAILS.latitude","OSD.latitude","APP_GPS.latitude","IMU_EX_1:rtk_lati1:D"],["IMU
_ATTI(0):Longitude","IMU_EX_1:rtk_long1:D","ahrs_data:ahrs_longti:D","GPS:Long","ahrs_data
:ns_longti:D","DETAILS.longitude","OSD.longitude","APP_GPS.longitude","IMU_EX_1:rtk_long1
:D"]], \
                        ]
#Battery Voltage (vs time) Graph --- FLYxxx

#Battery Temperature (vs time) --- FLYxxx



def plotData(attrIdx, droneData):

    allTitlesToBePresented =  []
    presentationDataList   =  []
    gpsLatitudeData        =  []
    gpsLongData            =  []
    presentGPS             =  False

    numberOfRows    = len(droneData)

    for idx in attrIdx:
        if idx == 3:
            presentGPS = True
            continue
        for title in flyXXXColumnNamesForCategories[idx-1]:
            allTitlesToBePresented.append(title)

    colIndex = -1
    for columnName in droneData[0]:
        colIndex += 1
        if columnName in allTitlesToBePresented:
            newPresentationData = []
            newPresentationData.append(columnName)
```

```
            for rowNum in range(5,numberOfRows):
                newPresentationData.append(droneData[rowNum][colIndex])
            presentationDataList.append(newPresentationData)
        elif presentGPS:
            x = flyXXXColumnNamesForCategories[2][:]
                if columnName in flyXXXColumnNamesForCategories[2][0] or columnName in
flyXXXColumnNamesForCategories[2][1]:
                for rowNum in range(5, numberOfRows):
                    if "lat" in columnName.lower():
                        gpsData = droneData[rowNum][colIndex]
                        if gpsData == ''  or gpsData in gpsLatitudeData:
                            continue
                        gpsLatitudeData.append(float(gpsData))
                    elif "long" in columnName.lower():
                        gpsData = droneData[rowNum][colIndex]
                        if gpsData == '' or gpsData in gpsLongData:
                            continue
                        gpsLongData.append(float(gpsData))

    if presentGPS == True:

        m = Basemap(projection='mill', resolution='c',\
            llcrnrlat=-90,urcrnrlat=90,\
            llcrnrlon=-180,urcrnrlon=180
            )
        m.bluemarble()
        m.drawcoastlines()
        m.drawcountries()
        xpt = 0
        ypt = 0
        xpt, ypt = m(gpsLongData, gpsLatitudeData)
        m.plot(xpt, ypt,'o')

    count = 0
    for dataList in presentationDataList:
        y_axis = dataList[1:]
        x_axis = [i for i in range(0, len(dataList[1:])) ]
        plt.figure(dataList[0])
```

```
        plt.plot(x_axis, y_axis, 'k')
        plt.title(dataList[0])
        count += 1

    plt.show()


#   read data for each index

def validateInputNumbers(grapNumList):
    numbers = grapNumList.split(",")
    if len(numbers) > 3 or len(numbers) < 0:
        printErrorAndExit("Invalid number of graph index values")
    numbersList = []
    for i in range(0,len(numbers)):
        try:
            x = int(numbers[i])
            if x > 3 or x < 0:
                raise Exception('')
            numbersList.append(x)
        except ValueError as e:
            printErrorAndExit("Invalid value of graph index values")
    return numbersList

def printDroneCharacteristics(filePath):
    with open(filePath, 'r') as file:
        firstLine = file.readline()
        characteristicsIndex = -1
        headers = firstLine.split(",")
        for i in range(0, len(headers)):
            if headers[i] in characteristicTitlesList:
                characteristicsIndex = i
                break

        data = file.readline()
        print("\nDrone Characteristics:\n")
        for i in range (0, 10):
            data = file.readline()
```

```
            data=data.split(",")
            if data[characteristicsIndex].strip() != "":
                print(data[characteristicsIndex].strip())
        print("\n")


def printErrorAndExit(message):
    print("The following error occured:\n\n")
    print(message)
    sys.exit("Exiting...")

def parseDJIFile(filePath):
    printDroneCharacteristics(filePath)
    with open(filePath, 'r') as f:

        droneData = []
        for line in f:
            line = line.split(",")
            droneData.append(line)

        #print event log
        for i in range(0, len(droneData[0])):
            if droneData[0][i] in EventTitlesList:
                print(str(droneData[0][i]))
                print("\n")

                for j in range(1, len(droneData)):
                    if droneData[j][i] not in EventListDiscard:
                        print(droneData[j][i])



        print()
        inputMessage = "Please give the number(s) of the required graph(s) in comma separated
list (e.g. 1,2)\n" + \
        "1: Centre Battery Cells Voltage\n"+ \
                            "2: Battery Temperature\n"+ \
                            "3: GPS\n:"
        graphNum = input(inputMessage)
```

```
        numList = validateInputNumbers(graphNum)

        plotData(numList, droneData)



def validateDJIFile(filenamePath):
    if filenamePath.endswith(".csv") or filenamePath.endswith(".csv' ") == False:
        return False, "Provided file is not a csv file"
    else:
        return True, ""


#MAIN starts here

parser = argparse.ArgumentParser(description="Drone Forensics Framework")
parser.add_argument("--mode", choices=['dji','gryphon'],\
    required=True)
parser.add_argument("--file", required=False)
parser.add_argument("--analyse", action='store_true')


args = parser.parse_args()

if args.mode == "gryphon":

    if args.file == None:
        exit("gryphon mode requires a file in arguments (--file <filename>)")
    file = args.file
    p = subprocess.Popen(["python3", gryphonePath, file])
    p.wait()
    #add code to call gryphon
elif args.mode == "dji":
    currDir = pathlib.Path(__file__).parent.resolve()
    if args.analyse:
        #setting file argument to None so that user will be prompt to provide it below
        args.file = None
        p = subprocess.Popen(["java", "-jar", str(currDir) + "/DatCon.4.0.4.jar"])
        p.wait()
```

```
if args.file == None:
    file = input("Please provide a csv file for parsing:")
else:
    file = args.file

file=file.strip().replace('\"', '').replace("'",'')
code = True
if code == False:
    exit("The provided file does not seem to be a valid")
parseDJIFile(file)
```