A 3-DIMENSIONAL UAS FORENSIC INTELLIGENCE-LED TAXONOMY (U-FIT)

by

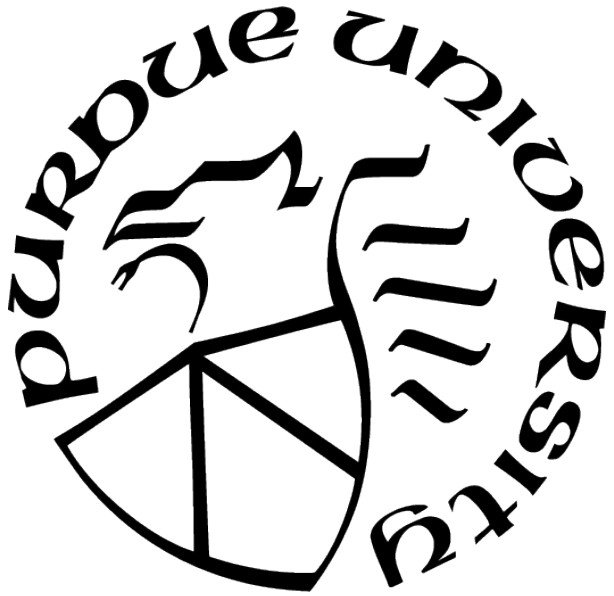
Fahad Esaam Salamh

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy



Polytechnic Institute

West Lafayette, Indiana

August 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Marcus Rogers, Co-chair

Department of Computer and Information Technology

Dr. Umit Karabiyik, Co-chair

Department of Computer and Information Technology

Dr. Eric Matson

Department of Computer and Information Technology

Dr. Albert Marcella

Walker School of Business and Technology

Approved by:

Dr. Kathryne Newton

To my family

Essam Salamh, Kawther Anbari, Rawan Sultan, Hala Salamh, Tala Salamh

ACKNOWLEDGMENTS

First and foremost I am extremely grateful to my supervisors, Dr.Marcus Rogers and Dr.Umit Karabiyik for their invaluable advice, continuous support, and patience during my PhD study. Their immense knowledge and plentiful experience have encouraged me in all the time of my academic research and daily life. I would also like to thank Dr.Eric Matson and Dr.Al Marcella for their support throughout my research development. Also, I would like to thank Dr.Kathryn Speller for her guidance throughout the survey design process.

A special thanks to the Saudi Arabian Cultural Mission in the United States and the Saudi Arabian government for their financial support during my PhD study.

Finally, I would like to express my gratitude to my parents, my wife and children, and my friends who were also a backbone to this research work. Without their tremendous understanding and encouragement in the past few years, it would be impossible for me to complete my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

APD	Antisocial Personality Disorder
DaaS	Drone as a Service
DoD	Department of Defense
DoS	Denial of Service
EPA	Elemental Psychopathy Assessment
FAA	Federal Aviation Administration
FFM	Five Factor Model
GPS	Global Positioning System
IMU	Inertial Measurement Unit
IoD	Internet of Drones
IoT	Internet of Things
IR	Incident Response
RPA	Remotely Piloted Aircraft
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

GLOSSARY

Anti-detection: tactics that prevent the ability of detection systems.

Anti-forensics: techniques that challenge the digital forensic examination process

Counter UAV: systems that interrupt UAV operation.

Drone: a flying object that can operate autonomously or by remote pilot

Flight Controller: a remote control to operate the drone

Forensic Intelligence: the interaction between investigative and behavioral domains

Non-Traditional Digital Forensics: updated approaches to cope with challenges.

Sensor: preprogrammed devices to measure and direct flight operation

Signal Jamming: an intentional interception to the communication channels

Traditional Digital Forensics: previous digital forensic methods and procedures

UAV Threat Actors: drone operators who involve in deviant and/or illegal actions

Gimbal: it stabilizes the camera movement

ABSTRACT

Although many counter-drone systems such as drone jammers and anti-drone guns have been implemented, drone incidents are still increasing. These incidents are categorized as deviant act, a criminal act, terrorist act, or an unintentional act (aka system failure). Examples of reported drone incidents are not limited to property damage, but include personal injuries, airport disruption, drug transportation, and terrorist activities. Researchers have examined only drone incidents from a technological perspective. The variance in drone architectures poses many challenges to the current investigation practices, including several operation approaches such as custom commutation links. Therefore, there is a limited research background available that aims to study the intercomponent mapping in unmanned aircraft system (UAS) investigation incorporating three critical investigative domains—behavioral analysis, forensic intelligence (FORINT), and unmanned aerial vehicle (UAV) forensic investigation. The UAS forensic intelligence-led taxonomy (U-FIT) aims to classify the technical, behavioral, and intelligence characteristics of four UAS deviant actions — including individuals who flew a drone too high, flew a drone close to government buildings, flew a drone over the airfield, and involved in drone collision. The behavioral and threat profiles will include one criminal act (i.e., UAV contraband smugglers). The UAV forensic investigation dimension concentrates on investigative techniques including technical challenges; whereas, the behavioral dimension investigates the behavioral characteristics, distinguishing among UAS deviants and illegal behaviors. Moreover, the U-FIT taxonomy in this study builds on the existing knowledge of current UAS forensic practices to identify patterns that aid in generalizing a UAS forensic intelligence taxonomy. The results of these dimensions supported the proposed UAS forensic intelligence-led taxonomy by demystifying the predicted personality traits to deviant actions and drone smugglers. The score obtained in this study was effective in distinguishing individuals based on certain personality traits. These novel, highly distinguishing features in the behavioral personality of drone users may be of particular importance not only in the field of behavioral psychology but also in law enforcement and intelligence.

1. INTRODUCTION

1.1 Background

There are several important terminologies related to the technology behind unmanned aerial vehicle (UAV) – sometimes called drones. The evolution and capability of the UAV have an association with these terminologies, which include old unmanned aerial vehicle (OUAV), aerial target (AT), unmanned aircraft system (UAS), robotic aerial system (RAS), remotely piloted aerial system (RPAS), and autonomous aerial system (AAS). Each term describes the architecture and capability of a specific flying object [1]. With the rapid increase of commercial drones' use and ease of access by any individual, crimes committed by drones have increased as well. Some of these commercial off-the-shelf (COTS) UAVs are equipped with advanced technologies such as obstacle avoidance sensors. The Federal Aviation Administration (FAA) describes a drone as a small UAS with a size of less than 55 pounds [2]. Also, it should be noted that UAS encompasses the complete system that flies drones (e.g., the UAV operator), while UAV describes the drone body only, without the remote control and/or the ground station control. The author utilizes the term UAS in this research because the selected approach incorporates several elements associated with drone deviant behaviors.

There are several operation capabilities of small UASs that categorize them into classes based on the operational requirement. For instance, hobbyists might be interested in a small UAS that flies between thirty to forty-five minuets compared to a criminal who plans to operate a drone at least two hours. Also, custom-built UAVs provide additional options such as preprogrammed missions and custom communication links. The technology provides a great value to the community from leisure to delivery services; however, the capabilities of small UASs pose many challenges to legalization, forensic investigation, safety, privacy, and cybersecurity. Dedrone, a company specializes in counter UAV technologies, deploys a web scraping technology to map publicly reported drone incidents all over the world—incidents related to multiple UAS threat actors such as drug smuggling and prison contraband, collisions, disruption, surveillance, and weaponization (see Figure 1.1).

Figure 1.1. Reported Small UAS Incidents Wordwide [3]

1.2 Problem Statement and Significance

The number of small UAS incidents, including drug smuggling and airport surveillance are rapidly increasing. Most of the approximately 382 incidents reported between October and December 2019 in the United States were classified as unauthorized small UAS activities (i.e., flew a drone too high, close to a government building, or over an airport) [4]. Research in the UAS forensic field has led to a fair improvement in discovering technical methodologies from acquiring to recovering digital evidence related to drone activity. Tracing information and following a forensic intelligence approach in responding to the massive number of UAS incidents is necessary. For instance, the absence of behavior profiling studies on UAS threat actors might be an opportunity to demystify some investigative complexities, especially in enhancing the classification taxonomy. On the other hand, drones have enabled criminals to utilize their technology to make them untraceable, and it is thereby easier to complete illegal redand/or drone deviant activities. The root cause of these incidents tends to scientifically tie to a certain level of individual's behavior, which can be further studied with some demographic background of UAV threat actors and self-reported crimes. In regard to UAV customization, a high technical background is expected as most operations require either long range flight, autonomous mode, or sophisticated techniques (e.g., anti-forensics). Drone crimes share similar techniques, and autonomous flight operation is not always necessary. This study takes several factors into consideration from several perspectives. From the

psychological perspective, the author examines certain personality patterns associated with UAS crime intention. The behavioral examination of the five threat actors will be employed to distinguish between them and enhance the proactive investigative technique.

The psychological aspect of deviant activities related to drones (equipping drones with a weapon, monitoring a large area for nefarious purposes, transport drugs, etc) is not well studied. Therefore, the goal of this research is to enhance the current UAS forensic investigation procedures and identify the behavioral characteristics of UAS threat actors. The behavioral examination of UAV threat actors will provide an extra layer to the current UAS forensic investigation process. Additionally, there are many attempts to prevent and control malicious drone operations. Some countries adopted detection technologies, whereas others updated their regulations for legal drone use. None of the implemented techniques have reached a high accuracy rate of success. The psychological element of drone deviants is missing from the drone ecosystem and incident response plan. As a result, profiling personality traits of drone deviant behavior might provide a valuable addition to both the UAV ecosystem and investigative techniques.

Furthermore, this study focuses on forensic intelligence attributes (i.e., information + evaluation = intelligence) United Nations [5]. Intelligence aids in enhancing the crime scene investigation process and/or forensic intelligence analysis techniques (e.g., active and passive intelligence). There are several known and unknown expectations when responding to a crime scene that involves a UAS incident. Also, from drone detection to mitigation, the technical capabilities are not efficient, and the data flow mechanism during drone operation poses more challenges to the UAV forensic investigation process (e.g., encrypted communication and customized software features).

The technical domain suffers from several challenges, and the increased number of drone incidents creates technical deficiencies in the fields of digital forensics and cybersecurity—for instance, the anonymity and obfuscation techniques (e.g., custom data link and low remote control signals) that enable deviant activities related to drones to utilize these flying devices in their actions. Another example could be the anti-forensic techniques. These techniques are the practice of tampering or removing digital evidence with a high success rate, which challenges digital forensics practitioners. Drone incidents are dramatically increasing, and

antiforensic techniques (e.g., data tampering) are considered as one of the crucial elements when developing and classifying an intelligence-led taxonomy.

Challenges related to UAV forensic include but are not limited to inference to GPS data, flight logs, sensor data, ownership data, network logs, and cloud data. Drones operate on multiple systems, storage devices, and components; thus, data flow is processed and stored in different places depending on the model of the drone. Furthermore, the encryption mechanism used to secure data transmission is a security and privacy issue that might leave the door open for man-in-the-middle attacks. In general, data storage is considered one of the most challenging aspects of drone forensics [6]–[8]. Furthermore, custom-built UASs have not been investigated by researchers yet, and its associated challenges have not been discussed. Therefore, this study also focuses on forensic challenges with respect to customized UAS. To this end, we incorporate the current UAV forensic investigation techniques on COTS and home-built UAVS to point out the technical challenges and enhance the feature selection process when developing the taxonomy. The behavioral dimension will play an important role in identifying and understanding UAS threat actors and make a significant contribution to the UAS forensic investigation process. The current UAV forensic and counter measures are not sufficient to some UAS incidents [9].

The research question consists of three important dimensions— behavioral analysis, forensic intelligence (FORINT), and UAV forensic investigation to help in building a robust taxonomy that incorporates .

- **Research Question**: How can evaluating the behavioral characteristics of UAS deviant and illegal activities, self-reported techniques, and forensically sound digital evidence supplement the proposed UAS Forensic Intelligence-Led taxonomy?

There are several aspects that aid in generating a comprehensive taxonomy. The approach concentrates on some behavioral assumptions, reviews the current UAV forensic investigation techniques, and proposes a forensic intelligence model that includes reactive and proactive techniques based on the evaluation of self-reported information by UAS threat actors. The author considers the following hypotheses to examine the behavioral patterns of the five UAS threat actors. This could aid in proposing a generic UAS forensic investigation taxonomy that

adopts forensic data from multiple sources such as behavioral analyses, forensic investigation, and forensic intelligence. These hypotheses are as follows:

- H1: Behavioral patterns significantly predict the tendency for UAS deviant and illegal activities at a significant level of 0.05.
- H2: Self-reported techniques significantly improve the proactive and reactive intelligence modeling techniques.
- H3: Forensically-sound UAV digital evidence significantly increases the reliability of the proposed UAS Forensic Intelligence-Led taxonomy.

1.3 Assumptions

The assumptions for this research include:

- Psychology plays a major role in digital forensics investigations.
- The evaluation of the self-report data will improve the proposed U-FIT taxonomy.
- The current drone incident response procedures and counter measures are not enough to cope with different types of incidents.
- UAV antiforensic techniques pose challenges.
- An interdisciplinary approach is essential to complex digital crimes.

1.4 Limitations

The limitations for this study include:

- Some participants may decline to respond to identifiable questions, which results in reducing our sample size.
- Selection and confirmation biases may exist.
- The validity of the responses was based on answering the validation question.

- The proposed UAV digital evidence metrics do not cover legal and expert witness perspectives.
- Admissibility of digital evidence can not be measured with the proposed UAV digital evidence metrics.
- There might be other unknown UAS threat actors who were not part of this study.

1.5 Delimitations

The delimitations for this study include:

- No specific geographic regions covered in the study.
- The study will not interview drone forensic practitioners.
- The proposed U-FIT taxonomy does not include the evaluation of counter- UAS systems.

1.6 Summary

This chapter gives an overview of UAV technology and a three-dimensional perspective including UAV forensic investigation, behavioral analysis, and forensic intelligence. Also, this section presented the background study, problem statement and significance, and the research questions. The goal is to support the intelligence forensic investigation of UAS incidents through a 3-D UAS forensic intelligence-led taxonomy. Moreover, this section introduces the reader to the assumptions, limitations, and delimitation of the study. The next chapter reviews previous works related to areas such as UAV cyber threats, UAV forensics investigative frameworks, and personality traits in cybercrimes.

2. LITERATURE REVIEW

An unmanned aerial vehicle is a flying device that operates via several communication protocols and controlling devices. It is a device that has certain technology specifications and capabilities to fly in the air for recreational, martial, and commercial purposes. Recently, there has been a dramatic increase in the number of COTS drones, and the future market of drone technology is growing. These flying devices have different types, terminologies, and categories. Likewise, there appear to be several terms when referring to a flying object. These terminologies pertain to different aviation agencies. unmanned aerial vehicle (UAV), remotely piloted aircraft (RPA), and drones are widely used as common terms for flying devices. Nevertheless, unmanned aerial systems (UAS) refer to all equipment related to operating a drone (i.e., flight controller, drone body, GPS module, sensors, Gimbal, etc). In addition, drones are categorized based on their rotors, capability, and purpose of user. UAVs are classified by their size, flight distance, and endurance. For instance, size classification is comprised of micro, mini, medium, and large UAVs. The Federal Aviation Administration (FAA) has classified small UASs as weighing less than 55 pounds with a maximum speed of 100 mph and 400 feet altitude, which requires a part 107 certificate unless the operated drone weighs less than 0.55 lb (FAA, 2016). Alternatively, the Department of Defense (DoD) has classified UAVs into several categories according to weights, operating altitude, radius, and endurance (see Table 2.1). Moreover, a classification matrix has been proposed by NASA that includes three categories with three different air speeds less than or equal to 70 knots (kt) (model or sUAS), less than or equal to 200 kt (sUAS), and more than 200 kt (UAS) [10].

Table 2.1.
US Department of Defense Classification of UAVs

Weight (kg)	**Normal Operating Altitude (ft)**	**Radius (km)**	**Typical Endurance (hr)**
less than 2	less than 400	5	less than 1
between 2 to 25	less than 3000	25	between 2 to 8
between 25 to 150	less than 5000	50	between 4 to 12
between 150 to 600	less than 10000	200 to 500	between 8 to 14
more than 600	less than 18000	1000	more than 20
more than 600	more than 18000	5000	less than 24

UAVs have multiple components such as sensors, actuators, software, communication protocols, power supply, flight control loops, and flight controls. These are important pieces of hardware and software to operate the flying device.

Remote sensing technologies have been deployed in UAVs to enhance their operation and performance. Sensors that are mostly found in all drones include gyroscopes, barometers, accelerometers, global positioning systems (GPS), magnetometers, rangefinders, inertial measurement units (IMUs), and obstacle avoidance. Overall, sensors and actuators are essential components in drone development and operation. An example of this is the pre-programmed flight path (i.e., roll, yaw, pitch) of the drone. Another example would be a systematic calculation of air pressure and avoidance of objects.

Regarding communication protocols, UAVs operate on several data links depending on the purpose and application. The communication architecture is designed between the flight control or the base station control and the drone. This requires radio or WiFi communication to send and receive commands. The radio frequency works on 2.4 GHz to 5.8 GHz, while WiFi communication is based on a wireless local area network (WLAN), and both protocols are specifically for short range (i.e., less than 5 miles) operation purposes. Operating a drone at a long-range distance requires efficient communication protocols such as 4G Long-Term Evolution (LTE). UAV components might be exposed to cyber threats; therefore, it is important to enhance the security of flying devices.

The increasing number of drone incidents and deviant activities, including drone terrorism, pose a significant threat to digitization. Simultaneously, the structure and design of flying devices pose challenges to the field of digital forensics. These challenges pertain to evidence analysis when a drone incident is involved. Recently, there was a fair amount of work related to technical challenges, whereas little is known about psychological factors pertaining to drone deviant actions. This chapter reviews previous works related to three important dimensions of this study; UAV forensics, UAV security, and behavioral analysis, respectively.

This section discusses previous works pertaining to the three dimensions selected that enhance the proposed UAS taxonomy. Section 2.1 includes several topics such as the importance of behavioral analysis in the cybersecurity and forensic domains, a review of psycholog-

ical psychometrics, and Section 2.2 describes the importance of the forensic intelligence approach in the forensic science field. Finally, Section 2.3 provides a comprehensive overview of scientific works, including investigative techniques and challenges to specific types of drones.

2.1 Behavioral Analysis

The author examines the research problem by looking at the complete components of the Unmanned Aerial System (UAS), which include the behavior of UAS threat actors. There is an increase in different deviant actions pertaining to the use of UAVs (i.e., drug smuggling, drone disruptive activities, prison contraband, and drone as a hacking tool). As a result, it is crucial to study the psychological elements behind the use of drones to commit a crime, which enables investigators to profile multiple UAS threat actors effectively.Researchers have shown a scientific correlation between personality traits and other criminal behaviors, and the big five personality traits are commonly used in profiling cybercriminals [11]. With the advancement of technology, studying the human factor (i.e., personality behavior) is not an old-fashioned research methodology. Technology has enabled traditional criminals to practice their tactical deviant behaviors in a semi or even fully autonomous mode. When the new technology is developed, criminals take advantage of exploitable vulnerabilities of that technology to initiate their drone deviant actions. For instance, drones can be autonomously operated, posing challenges to the digital forensic field (e.g., recovery of waypoint traceroutes, and identification of drone operators). In this research, the concentration will be on the psychological factors related to drone-flying deviant activities combined with the technical investigative components. The aim is to examine the personality and behavioral differences between drone-flying deviant activities, normal drone users, and non-drone users, which would help in enhancing the drone forensic investigation model. This enhancement will look at drone forensic investigation models (i.e., technical challenges and frameworks), and behavior profiling stimuli generated in this study (i.e., individual differences among drone-flying deviant activities, normal drone users, and non-drone users). The assumed association between the behavior of drone- flying deviants and personality traits would aid in developing

a comprehensive framework specifically for drone forensic investigations. Accordingly, this research examines the association between the Five-Factor model and psychopathic behaviors among drone-flying deviants who committed a previous felony using flying devices, which would be achieved by statistically analyzing the mean differences in the sample, and the correlation of the FFM and Anti-Social Behavior among respondents.

2.1.1 The Big Five and Antisocial Personality Traits

People have different levels of personality characteristics based upon their genetic. Various researchers have conducted studies to identify different types of personality traits listed. It is believed by the majority of psychologists that there are five basic personality traits (see Figure 2.1). These traits include openness, neuroticism as well as agreeableness, extraversion and conscientiousness [12]. It is extremely significant to understand that ranges are represented by these big five personality traits. For example, the range between extreme extraversion is represented by extraversion while people with low extraversion lies towards introversion. Based upon the traits, individuals belong to different extremes or exist somewhere in between the extreme ranges. The big five personality traits along with their ranges are discussed one by one as follows:

Openness

Oshio et al., (2018) defined openness as a trait related to insight and imagination that explains that how open-minded a person is [13]. Moreover, openness is a philosophy or a concept that is categorized by an emphasis on collaboration and transparency. People possess different ranges of openness personality traits. If the people are high in openness traits then it indicates that:

- They have a high-interest range, are curious about the world, and are interested in exploring new things.
- Such people are considered to be highly adventurous as well as creative that enjoy new experiences

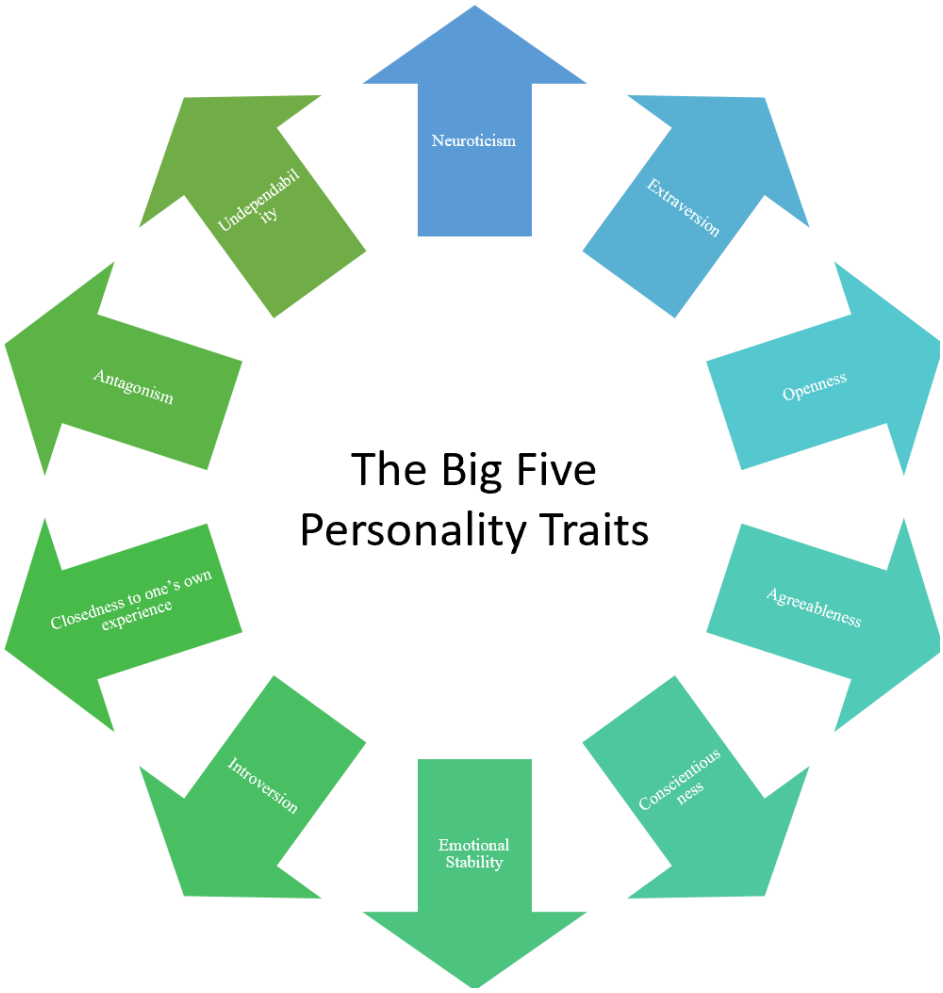


Figure 2.1. The Big Five Personality Traits

- Such people also accept challenges easily and take interest in exploring concepts that are abstract in nature The people who possess low openness personality traits are:
- Traditional and do not like the change
- The new things and experiences are not liked by such people
- Such people are not creative or imaginative, dislike new ideas as well as take no interest in abstract concepts

Conscientiousness

The conscientiousness represents the trait of being hardworking or careful and such people have an urge to take responsibilities seriously [14]. Also, people can be highly conscientious or can lie towards the other extreme side. Some of the main features of these personality traits include a high level of goal orientation, good control over impulse as well as thoughtfulness.

The people with high conscientiousness are:

- Good at planning and they spend enough time on preparation.
- Completes important tasks and responsibilities on a timely basis.
- Too much concerned about the details.
- Focuses on setting the schedule and standards.

The people having low conscientiousness:

- Do not take interest in schedules, timetables and structures.
- Are not concerned about the messes and are not very much careful.
- Do not pay attention to returning things to their place or putting them back.
- Are not able to complete the assigned tasks to them.
- Delay the important responsibilities and tasks.

Extraversion

The main characteristics of extraversion include sociability, excitability as well as the huge amount of emotional expressions, assertiveness and talkativeness [13]. Also, it is important to understand that the people who possess high extraversion traits try to get the energy in social situations and are quite outgoing in nature. Such people feel very excited and energized when they are surrounded by people. People who are introverts or low in extraversion have a reserved nature and their energy in social situations is low. Such people remain silent in gathering and remain in solitude.

Agreeableness and antagonism

The personality attributes included in the agreeableness include kindness, trust as well as affection and self-sacrifice [14]. The individuals who possess high agreeableness attributes are very cooperative in nature while those with low attributes are manipulative and even competitive in nature. More detail is given as under:

People with high agreeableness attributes are:

- Cares and think about others.
- Like to help others and assist them in doing their work.
- Take interest in other people.
- Have likeness towards happiness of others.

The low pole of agreeableness is considered to be the antagonism trait. People with low agreeableness attributes or antagonistic in nature are highly aggressive as well as antisocial. Moreover, such people:

- Belittle and insults others
- Do not care about other people's feelings
- Have no interest in others and good at manipulation to get personal gain

Neuroticism and emotional stability

It was mentioned by researchers that the trait of neuroticism is characterized by moodiness, sadness as well as emotional instability [15]. Moreover, people with high traits have anxiety, mood swings as well as sadness and irritability. Such people experience a high level of stress and worry about little things. The opposite pole of neuroticism is named emotional stability which is considered to be the ability of a person to emotionally balance him/herself under stressful conditions. People that possess low neuroticism traits or are emotionally stable easily manage the stress and do not worry about things, remain relaxed, emotionally stable and rarely get feelings of depression and sadness. They rarely become angry, tense, or nervous.

Disinhibition

Disinhibition is a trait of personality that deals with the individual differences in their ability to control or self-regulate their behaviors [12]. Furthermore, the ranges start from under controlled to overcontrolled. It is extremely significant to understand that such people do not possess the ability to suppress unwanted or inappropriate behavior and they make inappropriate actions or comments. Such types of issues mostly occur due to some kind of mental health issues, injury, or usage of drugs or some medicines.

2.1.2 What is Deviant Behavior?

Different researchers and scholars have studied deviant behavior in different contexts. It was stated by [16], that deviant behavior is considered to be the behavior or action through which the formal rules or informal social values and norms are violated. Also, the person shows deviant behavior when he/she violates the law and is termed as formal deviance [17]. However, informal deviance occurs when a person violates that social norms and values. There are different reasons behind deviant behavior and different theories have proposed different causes. As per conflict theory, deviant behavior occurs because of political, material, or social inequalities present among different social groups [18]. However, the labeling theory

states that deviant behavior happens when an identity is forced upon people and they are compelled to adopt that identity [19]. This indicates that different theorists and scholars have provided different causes of deviant behavior as per their findings and perspectives.

In the view of [20], there are five types of deviant behavior and the criteria for this behavior include conformity, ritualism as well as innovation, rebellion, and retreatism. Furthermore, deviant behavior is mainly caused when one social class is exploited by another social class. It can also occur when conflicts are present between the production relations and productive forces. It was found by [21], that mainly there are three types of deviant behaviors that arise due to different reasons. Firstly, it was found that deviant behavior occurs when a person is intended to adapt to the values and norms of a standard group. Secondly, deviant behavior can occur due to loss of self-control and is caused impulsively. A person can show deviant behavior even at a time of extreme excitement. Thirdly, deviant behavior occurs compulsively because of different types of disorders including insult, alcohol abuse and drug addiction.

Hirschi's social control theory reflects on the effects of a person's bonding with his surrounding people like from family, friends, colleagues and other known acquaintances on his inclination towards unaccepted actions or behaviors. According to social control theory a man is more likely to perform criminal offences if he lacks bonding with people. It is stated by theorists that without such bonding, criminal acts are inevitable outcome [22]. Control theories are more inclined towards finding the cause of people refraining from any deviant behavior [23]. So, as per social control theory everyone can be a part of criminal offence but the chances of someone who has strong bonds with people around him are unlikely to be part of any offensive act. Attachment with people (family and friends), commitment to goals (education and career), involvement in positive activities and belief in social and ethical values of the society, are main aspects that prevent an individual from committing a criminal act.

2.1.3 Personality Traits and Cyberdeviancy

Although no previous work has been conducted on the association between the big five personality traits and drone deviant activities, several studies have psychologically analyzed the individual differences among cyber criminals. A study demonstrated the relationship between computer criminal behavior and personality disorder [24], by distinguishing individuals through measuring personality characteristics, psychopathy level, and different types of computer misbehavior such as online identity theft. Researchers have examined individual differences to produce a more coherent interpretation of such a digital crime [24]. The behavioral science studies in the digital forensic field is crucial because of the human involvement in technological use [11]. Similarly, researchers discussed the importance of studying psychological and cultural differences to improve investigative techniques [25]. Studies in [26] claimed that an individual who has been engaged in a cybercrime such as cyberstalking, cyberbullying, online fraud, and online harassment is identified to have high level of extroversion, low in agreeableness, high in negative emotions, and low in consciousness; whereas, the researchers argued that openness to experience has no effect and association with cyberattack victimization [27]. Another piece of work supported the negative association between neuroticism and tendency to commit while-collar crime; however, researchers indicated that it is linked to certain circumstances [28]. Also, researchers have illustrated a significant correlation among certain personality traits and cyberdeviancy [11]. The adoption of the big five personality traits to examine behavioral differences among cyber criminals has added more knowledge to the scientific field by empowering the investigative techniques with the unseen factors (i.e., behavioral characteristics).

Interestingly, researchers have embedded psychopathy into FFM, claiming that psychopathy comprises basic elements such as extremely high interpersonal antagonism, impulsiveness, absence of negative affectivity, anger and hostility, and interpersonal assertiveness [29]. Using this model, a profiling outcome for prototypic psychopathy was determined based on the 30 facets of the FFM rating [29], which consist of extraversion *(E)* (versus introversion), agreeableness *(A)* (versus antagonism), conscientiousness *(C)* (versus undependability), openness *(O)* (versus closedness) to one's own experience, and neuroticism *(N)* (versus

emotional stability) [30]. The prototypic psychopathy profile shows a mean value < 2.0 in all six items (anxiety, depression, vulnerability, trust, openness, and competence) *(A)*, three items *(C)* (dutifulness, self-discipline, and deliberation), one item *(N)* (self-conscience), and one item *(E)* (warmth) and mean > 4.0 was characterized as high in impulsiveness *(N)* and excitement–seeking behavior *(E)* [29].

The Elemental Psychopathy Assessment (EPA) tool comprising 18-items under three domains (i.e., antagonism, disinhibition, and emotional stability) was developed to measure psychopathy from a personality model perspective by Widiger et al., (nd). The EPA has been validated and is comparable to other psychopathy measures (e.g., Psychopathy Checklist–Revised (PCL-R) [31]–[33] and Self–Report Psychopathy (SRP) [34] to measure crime and criminal tendencies. Under the disinhibition domain that consists of various subscales (i.e., anger, opposition, rashness, thrill-seeking, and urgency), the inability for individuals to follow social rules is measured. Factors that influence online disinhibition include anonymity, invisibility, asynchronous communication, and apathy deficits [35]. The emotional stability domain, which has a strong correlation with the fearless dominance factor of the Psychopathic Personality Inventory (PPI) is inversely related to the social deviance associated with psychopathy LSRP Factor 2 (F2), and with small correlation with other psychopathy measures [36]. Under the antagonism domain that consists of various subscales (i.e., arrogance, coldness, callousness, distrust, disobliged, impersistence, manipulative, and self-centered), hostility, which is conceptualized as an emotional state that is strongly correlated to drug–dealing behaviors, is measured [37]. The short version of the EPA is a model driven by the FFM and has demonstrated an association with external criteria of psychopathy personality disorder [36].

The psychometric inventories (i.e., FFM and EPA) were selected to measure personality traits and disordered behavior. First, previous work proved that the five-factors model provides an effective measurement of personality traits [38]. According to the studies conducted by [39], the FFM is well captured by its robustness among other personality inventories. The FFM has been effective in providing significant distinctions among personality traits [38]. An individual who has been engaged in cybercrimes such as cyberstalking, cyberbullying, online fraud, and online harassment is identified to have a high level of extroversion,

low in agreeableness, high in negative emotions, and low in consciousness [26]; whereas, the authors claimed that openness to experience has no effect and association with cyber-attack victimization [27]. Researchers supported the negative association between neuroticism and tendency to commit while-collar crime indicating that it is linked to certain circumstances [28]. Although no previous work has been conducted on the association between the big five personality traits and drone criminals, a study demonstrated the relationship between computer criminal behavior and personality disorder [24], by distinguishing individuals through measuring personal characteristics, psychopathy level, and different types of computer misbehavior such as online identity theft. Researchers in [24] have examined individual differences to produce a more coherent interpretation of such a digital crime. Including behavioral science studies in the digital forensic field is crucial because of the human involvement in technological use [11]. Similarly, authors in [24], discussed the importance of studying psychological and cultural differences [25] to improve investigative techniques. The correlation between personality traits and certain types of computer crime were examined by researchers indicating that a person with low agreeability predicts self-reported hacking, a high neurotic and low moral value person predicts online identity theft, and low internal moral values predicts virus writing [40]. Additionally, researchers have illustrated significant correlation among certain personality traits and cyberdeviancy [11]. The adoption of the big five personality traits to examine behavioral differences among cyber criminals has added more knowledge to the scientific field by empowering the investigative techniques with the unseen factor (i.e., behavioral characteristics).

2.1.4 Antisocial Behavior

An individual who engages in antisocial behavior is seldom deemed a psychopath. Differences in factors (i.e., predispositions and biological attributes) related to the cause of behavioral disorders may be attributed to the, not so often, mutually exclusive nature of being a psychopath or having an Antisocial Personality Disorder (APD). However, these behavioral personalities intersect, as noted in population statistics that show a third of people with APD exhibit psychopathy [41], suggesting an association between the two [42].

[43] argued that it is possible for psychopaths to be sociable, when the differences between APD and psychopathy were examined. Moreover, an alternative perspective is that being narcissistic and histrionic correlates more to psychopathy than to antisocial behavior [44]. The authors further stated that APD can be measured by traits such as impulsivity, falsity, irresponsibility, and lack of remorse. However, considerable academic interest exists in examining psychopathy independently of its association with criminal behavior [43], [44]. Psychopathic personality is defined by several types of antisocial behavior disorder and the extent of certain traits may lead to a tendency for psychopathic personality disorder. Therefore, psychopathy has a strong correlation with APD in relation to crime and violence [34], [45].

While there are differences between psychopathy and APD, there is also an asymmetric relationship between the two [46], such that an examination of the boundaries between psychopathic behavior and APD reveals a minor role for interpersonal and affective behavior in the diagnosis of APD. Attitudes and motivations for criminal activity relate to antisocial behavior and APD is a general risk factor, with more usefulness in a civil psychiatric setting [47]. Psychopathy (i.e., lack of guilt, remorse, and empathy) and sociopathy (i.e., lack of remorse, but guilt and empathy can be present) [48] were classified under APD, and are characterized by failure to conform to social norms, deceitfulness, impassivity, aggressiveness, and lack of remorse [49].

As mentioned previously, the association between psychopathic personality and criminal behavior [50]–[52] revealed anti-Semitic attitudes are related to APD. Self-reporting psychopathy has many limitations as respondents may be deceitful leading to inaccurate responses. Specially validated self-reported instruments (i.e., Widiger's Five Factor Model (FFM)) for evaluating psychopathic traits [53] revealed an association between low levels of agreeableness and conscientiousness with psychopathic traits, in the absence of inference to report criminal offenses [54].

2.2 Forensic Intelligence (FORINT)

The concept of Forensic Intelligent (FORINT) refers to the interaction between investigative techniques and behavioral attributes. FORINT plays an important role at the intersection of forensic investigation and detective investigation, aiming to minimize bias and increase the accuracy of logical reasoning [55]. Researchers in the 'Forensic Intelligence' book [56] claimed that the integration of forensics and intelligence empowers intelligence-led solutions in countering investigation problems. Also, the authors mentioned that forensic intelligence successfully deals with the outcomes and results of processed forensic evidence pertaining to information and intelligence. The concentration of previous works were mainly on the association of forensic intelligence applied with the forensic science field (e.g., footprints and DNA profiling). Forensic science is considered to be the application of science to civil and criminal laws [57]. Also, the main focus is on the criminal side and forensic science is applied for the investigation of crimes. Forensic science has its roots in different scientific branches and its main emphasis is on identification, recognition as well as physical evidence evaluation [58]. According to researchers in [59], forensic science provides scientific knowledge related to criminal convictions and cases through which both prosecution and defense arguments can be served. Furthermore, the main emphasis of law enforcement during the criminal investigation is put on the DNA as well as fingerprints. Researchers in [57] stated that DNA fingerprinting is a useful technique for creating a connection/link between the suspect and biological evidence during the investigation of the crime. In addition, DNA is present in hair, blood drops, skin flakes, as well as saliva through which a person can be identified. The sample of DNA collected from the crime spot is matched with that of the suspect to find the criminal. The suspect can be identified through fingerprints that are collected from the place of the crime [60].

The pattern of fingerprints is different for each person and used as a basic tool for identifying the criminal history of suspects. Researchers in [61] stated that digital forensics is useful in recovering and investigating the evidence that is found on digital devices that can store the data in a digital form. Also, digital forensics is highly related to cybercrime. It is a branch of forensic science but mainly emphasizes collecting the evidence from digital

technologies used in the crime. The evidence in digital form is identified, stored as well as analyzed, and documented for the sake of record and to present in the court.

FORINT techniques incorporate gathered data into crime analysis to help identify patterns, links, and trends that enhance intelligence decision making, which can be applied to prevent crimes [62]. This research concentrates on addressing the proposed research problem by applying the FORINT (i.e., reactive and proactive intelligence approaches) to the UAS investigation taxonomy supported by the outcome of behavioral analysis and UAV forensics. With the sophistication of cyber crimes, the author emphasizes the importance of reactive and proactive intelligence techniques. The more studies of behavioral analysis, the faster we transform digital forensics to a non-traditional approach [63]. UAV forensic investigation is one of the fields facing many challenges related to detection, monitoring, prevention, and mitigation. No previous works have examined the techniques, tactics, and procedures (TTP)s used by UAS threat actors. Another challenge brought by researchers in [64] is related to the complexity of UAS system design, software components, and data storage. Therefore, the author selects an interdisciplinary approach to tackle the problem from two angles (i.e., UAV forensic and behavioral analysis) linked with a FORINT approach. Anti-forensic techniques are not limited to drones in motion, but also when drones are at rest. Some studies indicated that there were some techniques used by threat actors to avoid flight data logging [65]. This supports the need of forensic case data to aid UAV investigators and incident responders in advancing the current techniques. This research discusses some important intelligence techniques that aid the overall proposed UAS intelligence-led taxonomy. In addition, researchers in [66] claimed that the overall investigation techniques are not very effective in responding to some types of crime investigation due reasons such as the sophistication of cybercrimes and the increased number of cybercrimes. Also, the researchers argued that it is necessary to improve the current digital forensic investigation techniques by incorporating other resources that enable advancement in the field. To this end, the combination between behavioral pattern analysis, FORINT, and intelligence would be the enablers to the UAS forensic investigation and counter measures fields.

2.3 UAV Forensic Investigation

According to the National Institute of Standards and Technology NIST (2019), criminal drone operations are rapidly increasing, and criminals are constantly developing new approaches. Digital forensics techniques applied to UAV technology are a necessity due to the increased number of flying devices and the real-world threats posed by malicious drone activities. As discussed earlier, drones are controlled via different remote controllers, presenting challenges to the overall drone forensics process, from identification to reporting. Other challenges come from customized models operated on open-source operating systems. To account for this, the INTERPOL developed the first drone incident response framework that could aid in the investigation of such flying devices by addressing the challenges that are faced by drone forensic examiners [67]. It is crucial to classify artifacts (i.e., digital evidence) recovered from UAVs to enhance the performance of drone incident response. The Computer Forensic Reference Data Sets (CFReDS) enables active field researchers to conduct forensic investigation on flying devices to speed up the process of drone incident response. There has been a fair amount of studies [6], [8], [68] related to improving these security weaknesses, establishing new detection techniques, initiating policies and regulations, and addressing digital forensic challenges [6], [8], [68].

Studies have demonstrated several technical approaches in the field of drone forensic [69] considering several approaches that could aid investigators. Furthermore, researchers have investigated the top five issues impacting the digital forensics field, including education and training, technology, encryption, data acquisition, and tools [70]. The discussed top five issues are still valid until today because of the advancement of technology. For instance, [8], challenged the encryption mechanism used to cipher flight logs as they contain valuable evidence when it comes to drone forensic. However, these studies only deal with technical challenges such as data recovery, and possible anti-forensic techniques; therefore, understanding the behavioral aspect of drone criminality is crucial to improve the existing body of knowledge further.

Some of the early work in the area of drone forensics has illustrated Drone Open Source Parser's (DROP) forensic parsing technique as a tool specifically dedicated to the forensic

analysis of the DJI Phantom III [8]. The methodology demonstrated by the authors examined the decryption of digital evidence that is essential to drone investigation. Another study by [71] discussed the correlation between digital evidence found in drones and mobile devices. The authors of these studies claim that a high rate of drone incidents are due to the increased usage of flying devices. In later studies, researchers conducted a comparative analysis of three devices: the drone, mobile device, and internal memory of the drone. Interestingly enough, this analysis showed that the drone body held no valuable evidence. On the contrary, a separate study examined a drone's chip, internal memory, and controller, and found the correlation of these three components held a strong significance in drone forensic investigation [6].

Researchers in [68] recognized the pivotal artifacts in drone forensic investigation based on the classification of drones, fingerprints, volatile data, and the utilization of the live acquisition technique. The authors in [7] conducted a drone forensic investigation on DJI Phantom 3, and explained the importance of particular automation techniques to parse drone data. However, parsing and recovering drone data does pose challenges due to software development and varied system architectures. In an interesting article [72] an experimentation of incorporating open-source tools in drone forensics was conducted on the Parrot AR, Drone 2.0, and DJI Phantom 3. The experiment led to the discovery of recovered artifacts from both drones and mobile devices during operation. The authors illustrated a 46% reduction of drone data tempering during real-life scenario operations. The results indicated that different technologies, such as block-chain and self-adaptive forensics, enhance drone data security through time intervals, distance, and boundary techniques. Contrastingly, the security of drone live-stream data runs the risk of being tampered with.

Due to the rapidly increasing adoption of drones, researchers discussed potential security threats including GPS spoofing, maldrone, and un-encrypted data transmission [73]. These flying devices are being utilized for numerous critical operations, such as crime scene mapping, policing, and medical transportation. Data tempering is an additional example that could potentially impact the usage of drones. Flying devices have been spread heavily following the COVID-19 pandemic to collect data, identify infections amongst individuals, and to support lockdown control [74]. Publicly available firmware eases the process by distributing

a modified version of the firmware that is infected by a malware—something that has the ability to compromise the drone's entire system, not only its transmitted data. Restrictions like a no fly zone (NDZ) possessed the ability to be modified by overriding the software functionality. In [75]–[77] issues related to information disclosure through the initiation of an eavesdropping attack; whereas, researchers in [78] presented a denial of service (DoS) attack on an AR drone 2.0 that demonstrates the malfunctioning of live transmitted data.

Regarding UAV cyber threats, there are several attack vectors that could compromise flying objects. These threats are beyond the traditional cyber threats as UAVs operate on different communication protocols and transmit more data. Any standard flying device transmits data at rest, in motion, or in use. All these three types of generated data play a major role in security measures against UAVs. Therefore, minimizing the risk and protecting confidentiality, availability, integrity, and authenticity is a necessary, especially to certain UAV applications (e.g., military, industrial, emergency response, etc). Most UAV applications are not following a proper secure measure that enhances the safety and security operation of flying objects. Some researchers discussed solutions related to the active operational monitoring of UAVs, developing an Intrusion Detection System that actively alerts abnormal activities (e.g., denial of service (DoS), GPS jamming, and eavesdropping)[79]–[83].

In Figure 2.2, we demonstrate several possible attack vectors pertaining to data tampering, data exfliration, and take control over the drone.

Flying devices operate and function using different communication protocols through preprogrammed sensors and manual tasks. From a digital forensics perspective, the drone vital signs in-flight are invaluable to any investigation due to artifacts being typically stored in the drone's chip. Conducting a forensic analysis on a drone's chip will provide a greater understanding and assurance of the incident with the help of stored system events and software-related data. In knowing this, numerous researchers have proposed a technical forensic investigation process based on such validated and verified approaches. A recent study drew the importance of `lessons learned' in the drone incident response cycle and presented a POC relating to the antiforensic challenges in drone forensics [69]. Supplementing the previous research findings, work presented by [6] proposed a technical drone forensic

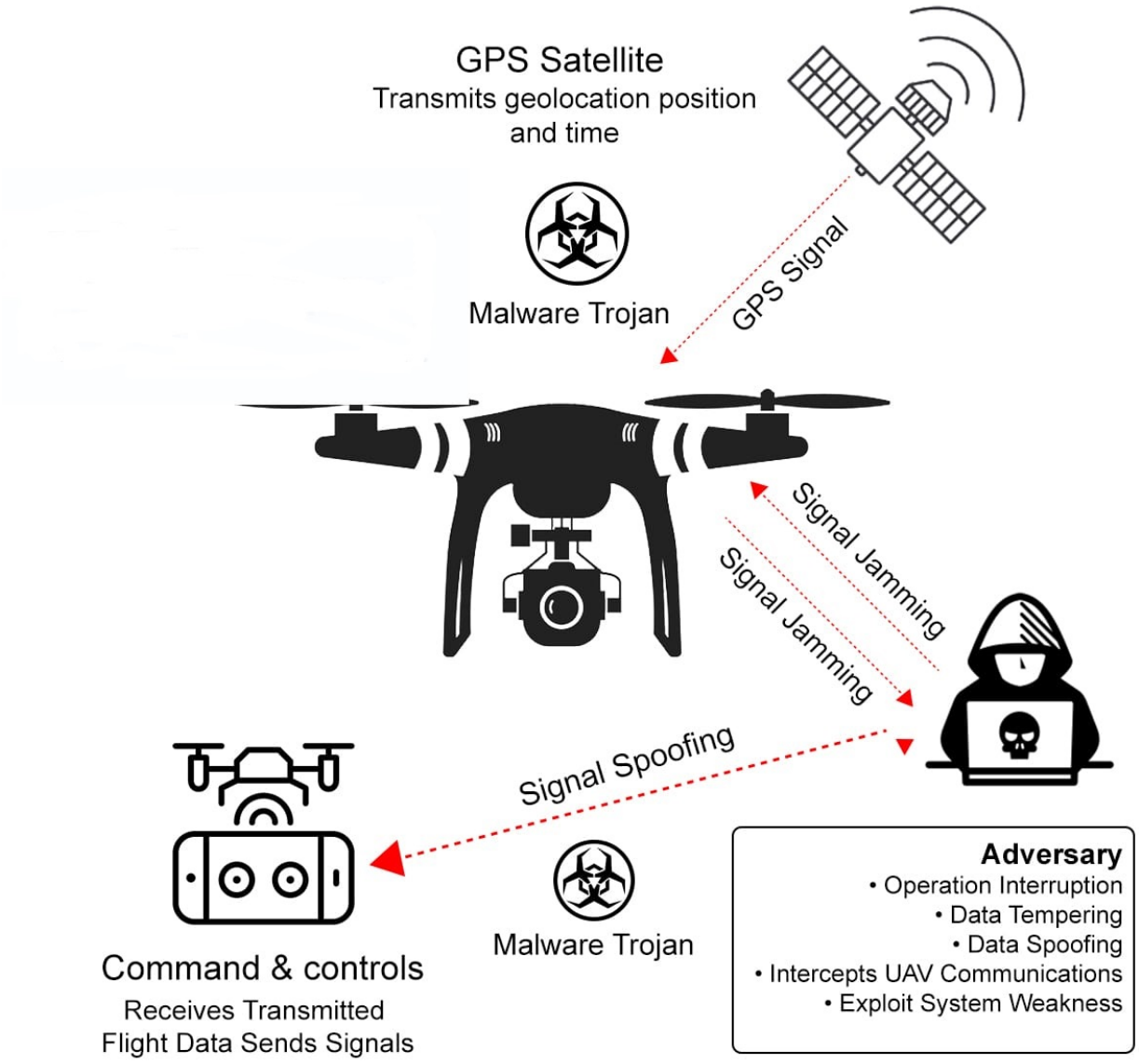


Figure 2.2. UAS Attack Vectors

framework to aid drone forensic examination. The researchers discussed the procedures used to detect customization in drones, and explored the current available customization techniques that could be used during a drone crime incident.

Researchers have investigated issues related to drone forensics and proposed a drone forensics framework covering various components. The proposed framework by [68] consists of the following steps:

1. Preparation
2. Identification and Collection
3. Identify Class and Category
4. Measure Weight: *if more than 0.55lbs then check FAA regulation* and *if the drone weight is less than 0.55lbs move to step 5*
5. Check for customization: *if customization present then compare specification with original*, but *if not, then move to step 6*
6. Check for fingerprints
7. WiFi
8. Bluetooth
9. Geo-location
10. Memory Card
11. Inbuilt Camera: *if not, then was Gimbal present?*; *if not, move to step 12* and *if yes, move back to step 10 for Memory Card*
12. Document and Report

The proposed framework by Jain et al., (2017) addressed very important aspects of drone forensics. For instance, classifying physical evidence (i.e., drone class, possible customization, and DNA evidence) at the crime scene, which is considered initial preparation and

identification of the evidence. Steps 7–11, relate to media storage devices and digital evidence linked to communication protocols (WiFi and Bluetooth). The authors did not specify the following:

- Analysis and Examination phase: the framework should include steps related to the technical investigation techniques.
- Customization should include software related techniques.
- WiFi and Bluetooth do not reveal invaluable digital evidence.

However, step 11 discusses an important phase related to commercial drone forensics. Forensic analysis of memory card and media storage has been presented by [6], where geo-locations were extracted from both videos and images captured by a drone.

Since the UAS is structured and designed based on several software components (i.e., sensors, actuators, and software applications), a framework was proposed by [84] to deal with log examination. The presented framework included a visualized figure highlighting steps to logs initiation. Therefore, the following steps provide more details about the proposed model by the authors:

1. Drone takes off
2. Logs created with values of all parameters
3. Processed flight including timestamps, flight path, power usage, three principals of aviation, geo-location, speed, IMU, distance traveled, etc.
4. Logs uploaded to a PC to refine and analyze using the proposed framework
5. Visualization using JavaFX and Google Maps API

In general, both drone frameworks presented different investigative aspects that could aid forensic investigators and law enforcement.

2.3.1 Published Drone Frameworks: 2018-2019

In 2019, a framework proposed an algorithm designed to extract log data from drones [85]. Steps included:

1. Upload log file— *success*
2. Read data—*success*
3. Detect drone—*convert from CSV to KML*
4. Visualize data on Maps

Another work proposed a forensic process framework for small-scale drones [86]. The framework included the following steps:

1. Is UAV in Mid-Air? *if yes, then move to step 2* and *if no, move to step 4*
2. Hack UAV and Controller
3. Navigate UAV to desired location
4. Confiscate UAV
5. Process UAV
6. Forensic Analysis
7. Document, Report, and Present

The proposed work concentrated on small-scale drones; however, hacking into a flying device is not a well-known methodology in the digital forensics field. As such, the proposed framework will not add much value to the drone forensic techniques. Nonetheless, the proposed work might contribute to the potential antiforensic techniques that can be performed on small-scale drones. For instance, an adversary might take control of an airborne drone to commit a crime.

The investigative drone framework presented by [87] included seven important phases:

1. Preparation: knowledge of diverse UAS systems is needed to prepare the evidence.
2. Scene Control: to maintain psychical evidence integrity.
3. Customization Detection: hardware customization might be present.
4. Data Acquisition: all data should be acquired (i.e., volatile and non-volatile including network based data).
5. Evidence Authentication: follow best digital forensics practice to avoid data loss or alteration.
6. Evidence Examination: analysis and examination of related digital artifacts.
7. Presentation: report presentation.

Moreover, authors in [7] proposed a forensic investigation process composed of 20 detailed steps related to the identification phase of traditional digital forensics; these include:

1. Identify and determine the chain of command
2. Have conventional forensic practices such as DNA analysis already been implemented?
3. Identify the role of the device in conducting the offence
4. Photographs
5. Identify the make and model
6. Open-source investigation to identify device characteristics
7. Identify capabilities (video/audio recording, carrying capacity and technique)
8. Identify potential modifications
9. Identify data storage locations
10. Identify ports
11. Extracts removable data storage mediums

12. Preserve evidence

The association between the proposed drone investigation framework and the traditional digital forensics process has been clearly illustrated. However, information related to network-based data has not been technically discussed. Therefore, acquiring network-based data is not essential at all when it comes to drone forensics. A ten-step drone technical forensic investigation process has been demonstrated by [6]. The proposed framework consists of the following steps:

1. Preparation
2. Identify Digital and Physical Evidence *if all drone components (i.e., remote control, memory cards, and drone body) are present, then move to step 4* but, *if not all drone components are present, then is the remote controller available? if yes, move to step 3*
3. Investigate available Media File Storage.
4. Investigation Media File Storage and Flight Logs.
5. Validate Digital Evidence.
6. Withdraw Fight Activity Log *if data is encrypted, move to step 7* but, *if data is not encrypted, move to step 8.*
7. Decrypt Data.
8. Visualize GPS data.
9. Interpretation of drone blackbox.
10. Report findings.

While this framework started with similar steps to some of the discussed frameworks, it focused on technical examination processes such as encrypted digital evidence, and the presence of all drone components.

2.3.2 Published Drone Frameworks: 2020

Recently, INTERPOL has developed a drone incident framework for first responders and digital forensics practitioners INTERPOL (2020). The 130 page document covered details such as categories of UAVs, components, payloads, associated evidence, possible offences using drones, process of investigation, etc. The process of drone forensic investigation is different as every incident is solved in a certain way. Furthermore, identifying the offender is a challenge which requires further investigation INTERPOL (2020). To this end, the proposed process of investigation mostly deals with postincident investigation to identify the suspect and answers the three **W** questions (Why, where, and When).

Researchers [88] discussed eight technical requirements of admissible digital evidence including—digital forensic models, digital forensic tools, chain of custody, digital forensic analysts and experts, digital forensic laboratories, technical integrity verification, digital forensic expert witnesses, and digital forensic reports, respectively. When applying these technical requirements to the UAV forensic investigation domain, there should not be any differences because the impact that emerging technologies (e.g., drones) have on the admissibility is related to the technical integrity validation. How reliable is that digital evidence? [88] discussed the requirements of admissible digital evidence in legal proceedings. The legal requirements consists of legal authorization, digital evidence relevance, digital evidence authenticity, digital evidence integrity, and digital evidence reliability.

In addition, researchers in [88] proposed the harmonized model for digital evidence admissibility assessment (HM-DEAA) that encapsulates some necessary technical and legal requirements of admissible digital evidence. This study adopts the HM-DEAA and determine if technical requirements of UAV forensics impact the legal requirements of admissible digital evidence. Researchers proposed three phases including— (1) digital evidence assessment, (2) digital evidence consideration, and (3) digital evidence determination. The classification of these requirements were based on the tendency and significant impact on the admissibility of digital evidence. To address the proposed hypothesis for the UAV forensic investigation dimension, the author selects only the core requirements associated with phase 2 (i.e., digital evidence consideration) as it has the most influential impact on evidence admissibility.

There are certain criteria for digital forensic evidence to be forensically sound. Before jumping to the definition of what is forensic-soundness, it is important to understand the meaning of forensic computing. Forensic computing was defined by [89] as: "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." On the other side, researchers have a different definition of the forensic computing concept. Some look at it as processes for digital crime investigation purposes [90], while [91] claim that digital forensic is completely different that other types of digital investigations. Evidentiary requirements and standards are the necessary components of any type of digital forensics, The computer forensic field has dramatically expanded and became broader in concept. This is correlated with the number of connected devices and advancement of technology. Therefore, what is forensically sound evidence? Researchers in [92] defined it as "the application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law.". An evaluation of digital evidence has been proposed in [92], where criterion 1 insures that the evidence has been altered during the digital forensic processes, criterion 2 potential errors and reliability of the recovered evidence, criterion 3 deals with reproducibility of the examination and analysis, and criterion 4 knowledge and experience of the digital forensic analyst. In this study, the author relies on few standards to propose a UAV digital evidence evaluation metric that aids in examining the soundness of digital evidence recovered from UAVs.

In summary, this Section 2.3 demonstrates the current challenges of UAV forensic investigation and provides an insight into the available UAV investigation frameworks. Some of these frameworks mainly concentrate on crime scene processing; while others concentrate on the technical investigation process. To add to these frameworks, the author aims to incorporate several disciplines (e.g., behavioral analysis and forensic intelligence) to supplement the proposed UAS intelligence-led taxonomy.

2.4 Summary

This chapter discusses an overview of UAS technology and a three-dimensional perspective—including behavioral analysis, FORINT, and UAV forensic investigation. In addition, this chapter presents the importance of incorporating several disciplines as a source of intelligence. The next section will demonstrate the research approach for each domain, behavioral analysis, FORINT, and UAV forensic investigation, respectively.

3. METHODOLOGY

The selected research methodology in this study aims to provide a holistic approach for UAS forensic investigations by incorporating intelligence techniques. This includes practical UAV forensics, personality patterns of UAS deviants, and forensic intelligence. The UAV forensic domain concentrates on technical elements and challenges. The technical investigation domain deals with the source and type of digital evidence, the UAV forensic models, and the forensic soundness of digital evidence based on the *Daubert* standards categorized by (1) the International Organization for Standardization in the field of information technology (ISO/IEC 27037), (2): the Scientific Working Group on Digital Evidence (SWGDE) documents, and (3) the four principles of digital evidence (i.e., authenticity, completeness, reliability, and believability). To this end, a three-dimensional approach is necessary to develop an extensive study that results in a novel UAS Forensic Intelligence-Led Taxonomy. Combining only two disciplines (i.e., UAV forensic investigation and behavioral pattern analysis) assists in developing an ontology that describes the relationship between their entities; however, the objective of this study is to develop a taxonomy that incorporates all three domains to empirically classify these entities; see Figure 3.1.

An Ontology is philosophically defined as a conceptual classification of individuals, classes, attributes, relations, and events [93], [94]; conversely, a taxonomy is an empirical classification technique that is based on similarities by maximizing the between-group variance and minimizing the within-group variance [95]. This research combines three disciplines together to generate a holistic taxonomy to build an intelligence-led taxonomy specific for UAV forensics. This chapter discusses three aspects of UAV forensics. The first aspect is the current UAV forensics components. The second aspect demonstrates the design of the conducted behavioral study on UAS deviants. The last aspect incorporates the forensic intelligence processes into the proposed taxonomy to link and deliver intelligence to the UAV forensics field.

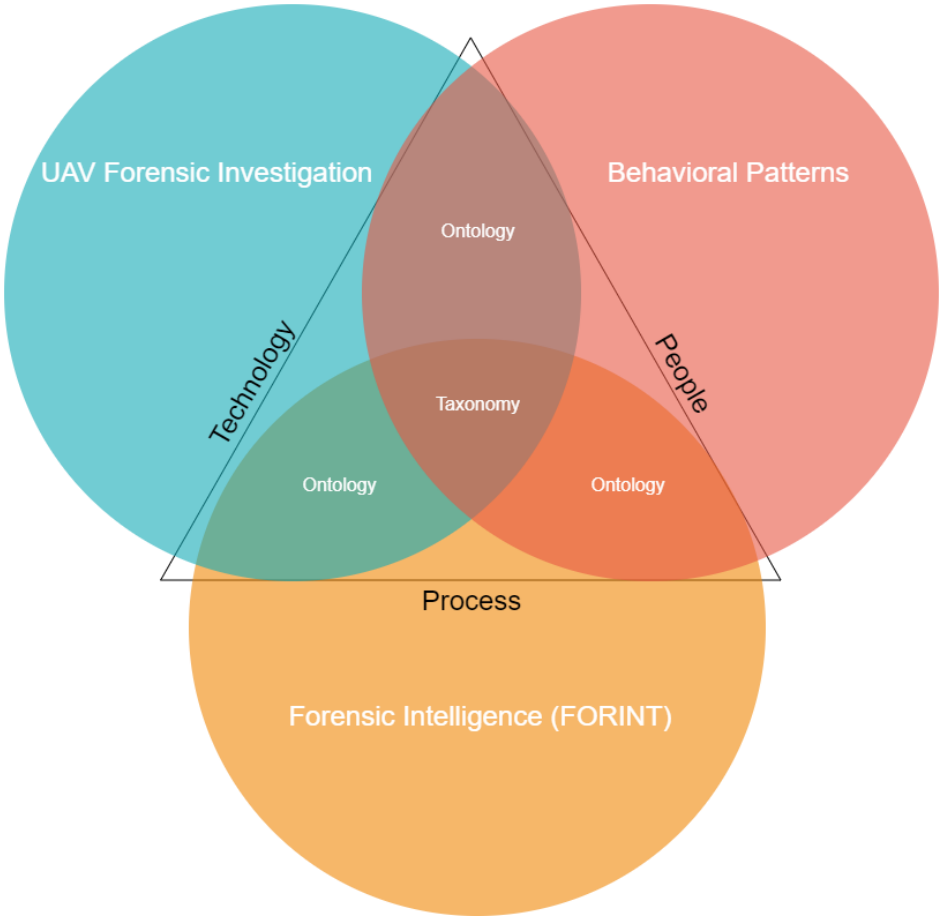


Figure 3.1. Venn diagram Showing the relationship between the three dimensions

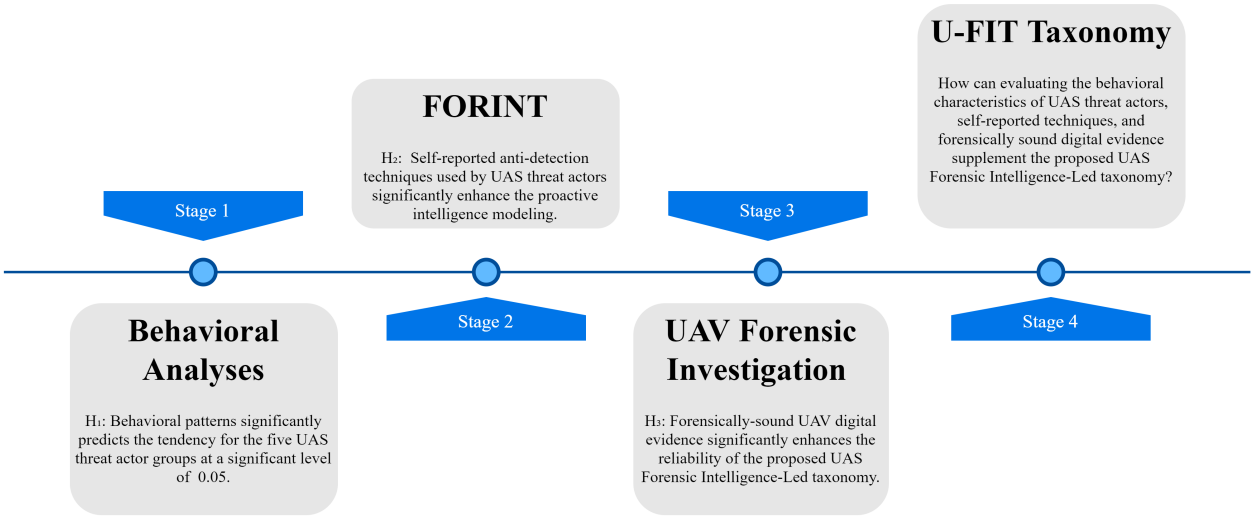


Figure 3.2. Research Methodology

The research methodology illustrated in Figure 3.2 investigates three important dimensions tied to the proposed research question. Each dimension addresses one hypothesis that follows a specific research approach aiming to enhance the proposed U-FIT. This study is divided into four stages, as follows:

- *Stage one:* This stage of the research applies behavioral analyses to examine the personality patterns of UAS deviance and distinguish them. The proposed hypothesis for this dimension is that *H1*: behavioral patterns significantly predict the tendencies for the UAS deviance at a significant level of 0.05. To test this hypothesis, the author conducted a survey that measures the behavior of UAS deviance in a self-reported format (see Section 3.1).

- *Stage two:* The second stage is to evaluate the collected data from stage 1 to propose a threat model based on the self-reported anti-detection techniques to enhance the proactive intelligence technique of UAS investigation. The hypothesis here is *H2*: self-reported anti-detection techniques used by UAS deviants significantly improve the proactive intelligence modeling techniques.

- *Stage three:* For stage three, the approach is different because the hypothesis requires the author to conduct an examination that measures the forensic soundness of UAV digital evidence. The selected approach is based on the proposed UAV digital evidence metric (see Section 3.3).

- *Stage four:* The final stage is to incorporate all outcomes from stages 1,2, and 3 and enhance the proposed taxonomy. This stage should address and discuss how evaluating the behavioral characteristics of UAS deviants, self-reported techniques, and forensic soundness of UAV digital evidence can supplement the proposed UAS forensic intelligence-led taxonomy.

3.1 Behavioral Study of UAV Deviants Actions

The selected methodology for this domain was based on a self-reported anonymous survey that includes a reliable psychometric to measure the behavioral characteristics of partic-

ipants. The author piloted a study to prepare and improve the final data collection process aiming to minimize some of the delimitations.The pilot study included a survey questionnaire and anonymously collected responses from 643 individuals in a self-reported format via Amazon MTurk (i.e., a crowd-sourcing service). This study was approved by the Institutional Review Board (IRB) of Purdue University, and informed consent was obtained from the participants to maintain the anonymity and authenticity of the collected data and the purpose of the study. Participants received $0.50 for their efforts via an anonymous payment system set up through Mechanical Turk. To validate responses, a validation question was randomly placed to ensure respondents' attention and avoid spambots. Of the 643 participants, 119 were excluded from completing the survey as they failed to pass the validation question, 18 were removed as they randomly failed to answer certain questions, and 15 participants who declined to self-report whether they were drone or non-drone users were excluded from the study. Finally, n=506 respondents were included in the dataset for annotation. The study contained 18 items of the short EPA version and the FFM with 30 items related to Big Five Personality Traits (BFPT).

3.1.1 Pilot Study

The pilot study investigated the observed variables to examine the feasibility of the collected data and the validity of selected approach. The questionnaire contained 48 questions and data were collected from 506 respondents after data manipulation. According to [96], the recommended sample size of a pilot study is (N = 100) when studying fewer than five constructs. On the other side, researchers in [97] suggested a sample size of (N = 150) when considering 40 item statements. In addition, the authors in [98] claimed that the sample size of a pilot test should be at least five times the number of indicators. In this pilot study, the questions were divided into 11 constructs. As a result, this pilot study examines only 5 constructs with a total of 30 items. The big five personality instrument has five scales. The total sample is size *(N* = 506) after data cleaning and by following the recommended methodology [99]; thus, there are 30 indicators (30 × 5 = 150), which means that 150 is the minimum required sample size for this pilot study. The design of the survey included

demographic items such as age, gender, ethnicity, level of education, and employment status. Furthermore, the survey contained some self-report questions related to illicit use of drones (i.e., operating an aircraft non-compliant with safety laws) and an item related to drone weaponization (e.g., have you ever equipped a drone with weapons?). These were forced response items as participants have the option to decline to respond to these questions. Individuals who self-reported drone incidents or illegal use will move to another item that further identifies the type of drone felony.

Past studies have shown that agreeableness and conscientiousness are important scales of the FFM because of their strong relationship to various antisocial behaviors (e.g., reactive and proactive aggression [100]; and relation regression [101]) [102]. In general, studies have shown that 75% of individuals who committed at least one crime exhibit antisocial personality traits [103], and it is evident that antisocial behavior increases the risk for violence [104].

The design of the pilot study variables is illustrated in Table 3.1, which include demographic items such as age, gender, ethnicity, qualification, and employment status. There are two psychological instruments, and several independent variables.

Conducting a pilot test could aid in enhancing the feasibility of the proposed study. The evaluation of the collected data indicates that there is no need to modify any of the study protocols because of the value that the data provides in categorizing UAS deviants actions. The pretest measured drone-flying deviants, normal drone users, and non-drone users.

The direction of the pilot study was to distinguish between drone-flying criminals and non-drone criminals. After a few considerations, the full-scale study will focus on deviant behaviros of drone users rather than criminals because of the criminal federal law related to drone use is not ready to be studied among some countries.

3.1.2 Full-Scale Study

The ontology illustrated in Figure 3.3 consists of three entities within the behavioral domain. For instance, UAS deviants actions included in the study, psychological instruments,

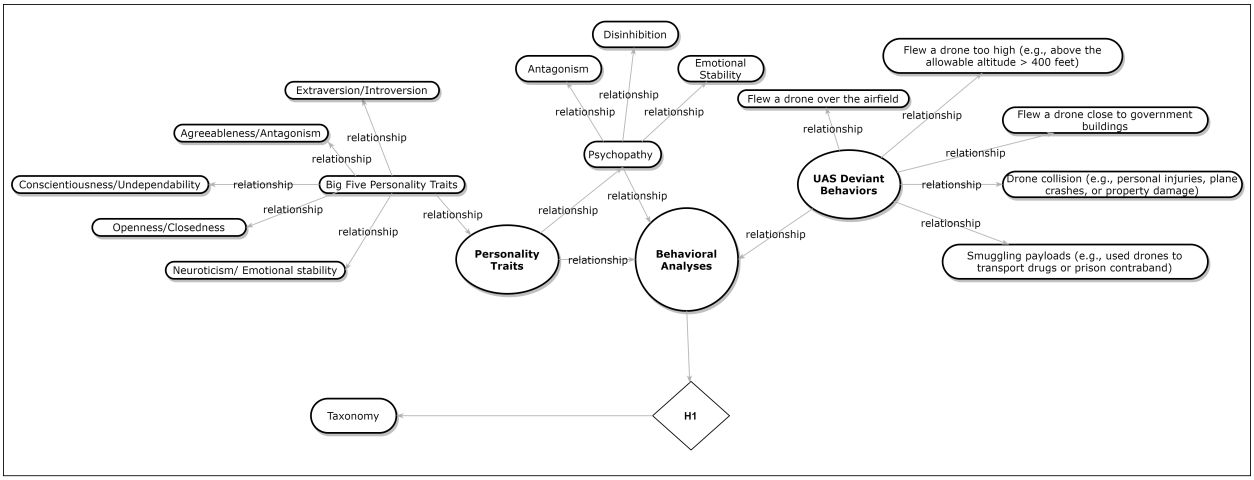


Figure 3.3. Behavioral Analyses Ontology

Table 3.1.
Study Variables

Category	**Variables**
Demographic	Gender - Age - Ethnicity - Degree - Drone vs Non-drone operators
UAV Background and Skills	FAA certificate - Type of use - Purpose of use - No-Fly-Zone
Self-reported UAV crimes	Drone drug smugglers - Drone deviant activities
Psychological Instruments	FFM - EPA

and additional entities pertaining to the examination of the behavioral characteristics of self-reported UAS deviants actions.

The outcome variables in the full-scale study are shown in Table 3.1.

This classifies UAS deviant actions. For participants who self-identify themselves as drone or non-drone users, they will be redirected to an item that identifies if they have been involved in any drone deviant actions. This will prevent misclassification when conducting the behavioral analysis that aims to distinguish between these individuals.

Hypotheses

The hypotheses for this study are the following:

- *H1:* Behavioral patterns significantly predict the tendency for UAS deviance actions at a significant level of 0.05.

- *H2:* Self-reported anti-detection techniques used by UAS deviance significantly improve the proactive intelligence modeling techniques.
- *H3:* Forensically-sound UAV digital evidence significantly increases the reliability of the proposed UAS Forensic Intelligence-Led Taxonomy.

3.2 FORINT

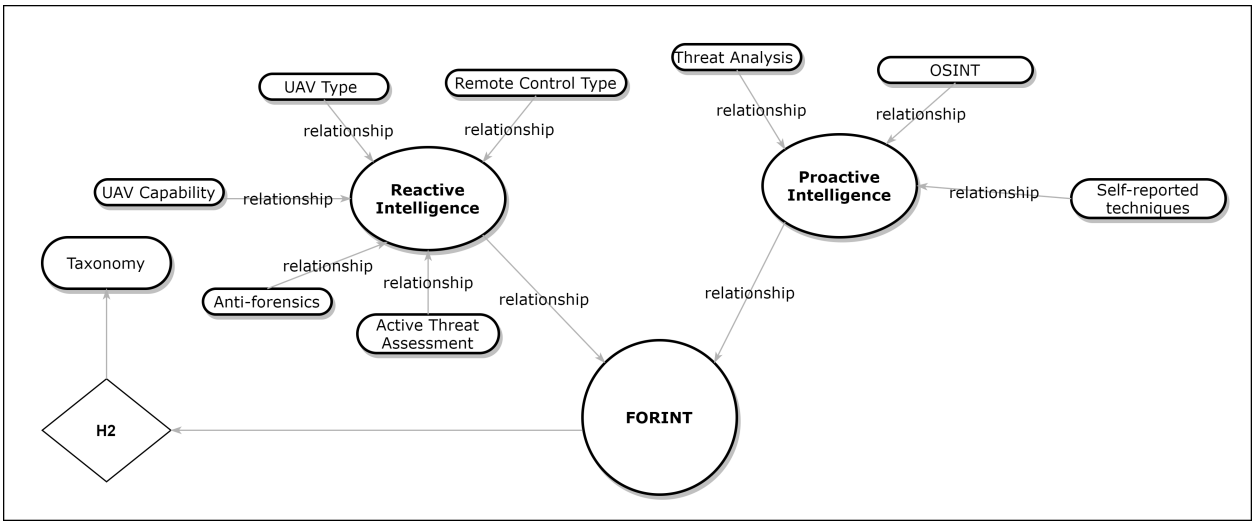


Figure 3.4. FORINT Ontology

FORINT is the second domain that links the other dimensions by providing forensic data intelligence that aids in supporting the UAV forensic investigative techniques (see Figure 3.4). This domain concentrates on UAS threat intelligence analysis. There are two types of intelligence that perfectly support the UAS investigation problem. The reactive intelligence approach deals with collecting data relevant to the counter-UAV measures and crime scene investigation. This means that data collected during the detection and monitoring stage should improve the active threat assessment to identify tactics, techniques, and procedures (TTPs). Alternatively, data pertaining to the UAV and remote control type can be collected at the crime scene investigation. Anti-forensic techniques related to UAVs are not very well studied; however, the author emphasizes the importance of identifying these techniques in both environments (i.e., the crime scene and UAV detection). There are several possible

techniques: flying a UAV on a custom data link or low remote control signal could avoid the radio frequency detection system. Another example relevant to the identification of anti-forensic techniques in a crime scene environment could be wrapping the GPS antenna with foil to bypass flight logging and other system features (e.g., no fly zone). A collection of forensic case data would contribute not only to the UAV forensic process, but also to threat assessment and predictive models. Proactive and reactive intelligence approaches will enhance several UAV investigation techniques. The author expects that intelligence analysis with regard to UAV forensic investigation and counter measures would add more value to the overall investigation framework. Figure 3.5 illustrates a hierarchical model of both approaches. Reactive approach begins from UAV detection and tracking going through multiple stages (e.g., UAV capability, antiforensic detection) to the crime scene investigation stage, where the identification of UAV and remote control is more accurate. The proactive approach consists of several important stages that should be taken into account in UAV forensic investigation—for instance, collecting data related to possible threats, UAS deviant actions, risk factors, and antiforensics identified at rest and not in-motion compared to reactive approach. Proactive intelligence includes open-source intelligence where most of the crime activities take place. For instance, the dark web is one of the interesting spots for UAS deviants to exchanges services and illegal transactions pertaining to UAVs. In general, the outcome of these approaches is to generate a reliable and accurate forensic case data that has the capability to predict and enhance the decision-making process. The UAS intelligence-led taxonomy incorporates these processes to aid in the process of UAV incident response.

The hypothesis for this section is to identify self-reported antidetection techniques used by UAS deviants to significantly enhance the reactive and proactive intelligence modeling. Collecting and evaluating self-reported information will enable the author to better understand some of the antiforensic and antidetection techniques. The evaluation of this information will also help in enhancing the the FORINT approach, illustrated in Figure 3.5. The overall outcome of this dimension is to feed the forensic case data with reactive and proactive information to evaluate the data targeting several aspects such as UAV threat hunting, counter measures, UAV incident response, adversarial risk analysis, UAV forensics—and to enhance investigative frameworks.

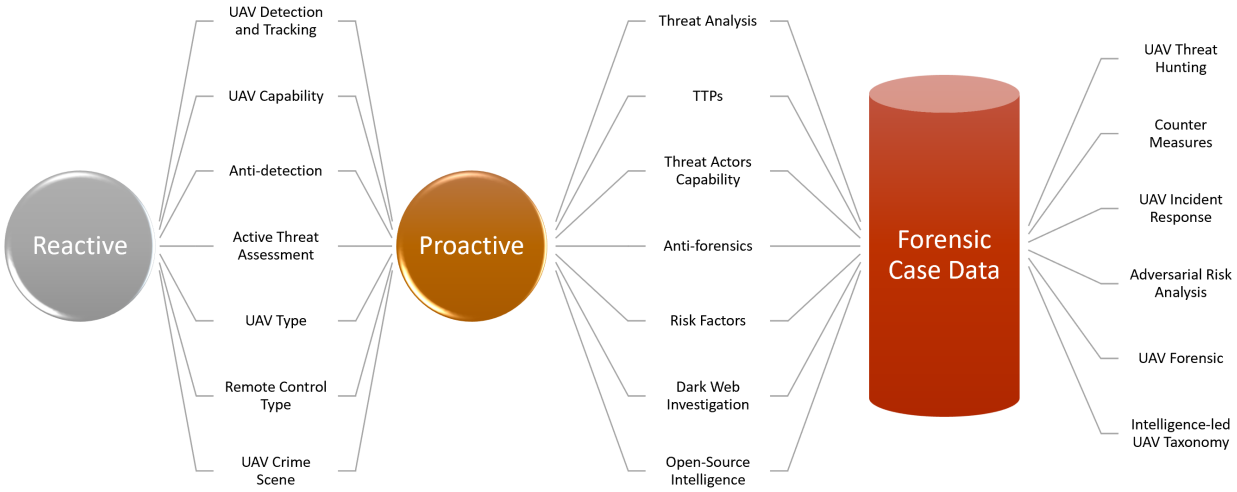


Figure 3.5. FORINT Approach towards the UAS intelligence-led taxonomy

3.3 UAV Forensics Investigation

The UAV forensic ontology illustrated in Figure 3.6 simplifies the elements involved with the technical investigation of UAVs. These elements include processes that have association with each other. The author examines multiple sources of evidence such as memory cards, cloud, chip-offs, remote control, mobile apps, and smartphones. It is important to note that each source of evidence has several categories depending on the UAV type. Moreover, there are two forensic layers in UAV investigation; the physical and digital layers. The physical layer deals with evidence found on objects at the crime scene such as DNA; whereas the digital layer deals with a broader scope of evidence acquired from multiple hardware. The third element of UAV forensic investigation is the type of evidence that needs to be preserved for further analysis. These types include media files, flight logs, Personal Identifiable Information (PII), sensor logs, software logs, and DNA. The analysis phase is performed based on the source and type of evidence. In the cyber forensics field, there are several tools that have a specific performance and capability. The UAV forensic ontology shows a fifth element that includes the currently available UAV forensic models. Frameworks proposed in [7],

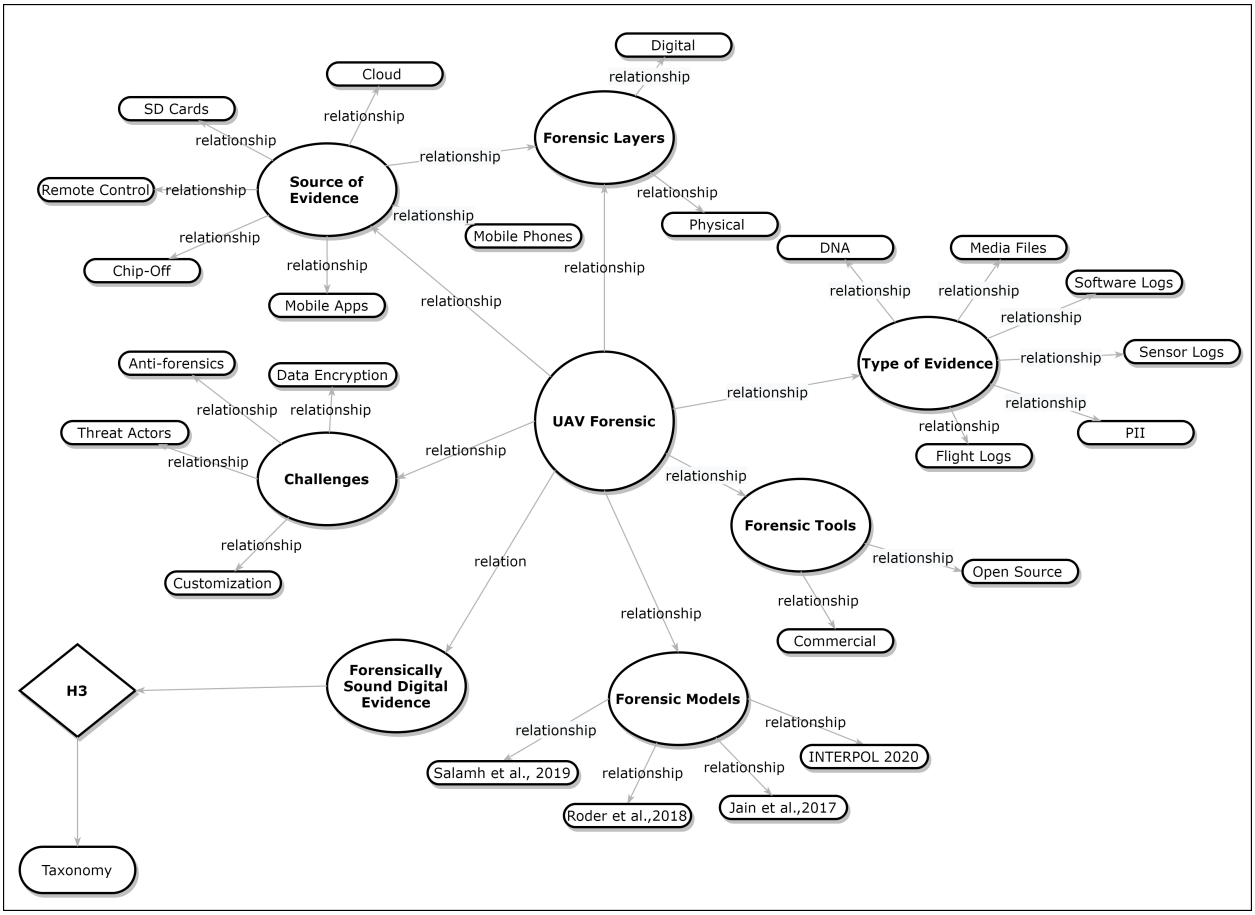


Figure 3.6. UAV Forensic Ontology

[68] demonstrate processes related to an identification and preservation of digital evidence, while the technical investigative framework proposed in [6] covers the analysis phase of UAV forensics. A good elaboration on the reporting and documenting phase has been discussed in the framework for responding to a drone incident [67]. None of the UAV frameworks has discussed the admissibility and integrity of evidence, or procedures to interpret acquired evidence in an acceptable form in courts. The UAV forensic ontology ends with an important process which determines whether the analysis is forensically sound or not. Also, there is a paucity of research work pertaining to the examination of UAS deviants. These actors have different approaches and it is necessary to study their behavioral characteristics, which the author proposes will enhance forensic data intelligence.

Finally, the author revisits digital evidence guidelines and standards to apply them on UAV digital evidence and measures weather the integrity and validity of technical prodecures might impact the legal requirements of admissible digital evidence in court. The hypothesis for this dimension is that forensically sound UAV digital evidence significantly enhances the reliability of the proposed UAS Forensic Intelligence-Led Taxonomy. The author conducted a comprehensive evaluation of UAV digital evidence. The methodology follows the *Daubert standards*. The author proposes novel evaluation criteria for digital evidence assessment illustrated in Figure 3.7.

The UAV metric consists of five *Daubert standards* and matches a technical criterion for each standards. For instance, the first standard suggests that *theory or technique has been tested*. The author classifies these standards under the *technical integrity verification*, which includes the type of digital evidence and UAV model. The second *Daubert standard* is that the *theory or technique has been subjected to peer review and publication*, therefore the author collects and evaluates current literature and open-source UAV forensic models and/or tools. For the third standard, *maintenance of standards controlling its operation*, the author selects the ISO/IEC 27037 standard pertaining to the evaluation of digital evidence. In addition, SWDGE and the four principles of digital evidence were selected to measure potential error rate. Finally, the last *Daubert standard* is that these peer-review articles are *widespread and acceptance within a relevant scientific community*. The author selects the *number of citations per article* as a measure.

To speculate on that, the proposed critical metrics for digital evidence extracted from UAVs was based on the following standards (see Figure 3.7): (1) the International Organization for Standardization in the field of Information Technology (ISO/IEC 27037), (2): the Scientific Working Group on Digital Evidence (SWGDE) documents, (3): the five principles of digital evidence,(4): the *Daubert* standards which include testing and peer review factors. These factors are applied to scientific produces in the field. The Daubert standards address if the scientific procedure has been tested, published, and subjected to peer review [105].

The proposed UAV metrics to evaluate digital evidence aids in the evaluation process and the technique demonstrated in Figure 3.8. The evaluation process begins with several variable such as X, Y, and Z. A description of each variable is given in Table 3.2.

Table 3.2.
Explanation of Each Variable in the Evaluation Process Illustrated in Figure 3.8.

Variable	Explanation	Criteria
X	variable refers to the evaluation of the ISO/IEC 27037	auditable, repeatable, reproducible, and justifiable
Y	variable refers to the evaluation of the SWDGE cretirias	evidence preservation, extraction methods, network isolation, and synchronization).
Z	variable refers to the evaluation of the four principles of digital evidence	believability, authenticity, completeness, and reliability
Total	array that calculates the total score of (X+Y+Z) for each article.	
D	array for the final decision of each article.	
sum	sum is the operation of calculating total divided by the number of articles.	
i	counter	
Average	average is to get the mean of all calculated creteria of all entered articles.	

The evaluation process illustrated in Figure 3.8 shows the calculation process for each metric and all criteria. Once the total of twelve criteria is calculated for all research articles, the average of the total score will be calculated to check evaluations above or below than the mean. In addition, a regression analysis will be conducted to measure the number of citations of research articles to predict the total score of these evaluations. Each criteria has either a value of zero or one for evaluation. For instance, if an article presents auditable techniques, then it will have a positive score. From the twelve criteria, there is only one reversed item (network isolation). This means that if an article demonstrated network isolation technique, it will be assigned with 0 and if the article did not follow network isolation procedures, it will be given 1.

3.4 An Interdisciplinary Approach

The main objective of this research is to explore techniques and procedures that blend three disciplines (UAV forensic investigation, behavioral analysis, and forensic intelligence) together. Each discipline has its own characteristics in supporting UAS intelligence-led taxonomy. The research methodology is illustrated in Table 3.3, where technical analysis will be performed for the UAV forensic and FORINT disciplines and a self-reported survey will be conducted to identify behavioral patterns related to UAS deviants. Finally, the

taxonomy will combine the findings of all three disciplines to answer the proposed research question.

Table 3.3.
Research Methodology & Contribution

Discipline	**Research Method(s)**	**Contribution**
UAV Forensic Investigation	Technical Analysis	Integrity and Reliability of UAS digital evidence
Behavioral Analysis	Survey	Behavioral profiling UAS deviant actions
Forensic Intelligence (FORINT)	Technical Analysis and Survey	UAS threat hunting and investigation techniques

3.5 Summary

This chapter provided extensive information about the research methodology. The study incorporates three domains in an interdisciplinary approach to enhance the forensic case data collection and analysis aiding the UAV forensic investigation techniques. This chapter demonstrate the importance of additional components to UAV forensics, such as behavioral analysis and FORINT. The main goal of the study is to integrate three important elements: technology, people, and process.

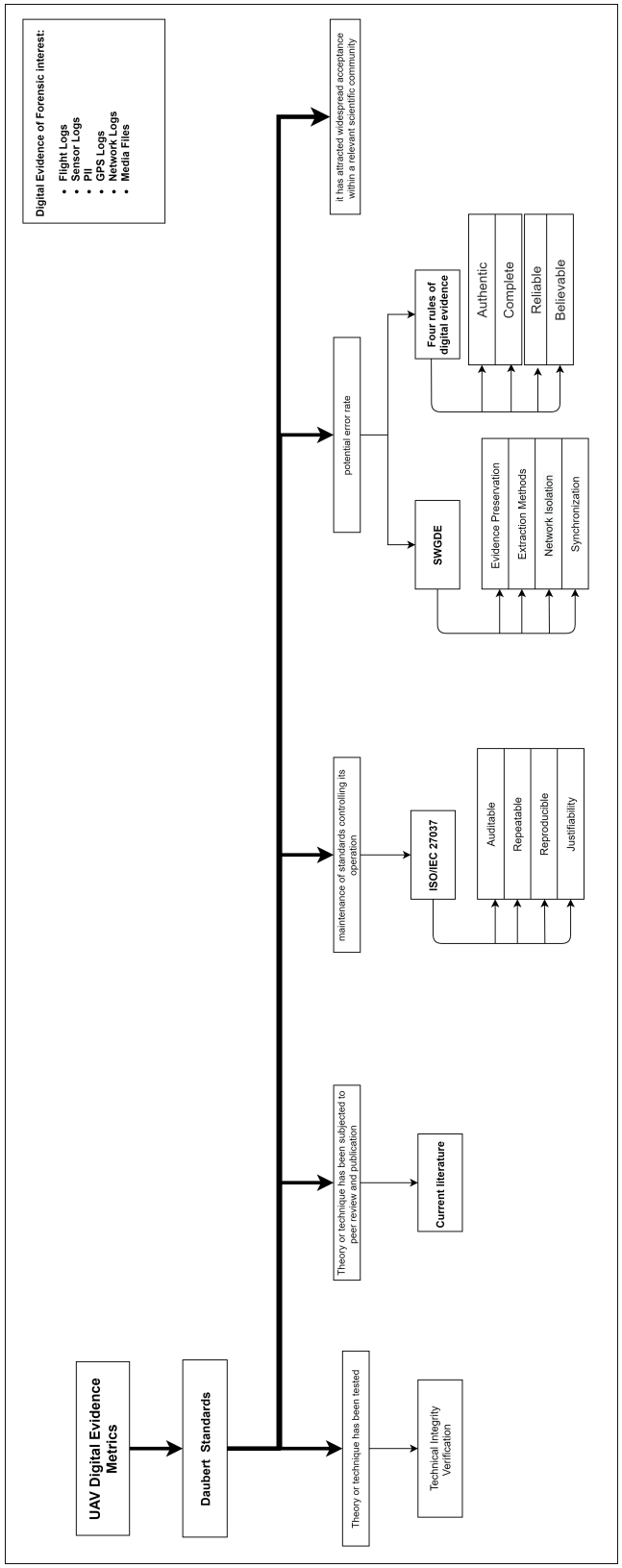


Figure 3.7. UAV Digital Evidence Metrics

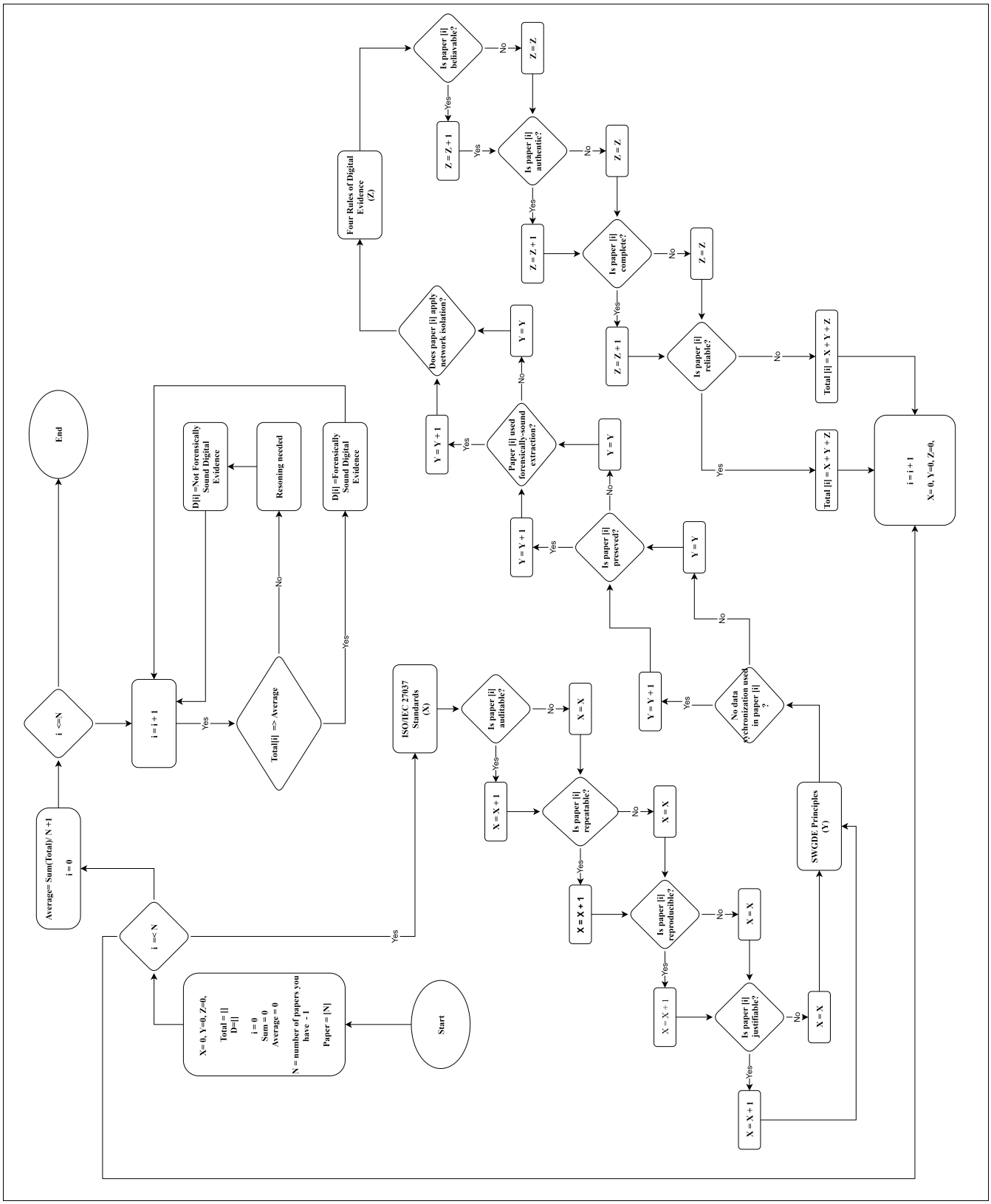


Figure 3.8. UAV Digital Evidence Evaluation Process

4. RESULTS AND ANALYSIS

In this chapter, the author discusses and addresses the proposed hypotheses of each dimension (i.e., behavioral analysis, FORINT, and UAV forensic). Each dimension is responsible for a specific contribution as shown in the UAS forensic intelligence-led taxonomy mind map (Figure 4.1). The author proposes a taxonomy that consists of three important aspects including—technical, behavioral, and procedural. The technical aspect deals with technical challenges associated with UAV forensics such as integrity, reliability, and reproducibility of digital evidence recovered from UAVs. The behavioral aspects classify the UAS deviance behaviors based on the level of tendency. Finally, the procedural aspect links the two previous dimensions by collecting all data and transforming it into an intelligence based information that adds novel techniques in responding to UAV attacks.

4.1 Behavioral Analysis of UAS Deviant and Illegal Actions

There exists a paucity of research in the evaluation of characteristics of reasoning related to the use of Unmanned Aerial Vehicles (i.e., drone) among hobbyists and drone-flying deviant actions. The aim of this behavioral analysis was to reveal differences in the Big Five Personality Traits (BFPTs) related to drone-flying deviants compared to individuals who never used drones for deviant actions. Self-reported data were obtained anonymously from respondents on questions related to the attitudes and behavior of drone users. Personality traits of the respondents were measured using Widiger's Five Factor Model (FFM), which included variables such as extraversion (versus introversion), agreeableness (versus antagonism), conscientiousness (versus undependability), openness (versus closedness) to one's own experience, and neuroticism (versus emotional stability).

4.1.1 Reliability Analysis

The reliability analysis indicated no reliability score reported a score below 0.6. The reported reliability score were extraversion (versus introversion) Cronbach $\alpha = 0.655$, agreeableness (versus antagonism) Cronbach $\alpha = 0.773$, conscientiousness (versus undependabil-

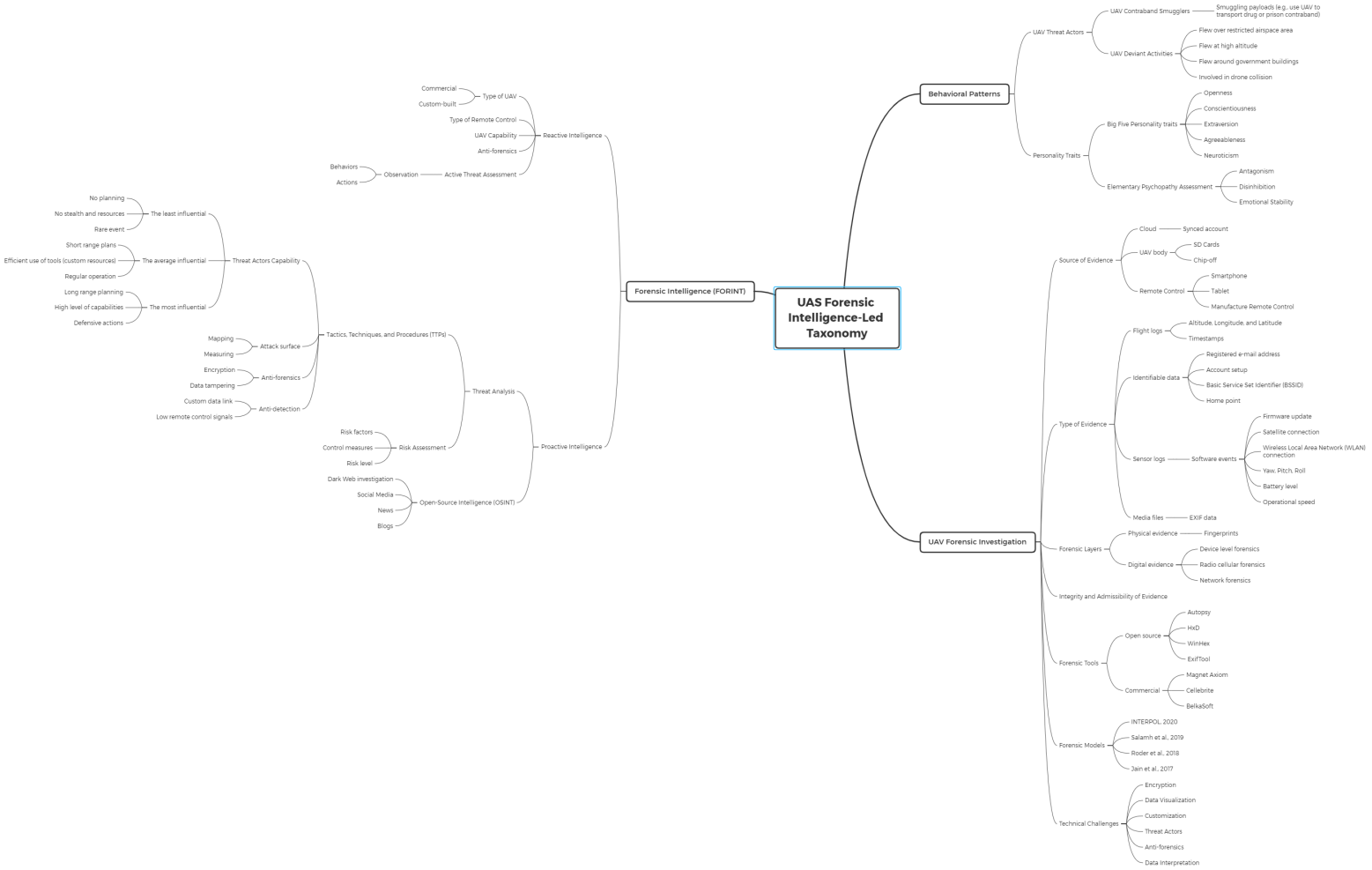


Figure 4.1. UAS Forensic Intelligence-led Taxonomy Mind Map

ity) Cronbach α =0.748, openness (versus closedness) to one's own experience Cronbach α = 0.729, neuroticism (versus emotional stability) Cronbach α =0.890, disinhibition Cronbach α = 0.815, and antagonism Cronbach α = 0.767.

4.1.2 Behavioral Profile of Drone Drug Smugglers

The analysis was performed on 266 respondents comprising 60.7% (n = 162) non-drone smugglers, and 39.0% (n = 104) who smuggle drugs using drones (see Table 4.1). The descriptive statistics illustrated in Table 4.2 indicate that the 266 respondents comprise about 184 males and 82 females. The majority of respondents were Asians followed by white race as shown in Table 4.3. The sample included variety of degree holders and most participants hold bachelor's or master's degrees; whereas, age group 18 to 35 represents 210 out of the 266 respondents (see Tables 4.4 and 4.5).

The BFPTs were able to distinguish drone drug smugglers from non-drone smugglers. The empirical results showed that drone drug smugglers reported a significant difference in the magnitudes of neuroticism and extraversion traits. Neuroticism trait significantly predicts the behavioral tendency among drone drug smugglers.

Table 4.1.
Frequency distribution of drone deviants vs nondeviant drone deviants (drug Smuggling)

Variables	**Frequency**	**Percent**
Drone Smugglers	104	39.0
Non-drone Smugglers	162	60.7

Table 4.2.
Descriptive statistics by gender

Variables	**Frequency**	**Percent**
Male	184	69.2
Female	82	30.8

Table 4.3.
Descriptive statistics by ethnicity

Variables	Frequency	Percent
White	74	27.8
Hispanic or Latino	11	4.1
African American	19	7.1
Asian	153	57.5
Native American	7	2.6
Other	2	.8

Table 4.4.
Descriptive statistics by degree

Variables	Frequency	Percent
High school diploma or GED	13	4.9
Associate degree	24	9
Bachelor's degree	159	59.8
Master's degree	69	25.9
Doctorate degree	1	.4
Other	2	.8

Table 4.5.
Descriptive statistics by age group

Variables	Frequency	Percent
(Ages 18 - 25)	60	22.6
(Ages 26 - 35)	160	60.2
(Ages 36 - 45)	31	11.7
(Ages 46 - 55)	11	4.1
(Ages 56 - 65)	4	1.5

Figure 4.2 shows no outliers for drone drug smugglers and non-drone smugglers distribution. The Kolmogorov-Smirnov and Shapiro-Wilk tests for normality, illustrated in Table 4.6, yielded p-values > 0.05 for all groups, thereby accepting the null hypothesis of normality. The normal Q-Q Plots shown in (Figures 4.3 and 4.4) confirmed the proximity of observed and expected quantiles of the distributions indicating that data were normally distributed.

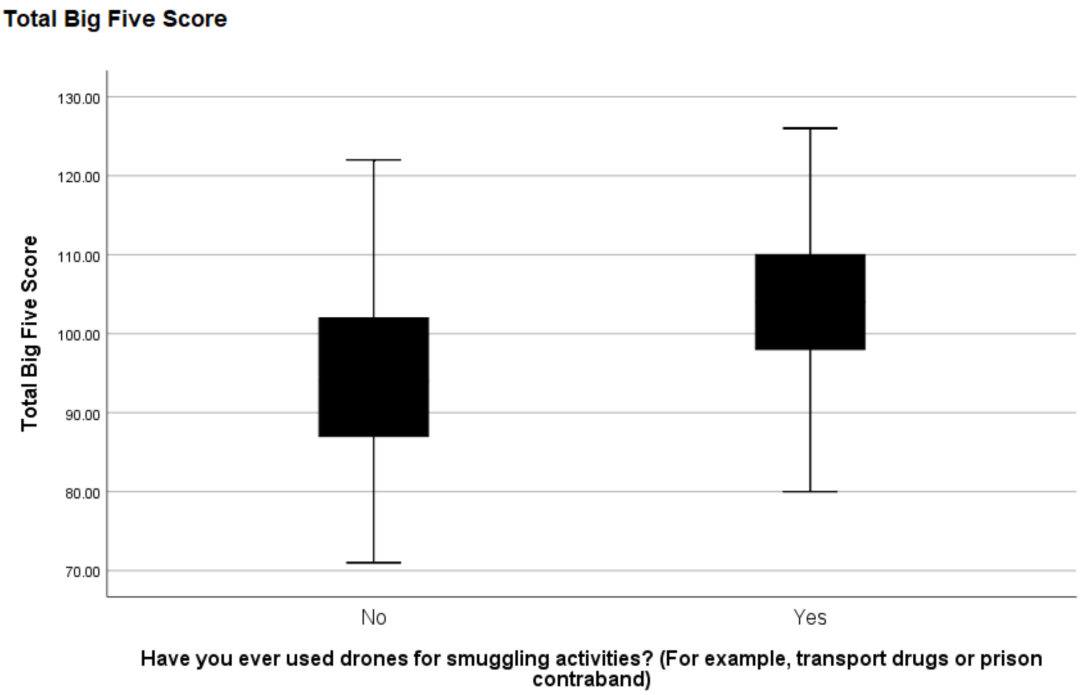


Figure 4.2. A boxplot showing no outliers for drone and non-drone drug smugglers distribution

Table 4.6.

Tests of normality of the big five personality traits among drone drug smugglers and non-drone smugglers.

Big Five Personality (total score)	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	Df	Sig	Statistic	Df	Sig
Drone Smugglers	0.108	104	0.005	0.960	104	0.003
Non-drone Smugglers	0.036	162	0.200*	0.995	162	0.848

*. This is a lower bound of the true significance.

[a]. Lilliedors Significance Correction.

Independent t-tests examining the distribution of neuroticism (versus emotional stability) among drone drug smugglers (n = 104) showed mean value (M) of 21.5 (SD = 4.6) compared to non-drone smugglers (n = 162) (M = 15.45; SD = 5.5) (see Table 4.8).

The between-group differences in values of SD were found to be significant (Levene's test; p= .001). Therefore, the equality of variances was rejected and the p-value of the t-test not assuming equal variances was reported: t (264.47) = -9.66, p= .00. Since p < 0.05, the null

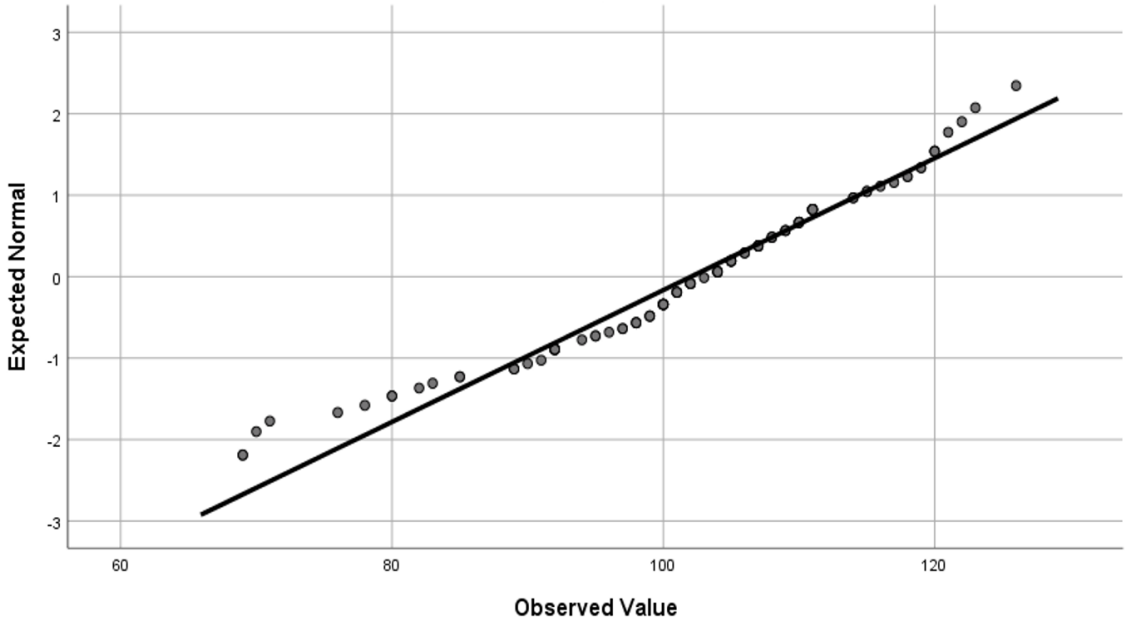


Figure 4.3. Normal Q – Q Plot BFPT for non-drone Smugglers

hypothesis was rejected, showing that neuroticism (versus emotional stability) was significantly different between drone drug smugglers and non-drone smugglers. The distribution of openness (versus closedness) to one's own experience among drone deviants (n = 104) showed (M = 21.46; SD = 4.2) compared to nondeviant drone users (n = 162) (M = 19.72; SD = 4.2). The between-group differences in values of SD were found to be not significant (Levene's test; p= .963). Therefore, the variances were assumed to be equal and the p-value of the t-test for the equal variances was reported: t(264) = -3.27, p= .01. Since p $<$ 0.05, the null hypothesis was rejected, showing that openness (versus closedness) to one's own experience was significantly different between drone drug smugglers and non-drone smugglers. The distribution of agreeableness (versus antagonism) among drone deviants (n = 104) showed (M = 21.62; SD = 3.9) compared to nondeviant drone users (n = 162) with (M = 20.91; SD = 4.3). The between-group differences in values of SD were found to be not significant (Levene's test; p= .149). Therefore, the variances were assumed to be equal and the reported p-value of the t-test for the equal variances was reported: t(264) = -1.34, p= .181. Since p $>$ 0.05, the null hypothesis was accepted, showing that agreeableness (versus antagonism)

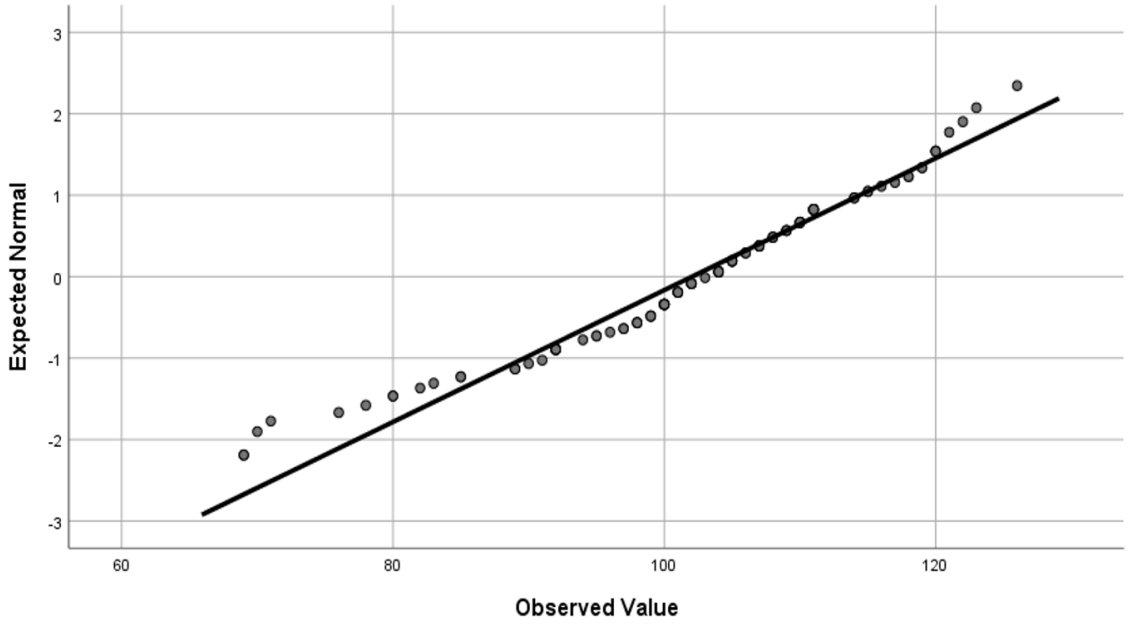


Figure 4.4. Normal Q – Q plot BFPT for drone drug smugglers

was not significantly different between drone drug smugglers and non-drone smugglers. The distribution of conscientiousness (versus undependability) among drone deviants (n = 104) showed (M = 22.41; SD = 3.5) compared to nondeviant drone users (n = 162) with M = 22.24 (SD = 3.8). The between-group differences in values of SD were found to be not significant (Levene's test; p= .307). Therefore, the variances were assumed to be equal and the reported p-value of the t-test for the equal variances was reported: t(264) = -0.37, p= .708. Since p > 0.05, the null hypothesis was not rejected, showing that conscientiousness (versus undependability) was not significantly different between drone drug smugglers and non-drone smugglers. Finally, the distribution of extraversion (versus introversion) among drone deviants (n = 104) showed (M = 11.51; SD = 3.6) compared to nondeviant drone users (n = 162) with M = 12.77 (SD = 3.3). The between-group differences in values of SD were found to be not significant (Levene's test; p= .914). Therefore, the variances were assumed to be equal and the reported p-value of the t-test for the equal variances was reported: t(264) = 2.90, p= .004. Since p < .05, the null hypothesis was rejected, showing that extraversion (versus introversion) was significantly different between drone drug smug-

glers and non-drone smugglers. The empirical results for the first deviant action (i.e., drone drug smugglers) indicates that there is a significant difference in the BFPT between between drone drug smugglers and non-drone smugglers; hence, the author concludes that there were individual differences between drone drug smugglers and non-drone smugglers.

A Simple Linear Regression (SLR) was carried out to test if neuroticism and extraversion personality traits significantly predict the tendency for drone deviant actions. The models linked the binary indicator of involving in a drug smuggling activity using drones or not (1 – yes, 0 - no) with the corresponding scores, which resulted in the estimation of two linear probability models.

The analysis showed a significant regression (F (1, 264) = 86.29, p= .000), with an *R2* of 0.243; hence, 24.3% of the variance in the probability of involving in a drug smuggling activity using drones may be explained by neuroticism (see Table 4.7).

Table 4.7.
Summary of simple regression analyses for neuroticism and extraversion predicting drone smugglers)

Predictors	***B***	***SE B***	β
Neuroticism	0.04	0.00**	0.5
Extraversion	-0.03	0.00**	-0.18
R^2		0.243	
		0.028	
F		86.29**	
		8.63*	

*$p < 0.05$. **$p < 0.01$.

The regression of individuals who involved in drug smuggling activity using drones status on extraversion score was also significant (F (1, 264) = 8.63, p= .004), thus involving in a drug smuggling activity using drones may be explained by extraversion. This indicates that neuroticism and extraversion personality traits are significant predictors for individuals who involved in drug smuggling activity using drones.

An increased level of neuroticism implies an increase in traits such as anger, embarrassment, temptation, and helplessness. The empirical result supported the research goal. Extraversion was another personality trait that can distinguish between drone and non-drone

Table 4.8.
Comparing personality traits between drone and non-drone smugglers .

		Groups			
Variable		Drone Smugglers ($n = 104$)	Non-drone Smugglers ($n = 162$)	t-value	p
neuroticism (versus emotional stability)	M	21.51	15.45	-9.29	0.000
	SD	(4.6)	(5.5)		
openness (versus closedness) to one's own experience	M	21.46	19.72	-3.27	0.001
	SD	(4.2)	(4.2)		
agreeableness (versus antagonism)	M	21.62	20.91	-1.37	0.171
	SD	(39)	(4.3)		
conscientiousness (versus undependability)	M	22.41	22.24	-0.37	0.708
	SD	(3.5)	(3.8)		
extraversion (versus introversion)	M	11.51	12.77	2.90	0.004
	SD	(3.6)	(3.3)		

smuggler. The results showed a significant difference between the two groups indicating that drone smugglers had a lower level of extraversion, suggesting an introverted personality trait.

To better understand antisocial personality traits that predict the behavior of drone drug smugglers, regression analyzses were conducted on the three instruments of Antisocial Personality Disorders (APD) including, disinhibition, antagonism, and emotional stability. These analyzes will determine if any of the APD behaviors significantly predict the tendency for drone drug smugglers.

A Simple Linear Regression (SLR) was carried out to test if disinhibition and antagonism behavior significantly predict the tendency for drone smugglers. The models linked the binary indicator of being a drone-flying smuggler `(1 - yes, 0 - no)` with the corresponding scores, which resulted in the estimation of two linear probability models.

The analysis showed a significant regression (F (1, 264) = 73.47, $p = .000$), with an *R2* of 0.218; hence, being a drone smuggler may be explained by disinhibition personality disorder. The regression of drone drug smugglers on antagonism was also significant (F (1, 262) = 53.82, $p = .000$), indicating that being a drone smuggler may be explained by antagonism personality disorder. As a result, this indicates that disinhibition and antagonism may be significant predictors of APD among drone smugglers (see Table 4.9).

Table 4.9.

Summary of simple regression analyses for disinhibition and antagonism predicting drone smugglers

Predictors	***B***	*SE B*	β
Disinhibition	4.11	0.00**	0.47
Antagonism	4.43	0.00**	0.41
R^2		0.218 0.171	
F		73.47** 53.82**	

*$p < 0.05$. **$p < 0.01$.

The APD and BFPT scores obtained were effective in distinguishing individuals based on certain personality traits such as APDs (i.e., disinhibition and antagonism). These novel and highly distinguishing features in the behavioral personality of the drone users included in this study may be of particular importance not only in the field of behavioral psychology, but also law enforcement.

For the first time, to the best of the author's knowledge, the personality traits of normal drone users and individuals who anonymously self-professed to being involved in deviant actions usign drones were tested in this study using the Five Factor Model (FFM) and the Elemental Psychopathy Assessment (EPA) to measure their level of personality. The FFM included all the BFPTs and the EPA comprise traits related to APDs (i.e., disinhibition, antagonism, and emotional stability). We excluded emotional stability scale as a variable in our analysis because the preliminary work of this research indicated that neuroticism was a significant predictor of drone drug smugglers, and further there were no significant individual differences in agreeableness (versus antagonism) between drone drug smugglers and normal drone users. The Statistical analyses showed no significance difference in the levels of agreeableness and conscientiousness between drone drug smugglers versus normal drone users. This may be attributed to the inclusion of participants who committed other types of crimes in the sample of normal drone users ($n = 162$). Thus, the results indicated that disinhibition and antagonism were significant predictors of APD in drone drug smugglers.

The findings supported the overall research question in regards to the evaluation of the behavioral characters to supplement the proposed UAS forensic Intelligence-led taxonomy.

4.1.3 Behavioral Analysis of UAS Deviant Actions

This research categories drone deviant actions into four groups:

- Drone users who flew a drone over an airfield.
- Drone users who flew a drone too high (i.e, above the legal altitude).
- Drone users who flew a drone up close to government buildings.
- Drone users who involved in a drone collision (e.g., personal injuries, plan crashes, or property damage).

The study sample included 5.1% (n = 26) drone users who flew in controller airspace, 5.1% (n = 26) drone users who flew around government building, 7.5% (n = 38) drone users who Flew at high altitude, and 5.7% (n = 29) drone users who involved in a drone Collision (see Table 4.10).

Table 4.10.
Frequency distribution of drone deviant actions.

Variables	**Frequency**	**Percent**
Flew in controller airspace	26	5.1
Flew around government building	26	5.1
Flew at high altitude	38	7.5
Drone Collisions	29	5.7

A Simple Linear Regression (SLR) was carried out to test personality traits that significantly predict the tendency for each deviant action. The models linked the binary indicator of involving to any of the four deviant actions `(1 - yes, 0 - no)` with the corresponding scores.

The analysis showed a significant regression (F (1, 500) = 8.251, p= .006); hence, drone users who flew in controlled airspace may be explained by neuroticism. The regression of

drone users who flew in controlled airspace status on antagonism score was also significant (F (1, 500) = 13.282, p= .000), thus drone users who flew in controlled airspace may be explained by antagonism. In comparison, the regression of this deviant group on disinhibition was significant (F (1, 500) = 17.331, p= .000); thus, drone users who flew in controlled airspace may be explained by disinhibition (see Table 4.11).

Table 4.11.
Summary of simple regression analyses for personality traits predicting drone users who flew in controlled airspace.

Predictors	***B***	***SE B***	β
Neuroticism	0.005	0.002*	0.127
Antagonism	0.006	0.043**	0.161
Disinhibition	0.008	0.002**	0.183
		0.016	
R^2		0.26	
		0.033	
		8.251*	
F		13.282**	
		17.331**	

*$p < 0.05$. **$p < 0.01$.

The second UAS deviant action is flying around government buildings. The regression model indicates that neuroticism, emotional tability, antagonism, and disinhibtion were significant predictors of drone users who flew around government buildings. The analysis showed (1) a significant regression (F (1, 500) = 13.084, p= .000); hence, drone users who flew around government buildings may be explained by neuroticism, (2) a significant regression (F (1, 500) = 4.389, p= .037); hence, drone users who flew around government buildings may be explained by emotional stability, (3) a significant regression (F (1, 500) = 28.692, p= .000); hence, drone users who flew around government buildings may be explained by antagonism, and (4) a significant regression (F (1, 500) = 27.212, p= .000); hence, drone users who flew around government buildings may be explained by disinhibition (see Table 4.12).

The third UAS deviant action is flying at a high altitude (e.g., above 400 feet). The regression analysis indicates that this particular group has four predictors—including, neu-

Table 4.12.
Summary of simple regression analyses for personality traits predicting drone users who flew around government building.

Predictors	***B***	*SE B*	β
Neuroticism	0.006	0.002**	0.159
Emotional Stability	0.006	0.003*	0.093
Antagonism	0.009	0.002**	0.233
Disinhibition	0.010	0.002**	0.227
		0.025	
R^2		0.009	
		0.054	
		0.051	
		13.084**	
F		4.389*	
		28.692**	
		27.212**	

*$p < 0.05$.**$p < 0.01$.

roticism, extraversion, antagonism, and disinhibition. The analysis showed (1) a significant regression (F (1, 500) = 13.994, p= .000); hence, drone users who flew too high may be explained by neuroticism, (2) a significant regression (F (1, 500) = 4.862, p= .028); hence, drone users who flew too high may be explained by extraversion, (3) a significant regression (F (1, 500) = 47.385, p= .000); hence, drone users who flew too high may be explained by antagonism, and (4) a significant regression (F (1, 500) = 27.812, p= .000); hence, drone users who flew too high may be explained by disinhibition (see Table 4.13).

The last UAS deviant action group is people who involved in drone collisions such as personal injuries and property damage. The statstical analysis indicates three predictors for this group—including neuroticism, antagonism, and disinhibition. The regression result showed (1) a significant regression (F (1, 500) = 7.173, p= 0.008); hence, drone users who involved in drone collisions may be explained by neuroticism, (2) a significant regression (F (1, 500) = 30.611 , p= 0.000); hence, drone users who involved in drone collisions may be explained by antagonism, and (3) a significant regression (F (1, 500) = 15.700 , p= .000); hence, drone users who involved in drone collisions may be explained by disinhibition (see Table 4.14).

Table 4.13.
Summary of simple regression analyses for personality traits predicting drone users who flew at high altitude.

Predictors	***B***	***SE B***	β
Neuroticism	0.007	0.002**	0.164
Extraversion	-0.008	0.004*	-0.98
Antagonism	0.013	0.002**	0.294
Disinhibition	0.012	0.002**	0.229
		0.027	
R^2		0.010	
		0.087	
		0.052	
		13.994**	
F		4.862*	
		47.385**	
		27.812**	

*$p < 0.05$. **$p < 0.01$.

Table 4.14.
Summary of simple regression analyses for personality traits predicting drone users who involved in drone Collisions.

Predictors	***B***	***SE B***	β
Neuroticism	0.005	0.002*	0.118
Antagonism	0.009	0.002**	0.240
Disinhibition	0.088	0.002**	0.174
		0.014	
R^2		0.058	
		0.030	
		7.173*	
F		30.611**	
		15.700**	

*$p < 0.05$. **$p < 0.01$.

4.1.4 Hypothesis One Testing

The hypothesis for this dimension is that *H1*: behavioral patterns significantly predict the tendency for UAS deviant and illegal acts at a significant level of 0.05. After conducting several statistical analyses, the results indicate that the null hypothesis is rejected as there

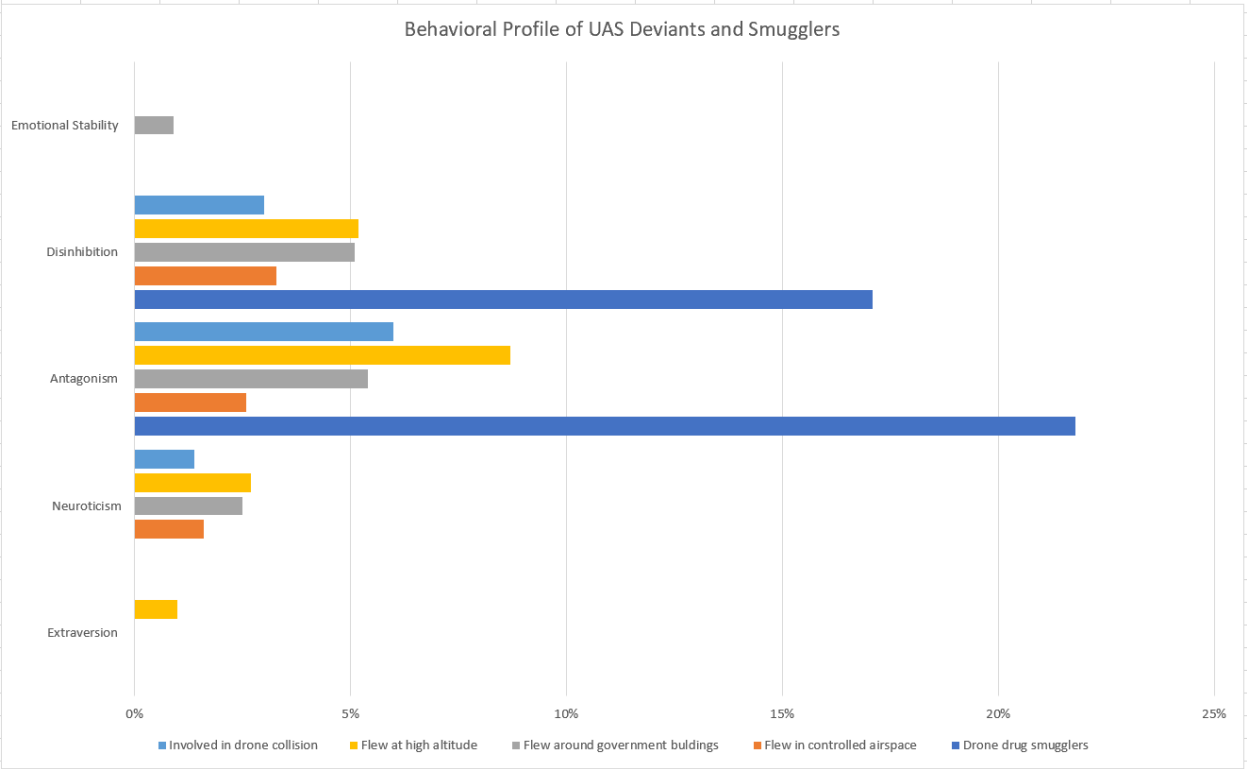


Figure 4.5. Behavioral profile of UAS deviant actions and drone smugglers

were some behavioral patterns that significantly predict the tendency for drone smugglers and drone deviant actions. The outcome of these tests will aid in building a robust taxonomy that classifies the studied groups.

4.2 Forensic Intelligence (FORINT)

The FORINT gathers and evaluates information collected from other aspects (e.g., UAV forensic and self-reported data). The evaluation of these data will be classified into two categories under the FORINT domain (e.g., proactive and reactive). Therefore, this section examines hypothesis two (i.e., self-reported techniques used by UAS deviants significantly enhance proactive and reactive intelligence modeling).

4.2.1 Reactive Intelligence

Reactive intelligence requires the collection and evaluation of information at the crime scene and/or from the counter UAS system. Information that can be collected at the crime scene for reactive intelligence includes but is not limited to the type of UAV, type of remote control, UAV capability, the anti-forensics technique used, etc. Alternatively, information that can be identified and evaluated via the counter UAS system includes the anti-detection technique used and custom data links. However, the author emphasizes the importance of using information examined throughout the digital forensic examination process as a source feed to the reactive intelligence evaluation process. For demonstration purposes, the author presents two case scenarios to support the argument that UAV forensic analysis is an important source feed to the reactive intelligence process.

Case scenario one illustrated in Figure 4.6 shows a UAV transporting drugs to a prison. Suppose that a counter UAV is deployed on the site with good coverage (e.g., 10 kilometers radius). The UAV mission was not successful as the UAV was seized while dropping contraband, and charges were made against the drone pilot. Reactive intelligence begins after seizing the UAV where UAV forensic examiners identify, collect, and analyze data stored in the UAV. The argument here is that UAV forensic analysis adds value to many decision-making processes.

These decision-making processes include:

- Identification of anti-forensic techniques.
- Identification of UAV behavior during a mission.
- Cross-validate information captured by counter UAV systems.
- Revisit the system requirements of deployed counter UAV systems.
- Increase the visibility of environmental challenges.

On the other hand, the case scenario presented in Figure 4.7 shows some of the challenges that could impact the visibility of counter UAV systems. The UAV was flying for surveillance purposes near critical infrastructure to test the capability of currently deployed

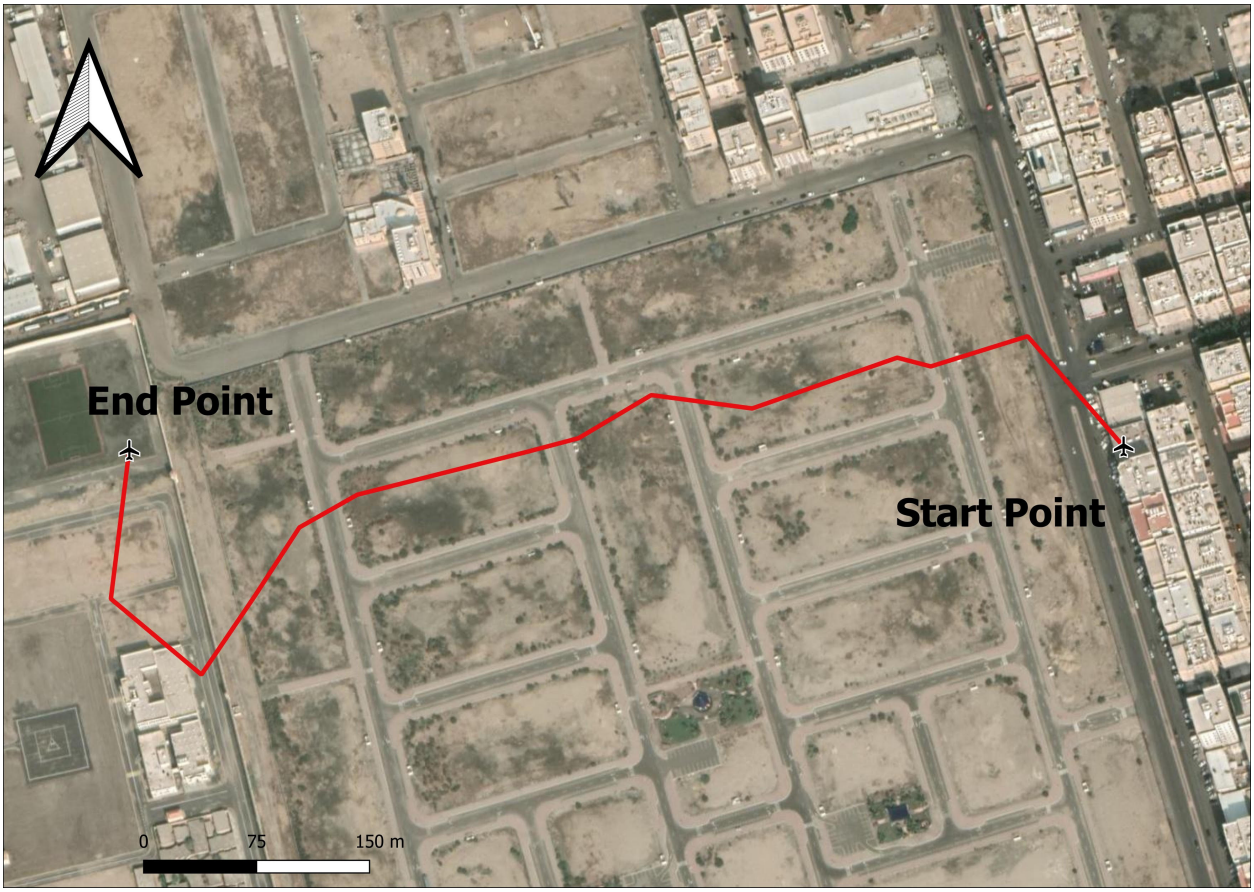


Figure 4.6. UAV Prison Contraband

systems. Supposingly, this UAV mission was not detected by all counter UAV systems and has successfully returned to the launch location. However, the same UAV crashed while operating near an airport (see Figure 4.8). Conducting a forensic analysis considering the chance that the UAV might have been involved in other malicious activities is important. For instance, examining media files and auto-generated flight logs. Also, investigating the slack space is important to determine if that particular UAV had any previous missions. From these analyses, an investigator will be able to report all findings and proceed to the legal context. When evaluating this information, decision makers will be able to enhance their capabilities in responding to such attacks. The constant change in the flight behavior of UAVs is not accurately captured from counter UAV systems and UAV forensic analysis could identify unknown features that pose challenges to these systems (e.g., software modification and anti-forensic techniques).

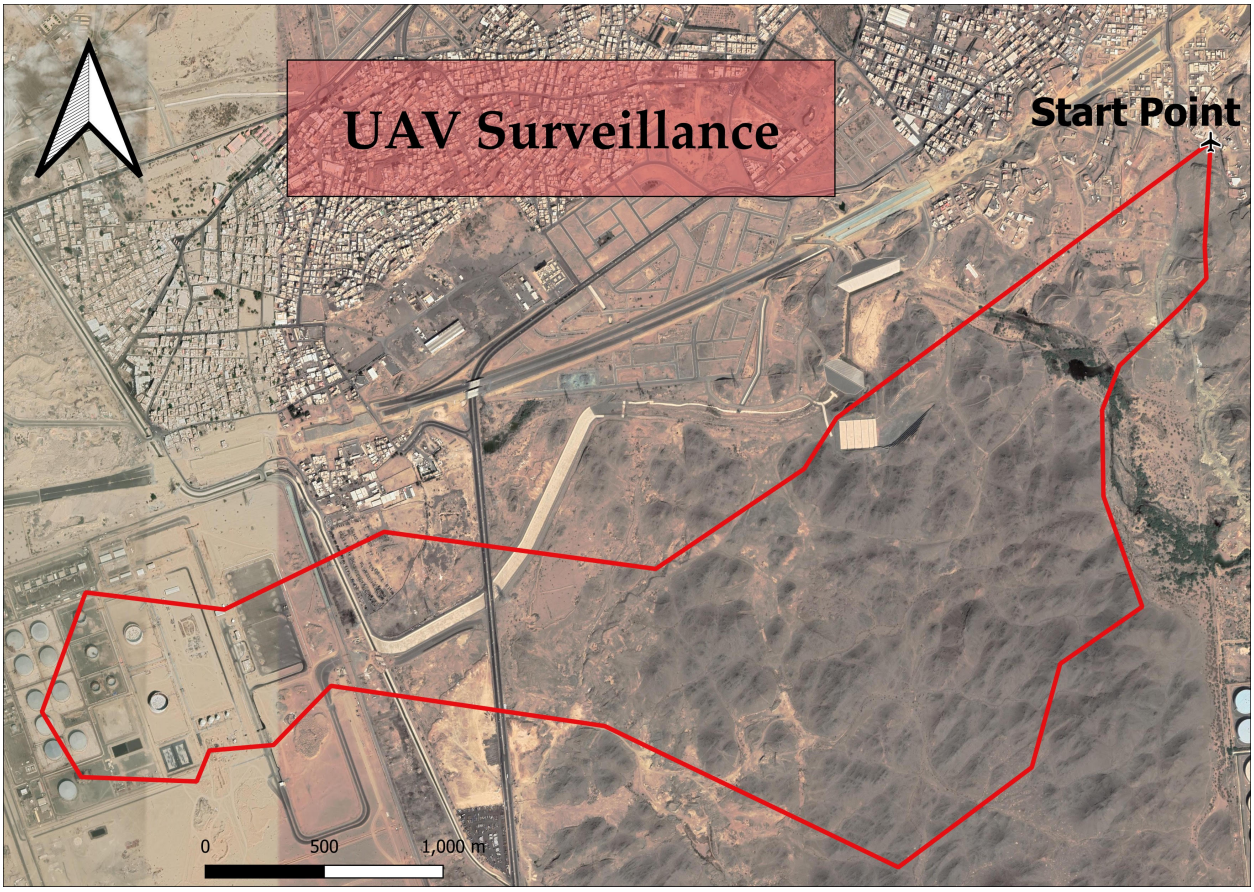


Figure 4.7. UAV Surveillance

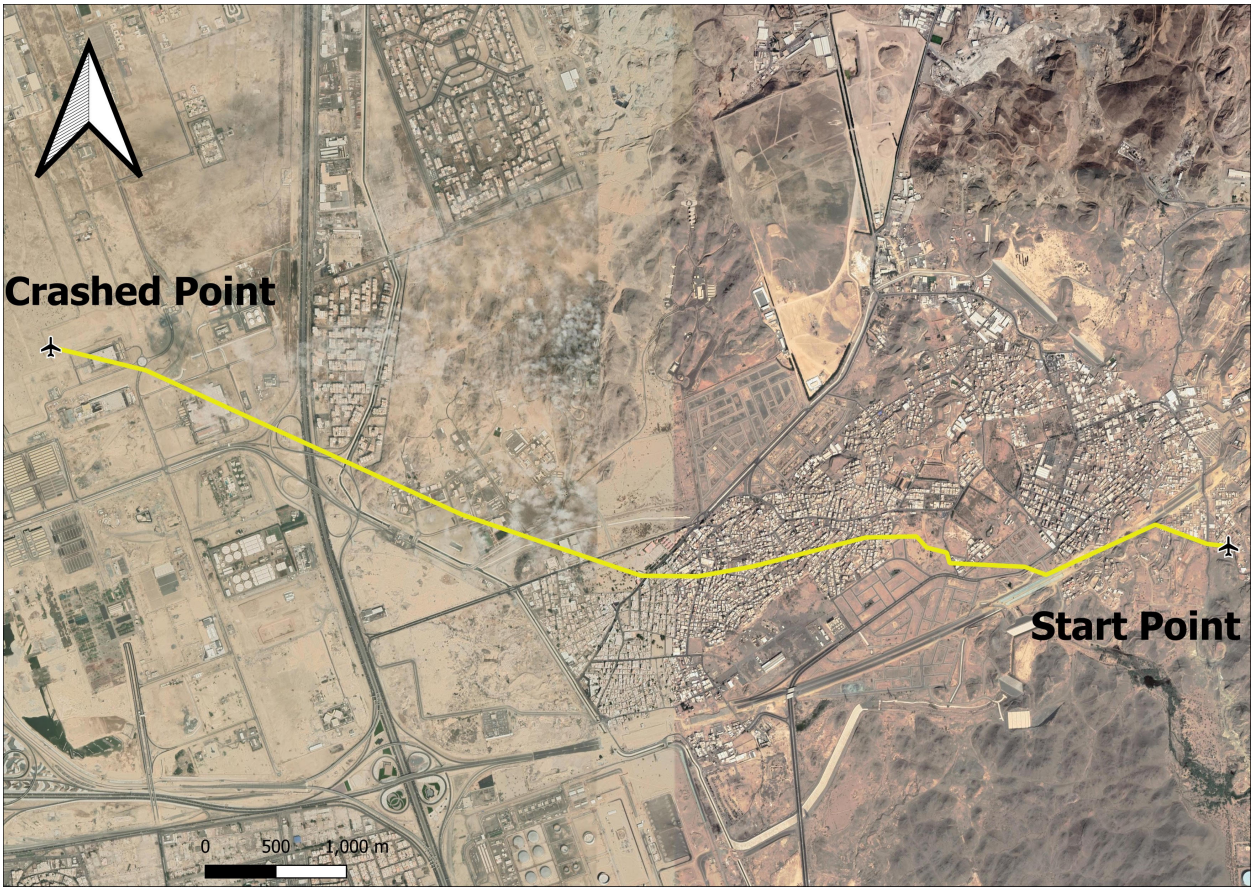


Figure 4.8. UAV Crash Incident

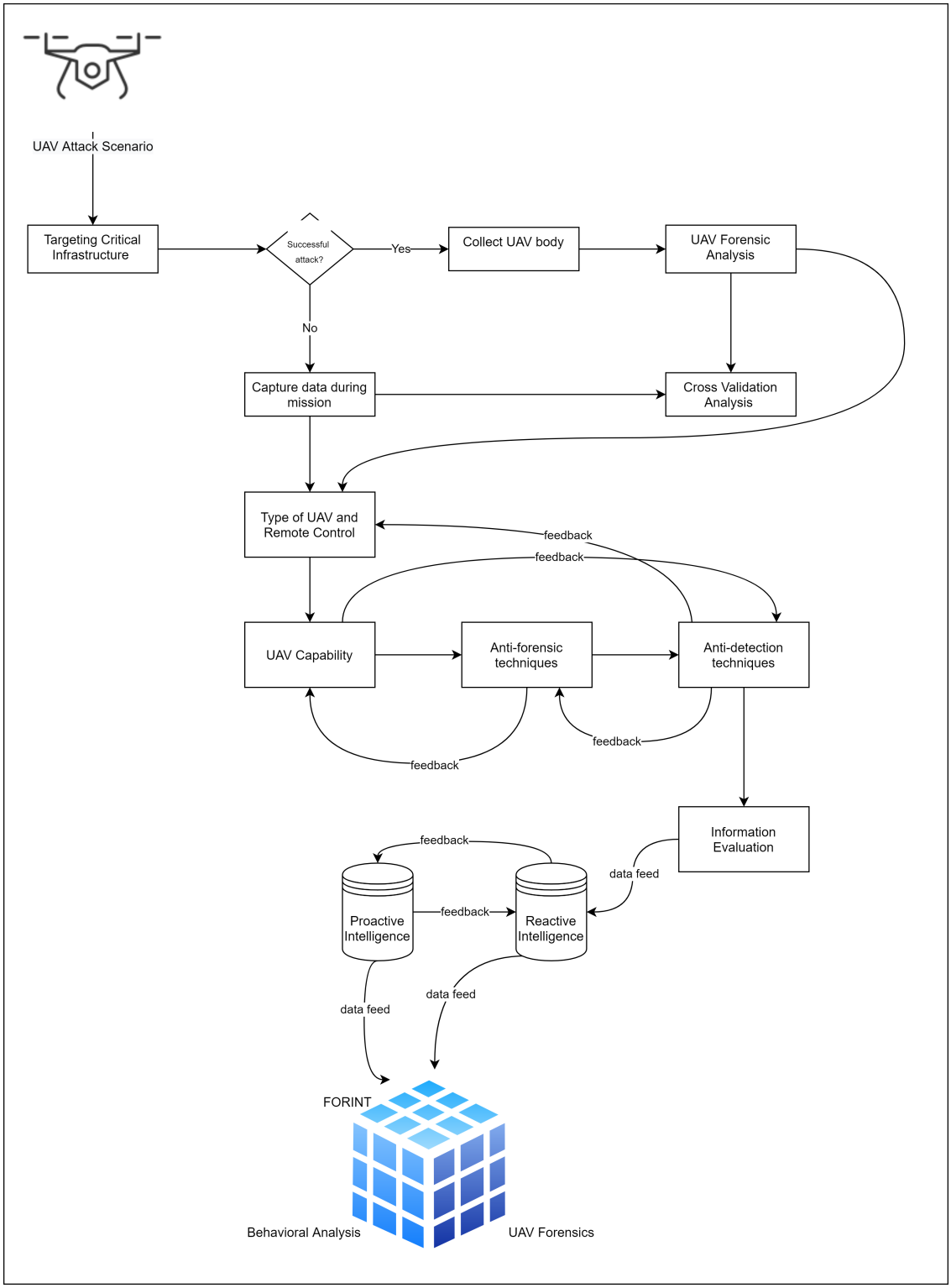


Figure 4.9. The process of reactive and proactive intelligence and their relationship to the other dimensions

4.2.2 Proactive Intelligence

As illustrated in Figure 4.9 proactive data collection feeds data into the main database collection moving to the next phase. The next phase is to gather proactive intelligence data to support the overall model. Information evaluation in this stage could involve open-source intelligence (e.g., dark web investigation) and self-reported data. Although, it is evident that the dark web has malicious activities related to UAS crimes, discussing open-source intelligence techniques is out of the scope of this research. Therefore, the proactive intelligence analysis in this research concentrates on evaluating self-reported data to draw a foundational base model. The hypothesis here is to test if self-reported techniques used by UAS deviants significantly enhance proactive and reactive intelligence modeling.

A Pearson correlation analysis was performed to further analyze the association between drone incidents (i.e., drone users who self-reported a history of drone incidents) and drone smugglers (see Table 4.15). A significant moderately positive relationship r (266) = 0.583, p < 0.01 was found; therefore indicating a significant association between drone users involved in drone-related incidents and drug smuggling using drones. This may also indicate that drone users are prone to drone incidents because they operate their drones in a manner that might result in an incident, including drone crashes due to lost signals or entering a restricted zone such as an airfield.

Table 4.15.
Correlations between drone incidents and drone drug smugglers.

Variable	Drone Smugglers
Drone Smugglers	-
Non-drone Smugglers	0.583**
Drone Incident = operating an aircraft non-compliant with safety laws	

**$p < 0.01$

Self-reported information about the UAV model used by drone smugglers and normal drone users was gathered for evaluation purposes. The evaluation started with collecting the data and identifying the UAV model used by each participant from each group. This

data can be very beneficial in determining the current technical gaps that could face UAV forensic investigators. A gap analysis-based, enhanced, UAV forensic investigation model was proposed as an approach to study these gaps and come up with an action plan that could enhance the overall UAS intelligence-led taxonomy. The model is illustrated in Figure 4.10 and it shows five important steps taken to highlight the gaps.

Gap Analysis Based Enhanced UAV Forensic Investigation Model

1. Identify technical challenges: The first step is to identify technical challenges. This includes challenges of custom-made UAV and digital forensics tools. The identification of challenges related to digital forensics tools has been discussed in Figure 3.3.

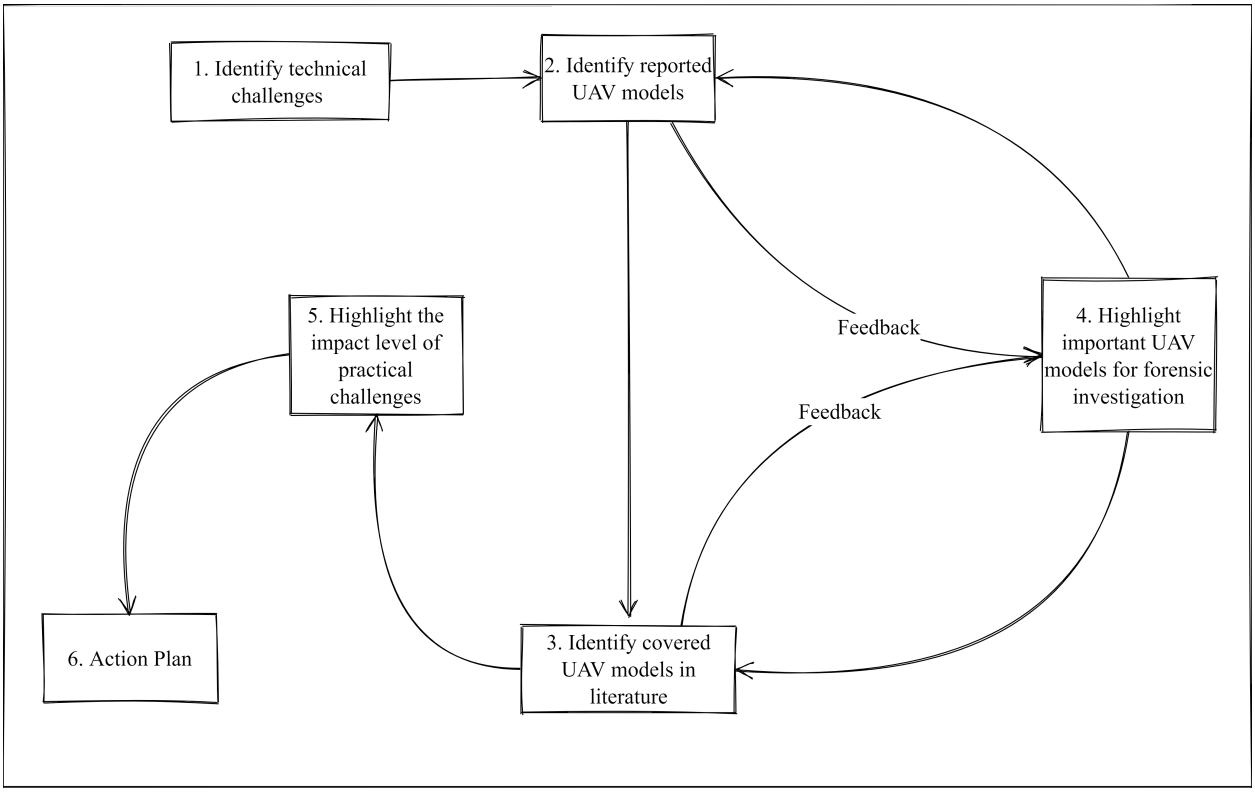


Figure 4.10. Gap analysis based enhanced UAV forensic investigation model

2. Identify reported UAV models: The second step is to gather information that was self-reported by participants on the UAV model that they use. Information gathering required some classification and data cleaning as the text entry question on the survey

was 'What is the make/model of the drone you fly?' Also, participants who declined to identify if they were involved in drone smuggling and/or deviant behaviors have been removed from the collected data (n=643). The next step is to evaluate the gathered information to enhance the proposed UAS intelligence-led taxonomy. To achieve that goal, the author classifies all reported UAV models based on several important factors such as flight endurance, weight, battery management, platform, remote control, and communication protocol. Table 4.16 illustrates the weight, flight time, and whether or not each reported UAV model has been discussed in scholarly articles.

The evaluation of this self-reported information provides intelligence related to drone smugglers and their system requirements. Mostly, they tend to target medium-sized and mid-range priced UAVs. Interestingly, the toyshine car drone reported has two functionalities. A car motor that drives to that targeted location and then it flies for about seven minutes. Most of the reported UAV models rely on wireless antenna as a communication protocol between the drone and the remote control. In addition, some smugglers reported the use of homemade and 3D printed models. Custom-made UAVs pose challenges to the UAV forensics field for several reasons. 1) The ability to customize hardware, software, and communication protocol; 2) the ability to deploy specific encryption algorithms to the stored data; 3) the ability to have more control on the UAV for data alteration purposes. All these will be discussed and included in the proposed UAS intelligence-led taxonomy.

3. Identify covered UAV models in literature: After evaluating each UAV model, the author found that most of the DJI UAV models have been recognized by researchers in the field and heavily discussed. There are still some technical challenges remaining, such as the decryption of flight logs to some specific models. However, the other reported UAV models were not presented by researchers. This does not mean that UAV forensic investigators are not aware of these models' challenges. This includes the recent drone incident response framework developed by the INTERPOL [67]. Therefore, the evaluation of this self-reported information suggests several important elements that will be discussed in the final chapter of this research.

Table 4.16.
Self-reported unmanned aerial systems with their specifications

UAV Model	Weight	Endurance	Researched
All DJI	500g - 1500g	20 - 45min	Yes
Parrot Anafi	320g	25min	Yes
3D printed	15% less than original weight	Over 20min	No
Toyshine Car	370 - 700 g	7min	No
Parrot Disco-Pro	940 g	2km	No
Vision	1360 g	N/A	No
X8 Mini	250 g	30min	No
Syma X8 pro	1560 g	12min	No
Snaptain Sp600	175 g	30min	No
Sky Viper Journey Pro	700 g	10min	No
Wingsland S6	230 g	25min	No
senseFly eBee Classic	700 g	45min	No

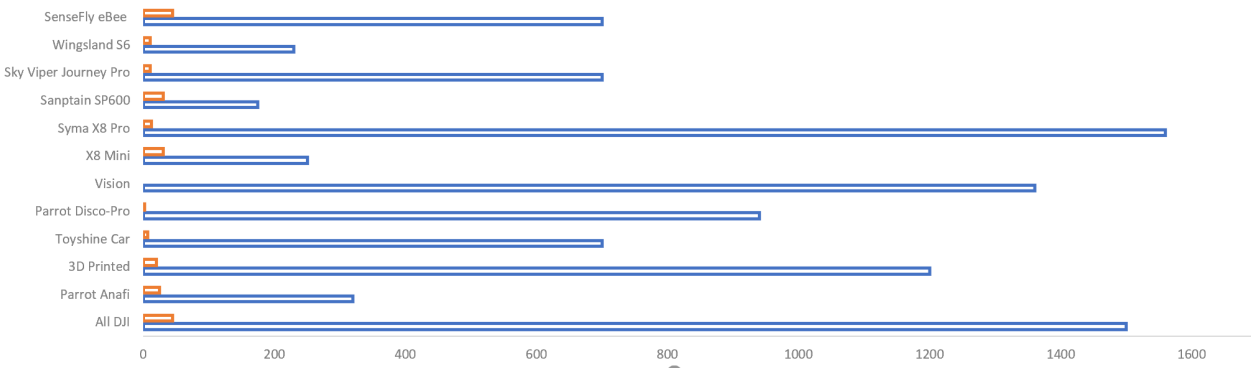


Figure 4.11. Self-reported UAV Models (Flight Endurance vs Weight)

4. Highlight important UAV models for forensic investigation: This process involves reviewing the currently available frameworks and determining unseen challenges that supplement the field. This adds to the knowledge of determining the current gaps. The current challenges include:

    - Limitation of current digital forensics tools.
    - Lack of accurate visualization of digital evidence.

- Issues related to the forensic soundness of digital evidence.
- Data encryption.
- User identification.
- File structure and operating systems of different UAV models.
- Interpretation of UAV digital evidence.
- Communication protocol vulnerability.
- Anti-forensic techniques.
- Unsecure data streaming.
- Unsecure pairing.
- Data tampering.

5. Highlight the impact level of practical challenges: Finally, this process incorporates all highlighted technical challenges and categorizes each one with its impact level on traceability. A comparative analysis model is presented in Figure 4.12 to highlight live and static technical challenges considering the level of impact. In addition, the identification of all custom-made UAV challenges is highlighted on the presented model. The model considers important factors such as monitoring, detection, prevention, and mitigation by linking each stage to the level of impact.

Figure 4.12 shows the highlighted challenges and their impact level on the traceability of digital evidence. For instance, the lack of tool support to cover the investigation of most UAV models. As discussed earlier, the evaluation of self-reported information indicate that there are a large number of UAV models that have not been discussed in previous works. Therefore, the technical challenges of those highlighted models are not clear at the time of writing this research. In addition, section 3.3 discusses further implications of the technical challenges pertaining to admissible digital evidence and some limitations such as visualization and interpretation of digital evidence. Alternatively, the impact of lacking analysis and acquisition support on some UAV models has a very high impact on digital evidence traceability. These types of challenges increase the complexity in the field and require a solid standardization document to cope with these challenges.

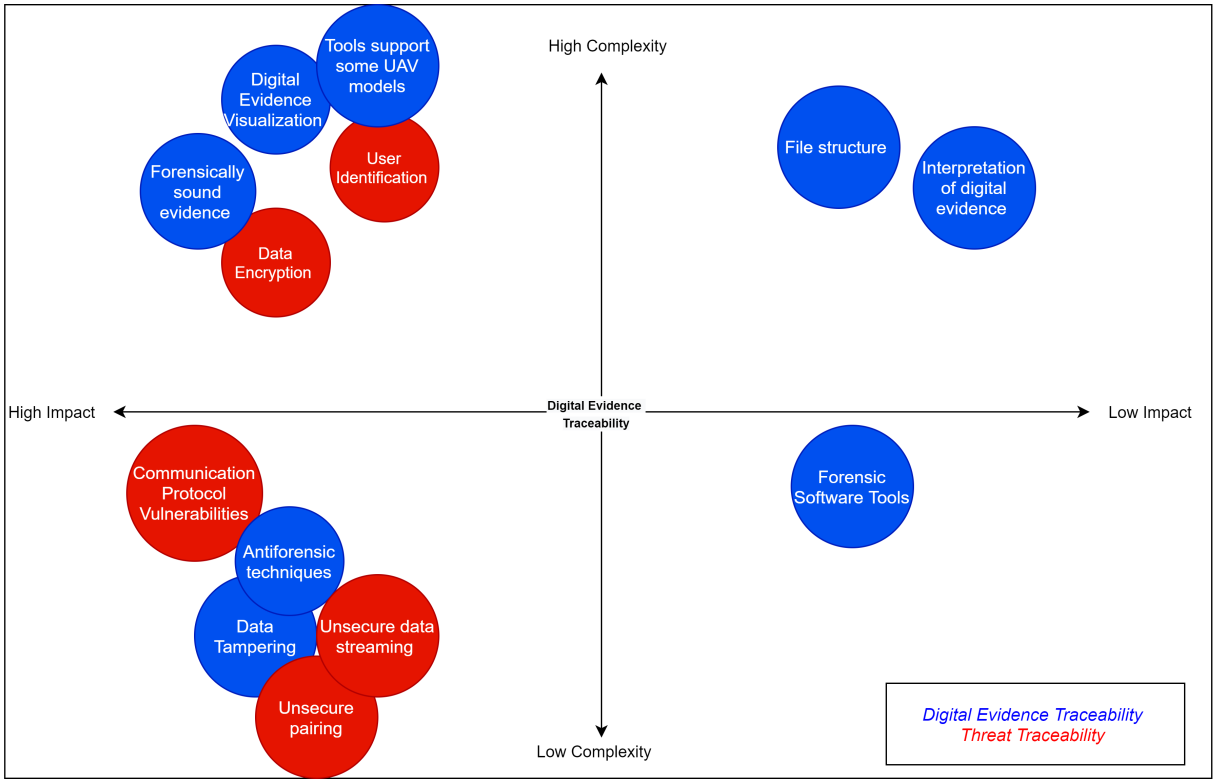


Figure 4.12. Categorization of UAV Static and Live Digital Evidence traceability Challenges [106]

Due to the importance of tactics, techniques, and procedures (TTP) followed by UAV threat actors, the author evaluates self-reported information to understand the capability and need based on their goals. The conducted study in this research used two groups: drone users who are involved in deviant behaviors, and drone smugglers who transport drugs and/or prison contraband. The TTP classification model illustrated in Figure 4.13 considers the drone smugglers group only as deviant behaviors, and should not follow a specific approach. Therefore, the TTP classification model indicates that the tactics that were self-reported include—creating a home-made drone, focus on mid-weight and range models (note: this was reported in Table 4.16), and good quality camera. During the evaluation process of the collected information, the author noticed that the majority of drone smugglers declared the use of a '4k camera'. This indicates that this is one of their system requirements to achieve their goals. Second, the reported techniques include— flying in a vertical motion, hovering in place, square pattern, quadcopter should not face the pilot, and multirotor flying.

The second arrow is pointing back to the tactics because all of these system requirements or techniques require some functions that should be available in the UAV model, for instance, multirotor flying. The evaluation of tactics such as projectile motion, hovering in place, and square pattern link targeted goals between these techniques. Therefore, hovering in place is a technique that is used by beginner drone users to learn how to control the drone and a drone smuggler might train themselves on this technique to be able to transport prison contraband or drugs. Also, projectile motion flying could be a technique used to reduce implications tied to the battery life and/or detection.

4.2.3 How behavioral characteristics add value to the technical threat intelligence field?

Table 4.17.
Correlations between Drone Incident and Disinhibition

Variable	**Drone Incident**
Drone Incident	-
DIS3	0.381**
DIS4	0.319**
DIS5	0.344**
ANT1	0.380**
ANT3	0.349**
ANT6	0.397**
ANT7	0.394**
AN8	0.340**

Drone Incident = operating an aircraft non-compliant with safety laws.
DIS3 = "Act first, think later", describes me well.
DIS4 = I am doing things that are risky or dangerous.
DIS5 = When I'm upset, I will do things I later regret.
ANT1 = I deserve special treatment.
ANT3: Feeling sorry for others is a sign of weakness.
ANT6: I quit things pretty easily.
ANT7: I could make a living as a con artist.
ANT8: I have more important things to worry about than other people's feeling.

A significant positive relationship $r\ (266) = 0.381,\ p < 0.01$ was found between drone incidents and individuals who described themselves as **Act first, think later**. A significant

moderately positive relationship $r\ (266) = 0.319$, $p < 0.01$ was found between drone-related incidents and individuals who self-reported as **doing things that are risky or dangerous**. As well, a significant moderately positive relationship $r\ (266) = 0.344$, $p < 0.01$ was found between drone-related incidents and individuals who **do things that they regret later when they are upset**. Therefore, the null hypothesis is rejected and concluded a significant association between drone users involved in drone-related incidents and types of antisocial behaviors. On the other hand, antagonism subscales (i.e., ANT1 = I deserve special treatment, ANT3: Feeling sorry for others is a sign of weakness, ANT6: I quit things pretty easily, ANT7: I could make a living as a con artist, and ANT8: I have more important things to worry about than other people's feelings) show a significant moderate correlation with drone incidents $r\ (266) = 0.380$, $p < 0.01$, $r\ (266) = 0.349$, $p < 0.01$, $r\ (266) = 0.397$, $p < 0.01$, $r\ (266) = 0.394$, $p < 0.01$, $r\ (266) = 0.340$, $p < 0.01$, respectively.

Ten out of thirteen (five disinhibition and eight antagonism subscales) reported a moderately positive correlation with drone incidents, and the other subscales showed a weak positive correlation. The correlations between users who self-reported drone incidents and the disinhibition subscale (rashness): **Act first, think later, describes me well** showed that these drone users exhibited a poor risk assessment. The significant moderate correlation between drone-related incidents and disinhibition subscales (thrill-seeking and urgency) indicated that drone-flying criminals were involved in risky or dangerous activities. On the other hand, antagonism subscales (i.e., ANT1 = I deserve special treatment, ANT3: Feeling sorry for others is a sign of weakness, ANT6: I quit things pretty easily, ANT7: I could make a living as a con artist, and ANT8: I have more important things to worry about than other people's feelings) showed significant moderate correlation with individuals who were involved in at least one drone-related incident. This may indicate drone-flying criminals were prone to drone-related incidents because they have poor risk assessment.

4.2.4 Hypothesis Two Testing

The hypothesis for this dimension is that *H3*: self-reported techniques significantly improve the proactive and reactive intelligence modeling techniques. To test this hypothesis,

the author conducted several analysis techniques that included collecting and evaluating the self-reported data and examining the reported TTPs. The analyses indicates that the null hypothesis is rejected as the self-reported information added value to the reactive and proactive intelligence. In addition, this will contribute to the overall proposed taxonomy by classifying the study groups (i.e., drone smugglers and drone deviant actions).

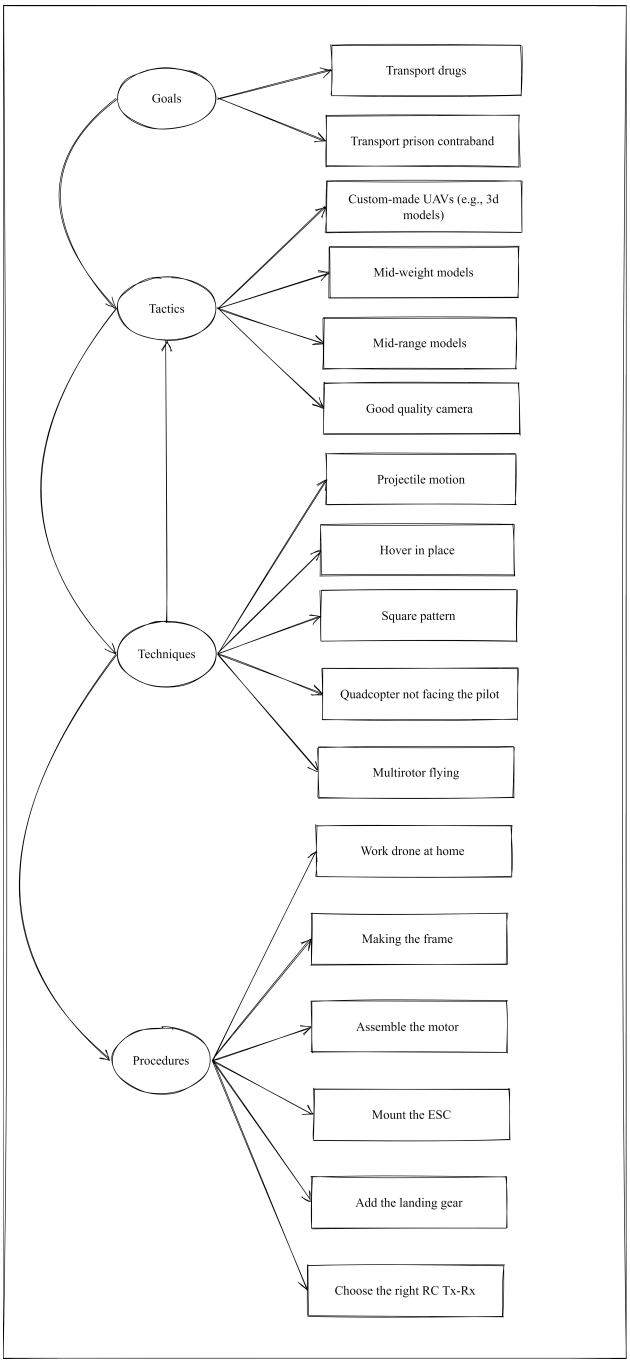


Figure 4.13. Tactics, Techniques, and Procedures (TTP) Classification Model

4.3 UAV Forensic Investigation

The number of drone-related incidents and crimes is rapidly increasing, and the heterogeneity of drone types leaves more challenges to investigative techniques. The digital forensics process begins with the identification phase and ends with the documentation and presentation phases. In this section, the author concentrates on the missing piece of the current literature (e.g., forensic soundness of digital evidence). Additionally, there will be some elaboration on the utilization of the selected UAV forensic models [6], [7], [67], [68] into these phases.

The UAV forensic investigation dimension is the primary element of the U-FIT taxonomy as it classifies digital evidence recovered from UAVs and aids investigators in making decisions when reporting findings in court. There are several important factors of the UAV forensic investigation dimension that need to be discussed. In this section, the researcher elaborates on factors that comprehend the sufficiency of the investigation process. These factors include— forensic layers, source of evidence, type of evidence, integrity and admissibility of evidence, forensic tools, forensic models, and technical challenges. All mentioned factors are linked to the admissibility standards of digital evidence. Therefore, the hypothesis for this dimension is that *H3*: forensically sound UAV digital evidence significantly enhances the reliability of the proposed UAS Forensic Intelligence-Led taxonomy. The proposed hypothesis (*H3*) investigates the UAV digital evidence technical integrity and the requirements to evaluate the forensic soundness of digital evidence extracted from UAVs.

The identification of the appropriate source of evidence is a crucial step that assists investigators in performing the next processes in a valid and reliable approach. Regarding UAV investigation, there are multiple sources with potential interest for investigators. The drone has several built-in and custom components that could lead to the recovery of digital evidence. Therefore, the author assumes that any UAV incident should have at least one or two identified components to deal with during the investigation. In certain circumstances, the analysis does not provide supportive digital evidence that could be linked to a specific suspect. In this research, the author incorporates three important disciplines aiming to minimize the issues related to the misidentification of suspects behind the controller. Sources of

evidence could be cloud accounts, mobile apps, chip-off data, storage device cards, or remote controls (i.e., built-in, custom, and mobile devices). Some of these sources are attached to the drone body, others are web-based, or separate components. Also, in some cases, physical evidence may reveal the identity of the drone pilot (suspect) and be considered as an important source of evidence.

UAVs transmit a huge volume of data in addition to the commands initiated by the user. Software logs are an example of data stored in several storage devices (e.g., remote control and drone body). The analysis of software logs reveals information related to the connected components during operation, such as the firmware version and serial numbers. Flight logs are an important piece of evidence to aid in conceptually visualizing the flight trajectory on a map; however, the recovered GPS coordinates might not be accurate and might be remotely altered. Therefore, deployed sensors transmit data that aid in validating the accuracy of the recovered flight logs. Flight logs are stored in different storage devices (cloud, mobile app, chip-off, remote control, etc). Also, flight logs are stored in different file formats depending on the UAV type. The analysis of multiple UAV types indicates that in some instances, these flight logs are encrypted, which poses technical challenges to investigators decrypting them.

Futher digital evidence that could aid in validating the examination is the analysis of media files. Media files hold evidence associated with GPS coordinates and could be used as a validation step; however, it is possible for these geotags to get altered and tampered with. In this way, the analysis of the file header and atoms is necessary to make sure that these are valid and reliable data. The analysis of media file content provides information related to the camera model, firmware version, and serial number and identifies if there were any customized components used to capture data. For instance, recovering and analyzing an 'MP4' file from a drone would start with the identification of atoms and file structure. The 'MP4' file consists of boxes beginning with the 'ftype' box that identifies the file type followed by the 'mdat' box, which holds metadata relevant to the video stream. The 'udat' atom contains two boxes (i.e., 'CAME' and 'FIRM') that could aid in identifying any customization or anti-forensic techniques deployed on the UAV. Regarding the recovery of timestamps, the movie header 'moov' holds some recurrent timestamps.

The remote control of the drone holds the most valuable digital evidence that aids forensic examiners. The issue is that UAVs have a variety of remote controls running different operating systems and storing data in different formats. Some UAVs apply encryption to transmitted data (e.g., flight and sensor logs), which requires an investigator to use software decryption tools to convert these files to a human-readable format.

Let's suppose that an investigator has encountered encrypted flight and sensor logs and used open-source tools such as the DROP [8] to decrypt flight logs from '.DAT' to '.CSV'. After accomplishing this task, the '.CSV' file needs to be visualized on a map to interpret flight patterns and determine other blackbox metadata such as waypoints, yaw, pitch, roll, speed, battery level, etc. From a technical point of view, some questions remain to the integrity of these processes. Converting an encrypted file to a readable format might alter and/or destroy some data. The author; examines this process and points out any issues associated with the integrity of digital evidence.

More important is the identification of the offender behind the remote control. As discussed earlier, that UAVs are operated with multiple components, and some may be abandoned at a crime scene. It is very challenging to obtain personal identifiable information from UAVs because in most cases flying devices do not operate on Internet networks, but satellite signals instead. However, sometimes the setup and firmware updates require an internet connection to push those updates and set up the cloud account for the flying device. In this case, network logs and personal identifiable information are valuable for investigators.

Identification of the UAV owner poses challenges to the forensic examination, especially when some UAV components have no presence at the crime scene. Since COTS UAVs usually require some setup and registration to update firmware, there should be some network records that are relevant to the identification of the owner. Therefore, the author conducted a further investigation and determines that network records (e.g., the basic service set identifier 'BSSID' and/or the service set identifier 'SSID') help investigators in identifying the suspect's physical location. However, this section deals with the forensic soundness of digital evidence recovered from UAVs, and discussing the proposed technical model is out of the scope of this subsection. In addition, the analysis of preserved network records incorporates open-source intelligence techniques; therefore, sub-section 4.2 will discuss the model in detail.

The UAV forensic investigation involves several components that need to be acquired in a certain way. For instance, the acquisition of internal storage of the drone requires some disassembling techniques to acquire an image of the internal memory. Furthermore, some cases involve cloud and/or mobile forensics. The current well-known digital forensic software tools are capable of acquiring data from UAVs. However, there are some challenges regarding the analysis, visualization, and documentation of data. As discussed earlier, UAVs share a large volume of data that is stored in a standard format, which poses challenges to the tools' development. From the current literature, there are good contributions from both commercial and open-source tool development to at least cover well-known types of UAVs such as the DJI type. Visualizing flight logs is recently supported by a few tools like Autopsy, Magenet Axiom, etc. In addition, some tools have integrated open-source parsing algorithms that can decode flight logs, which should keep the integrity of flight logs by avoiding errors during the file conversion processes.

4.3.1 Forensically Sound UAV Digital Evidence

The current literature pertaining to UAV forensic investigations covers the identification and analysis phases of digital forensics only. Most of the peer-reviewed works provide technical steps to investigators for counter challenges related to the identification, acquisition, and analysis phases. Therefore, the only missing component is the reporting phase that deals with UAV forensic investigation and specifically the interpretation of reliable and forensically sound digital evidence. Usually, the admissibility of digital evidence is the judge's role. To the best of the researcher's knowledge, previous works have not addressed the admissibility of recovered and analyzed digital evidence from UAVs.

Table 4.18 illustrates the five principles of digital evidence and a comparison of important forensic artifacts of interest to UAV forensic examiners. It is necessary to mention that there is no common metric or standard for the admissibility of all types of digital evidence; therefore, the author creates a metric for digital evidence extracted from several UAV models that were examined in scholarly articles (see Table 4.18). The proposed metric is based on several factors: extraction technique, nature of data, digital evidence standards, docu-

mentation process, data interpretation, and forensic tools. Researchers in [107] mentioned five principles of digital evidence that include— admissibility, authenticity, completeness, reliability, and believability. Since the admissibility of digital evidence is solely based on a judge's decision, a clear definition of these five principles will be given.

- Admissibility: any valid, relevant, and safe evidence that assists the jury to decide in the case [107].
- Authenticity: digital evidence has not been altered [107].
- Completeness: making sure that the digital evidence has not lost its evident value throughout the digital forensic processes, and does not show one perspective of the incident [92].
- Reliability: digital forensic processes should be undertaken in a reliable manner that does not impact the authenticity of digital evidence [92]
- Believability: digital evidence that consists of credible and true information [108].

To test hypothesis three, an investigation on the technical challenges associated with digital evidence extracted from UAVs and the integrity of tool analysis was carried out. In addition, the author conducted regression analysis on the selected variables (i.e., the evaluation score of each article) and if the citation count for each research article significantly predicts the total score of the evaluation (see table 4.20).

4.3.2 Technical Investigative Challenges

The author analyzes several *.DAT* files (i.e., encrypted flight logs) which contain important data for UAV forensic investigation. The analysis indicates that there were several issues pertaining to the integrity of recovered flight logs. Most well-known digital forensic tools (e.g., Autopsy, Magnet Axiom, and Cellebrite) process and decrypt 'DAT' flight logs using DatCon https://datfile.net/DatCon/intro.html. The decryption process follows the file structure to decode its content and allow investigators to move to the reporting and/or visualization phase. To perform this analysis, DAT' files were extracted from two DJI UAVs

that were openly available for researchers by the VTO lab as part of the drone forensics program sponsored by the United Sates department of homeland security science and technology division. Any issues were cross-validated by reproducing the same analysis on two workstations, two different UAV models, and at least two forensic software tools.

Some forensic tools were not able to decrypt the 'DAT' files recovered from the two UAV models (DJI Matrice 210 and DJI Phantom 4). In addition, the analysis indicate that there were some integrity issues pertaining to digital evidence integrity and reliability. Flight logs are the most important piece of digital evidence to be analyzed when dealing with UAV incidents. The deployed encryption by the UAV manufacturers is necessary to prevent data tampering. However, digital forensics investigators need to be able to decrypt and process the flight logs to determine the way-points, longitude, latitude, altitude, battery life, yaw, pitch, roll, etc. These flight logs contain a wide range of pre-programmed data related to sensors, actuators, and user commands. A tool like DatCon (version 4.0.5) which can decrypt the flight logs of several UAV models does not decrypt the flight logs in a forensically sound manner. The analysis shows that the DatCon software application does not produce the same cryptographic hash values for the same 'DAT' file. This means that if an investigator uses the DatCon tool, or any forensic software tool that uses the DatCon algorithm, they will encounter issues related to the reliability of the generated data.

The author provides a comparison table that includes the analysis of five 'DAT' flight logs decrypted by DatCon using two forensic workstations.

Two flight logs did not identically match when they were decrypted using two different work stations (see Table 4.18). All other flight logs matched and no reported issues were found. The two flagged flight logs indicate that the DatCon tool has some issues related to the decryption process. The author noticed that the difference is not great, but it is crucial for forensic investigators to keep the integrity of digital evidence. In addition, the difference between these files was because of additional random numbers assigned to one of the cells. Although there should be no major issues when visualizing the decrypted flight logs to view the flight route, the mismatch between the files is questionable and might lead to further implications to the investigation process.

Table 4.18.
An evaluation of the flight logs integrity as a digital evidence

File Name	MD5 Hash Value	Forensic Workstation	Modified Content	Data Type
FLY000.CSV	3342E694EF9D180123DA7FF9BBA82B55	1	Yes	$IMU\_ATTI(0) : gyroComposite : C$
FLY000.CSV	ee36a352c4052c080796096dc470406e	2		
FLY001.CSV	adb07609fe496ccd7a229b3fee0e27e0	1	No	NA
FLY001.CSV	adb07609fe496ccd7a229b3fee0e27e0	2		
FLY002.CSV	b19d668b07c53a3e909bd49019315eea	1	No	NA
FLY002.CSV	b19d668b07c53a3e909bd49019315eea	2		
FLY003.CSV	6b53a66e3ada5a9cd9ca491be48676ea	1	No	NA
FLY003.CSV	6b53a66e3ada5a9cd9ca491be48676ea	2		
FLY004.CSV	9adcf78d2887d33bfc3227c16f3d95a8	1	No	NA
FLY004.CSV	9adcf78d2887d33bfc3227c16f3d95a8	2		
FLY005.CSV	49dd94e6c3bf5c2e353255817c4641b0	1	Yes	$IMU\_ATTI(0) : distanceHP : C$
FLY005.CSV	a5763d45fbbbc264db0e4e7e315fb44e	2		

The DatCon documentation webpage provides details about the fields included in the decrypted flight logs. The following webpage https://datfile.net/DatCon/fields.html describes the fields of CSV files for two UAV models (Phantom 3 and Insprie). Most COTS models use the same terminology to define programmed events. For instance, the DatCon web page defines fields related to the internal bus clock, geo-coordinates, GPS, health, number of satellites, aviation principles, and gimbal information, etc. A digital forensic investigator would be very interested in interpreting and visualizing these data to be able to report findings. However, the current issue is when using unreliable open source tools to investigate UAVs. Therefore, the analysis conducted in this research indicates that the approach used by most of the well-known forensic tools musts meet best practices and standards to avoid issues related to data integrity and forensic soundness.

An evaluation of UAV forensic tools is out of the scope of this research; however, it is important to note that there are obvious issues concerning the forensic soundness of digital evidence acquired from UAVs. For example, the massive amount of data contained in the flight logs and the complexity of their structure. Also, it should be noted that flight logs differ from model to model. For instance, when 'FLY010.CSV' is decrypted using 'DatCon' on forensic workstation one the file size is 58,381 kilobytes, and when 'FLY010.CSV' file is decrypted on forensic workstation two the file size is 50,470 kilobytes. This means about

8000 kilobytes are missing from the second attempt at decryption. A visual comparison between the two flight logs is illustrated in Figure 4.14

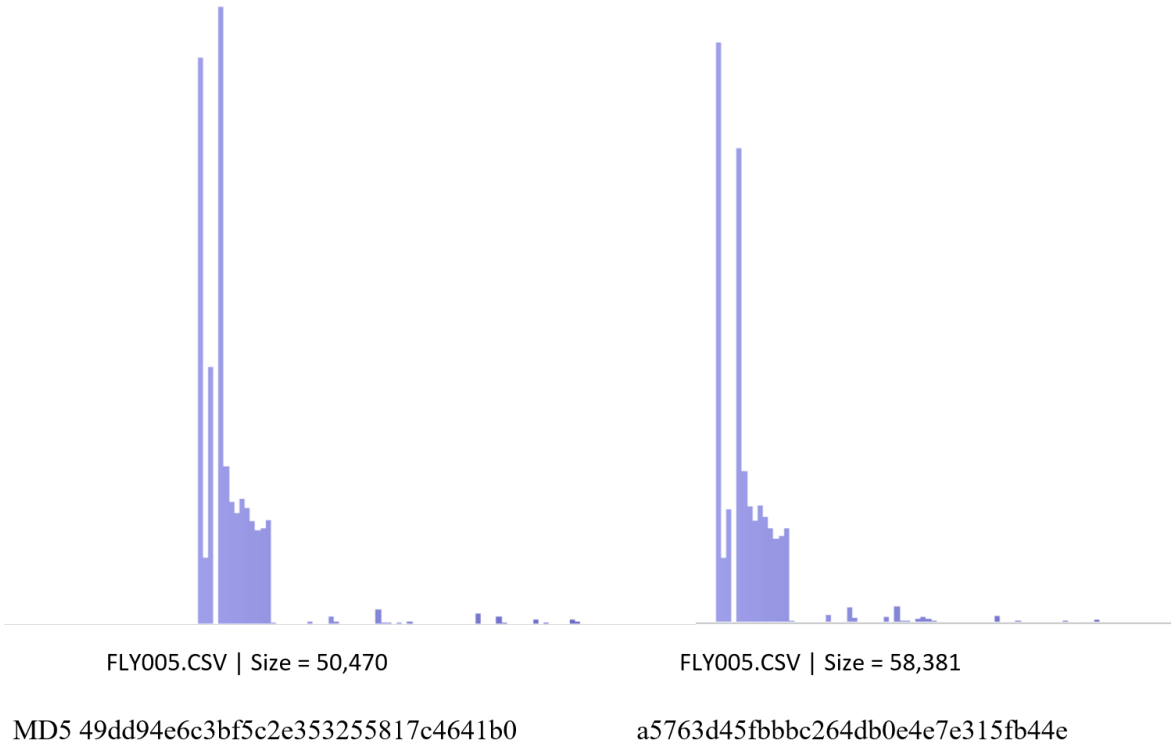


Figure 4.14. A statistical graph showing data comparison between two '.csv' flight log files

Some UAV models do not deploy a cryptographic algorithm on transmitted data, including flight logs, media files, or live-streaming video. Unencrypted data pose challenges to the UAV forensics field as the transmitted data might be tampered with. It is crucial for digital forensic investigators to make sure that the collected digital evidence has not been altered and/or compromised. This solely depends on the encryption algorithm used to secure data transmission. The UAV technical forensic investigation process model [6] illustrated in Figure 4.15 developed a technical UAV forensic investigation model that considers very important procurers such as validation techniques, data encryption, and source of evidence. The presented model includes ten processes that aid forensic investigators in drone-related

incidents. The model begins with the 'preparation' phase to prepare and collect the evidence, then the investigator needs to identify physical and digital evidence.

The UAV forensic investigation framework presented in [68] covers more details about the identification of physical evidence. For instance, the identification of fingerprints on the UAV body and customization (e.g., GPS signal prevention). The UAV technical forensic investigation framework also highlights the importance of investigating metadata recovered from media files along with the recovered flight logs. Media files contain metadata such as flight duration, GPS coordinates, and timestamps. These can be beneficial when validating the digital evidence recovered from flight logs. Particularly, Atoms inside media files provide information related to the camera model, firmware version, and serial numbers; therefore, the analysis of media files aids in identifying possible customizations.

Anti-forensic techniques are the next challenge for responding to UAV incidents. These techniques are not limited to covering the GPS antenna with a foil but also include software-related techniques. For instance, unlocking the restricted no-fly zone, deletion of flight records, fake GPS data, etc. The author presents a proof of concept technique that could impact the integrity of the recovered unencrypted flight logs simply by using the ExifTool command-line *exiftool -xmp:gpslatitude=(value) -xmp:gpslongitude=(value)*, which results in modifying the metadata inside media files. This also applies to unencrypted flight logs such as the '.CSV' format. Therefore, it is very important to validate any recovered data from UAVs. Challenges were not limited to the analysis phase only, but also include the acquisition and reporting phases. For the acquisition phase, some scholarly research demonstrates the technical forensic analysis of UAVs via network communication protocols. However, performing these analyses when the UAV is on can result in loss of data integrity due to various possible mishaps. Therefore, the best practice is to conduct the acquisition while the UAV is off.

Hypothesis Three Testing

The hypothesis for this dimension is that *H3*: forensically sound UAV digital evidence significantly enhances the reliability of the proposed UAS Forensic Intelligence-Led taxon-

omy. To test this hypothesis, the author conducted several analysis techniques that include evaluating issues pertaining to the forensic soundness of digital evidence extracted from UAVs, 2) the evaluation of current technical UAV forensic analysis in a scholarly research article. For the first technique, the author presents technical challenges that could lead to inadmissible digital evidence. For instance, the author discusses the most important piece of digital evidence regarding UAV forensics (i.e., flight logs). In addition, the author considers possible anti-forensic and alteration techniques related to digital evidence extracted from UAVs. Some UAV models do not implement the minimum security standards such as data encryption, which impacts the data reliability and makes data vulnerable to tampering. In addition, the analysis of several flight logs was performed on two forensic workstations with a decryption software tool that is specifically for UAV data decryption and highlighted some issues that might lead to inadmissible digital evidence. Two out of the five flight logs had issues measured with the cryptographic hash algorithm (MD5) to figure out if the encrypted file is identical when decrypted twice using the same tool. Overall, for the first analysis technique, the author emphasizes on the importance of data integrity when decrypting flight logs. These results will aid in highlighting areas that might cause technical and legal issues. Also, the visualization of extracted data from UAVs might not represent the real geographical interface. For instance, most of the current software tools do not consider the representation of altitude linked to a flight trajectory.

The second phase follows a statistical approach to measure and evaluate technical challenges pertaining to the forensic soundness of UAV digital evidence. Therefore, the author used the developed UAV digital evidence metrics (see Figure 3.7) that adopts Daubert standards supported by some standards framework such as the ISO/IEC 27037, SWDGE, and the four rules of digital evidence. The author proposes a novel technique that helps in evaluating digital evidence, not only UAV digital evidence. One reason is the fact that supporting the five standards of Daubert has not been presented before.

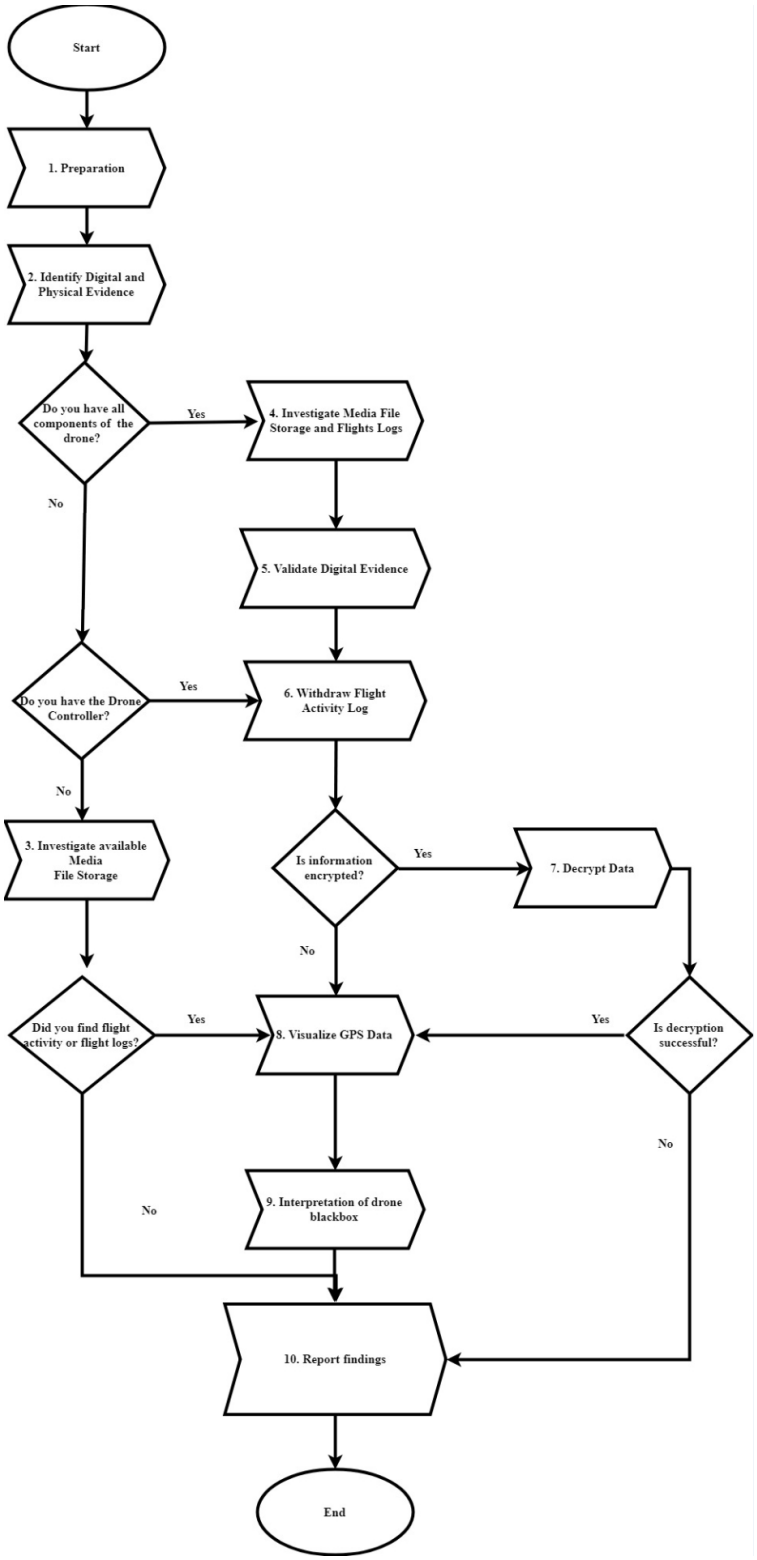


Figure 4.15. UAV Technical Forensic Investigation Framework [6]

Table 4.19.
Entered values for each scholarly article

Peer-reviewed articles	Auditable	Repeatable	Reproducible	Justifiable	Evidence Preservation	Extraction Methods	Network Isolation	Synchronization	Believability	Authenticity	Completeness	Reliability
[109]	1	0	0	1	0	0	0	1	0	0	0	0
[110]	1	0	0	0	0	0	0	0	0	0	0	0
[111]	1	1	1	1	1	1	1	1	1	1	1	1
[86]	1	0	0	0	0	0	0	0	0	0	0	0
[112]	1	1	1	1	1	1	1	1	1	1	1	1
[84]	1	0	0	0	1	1	1	1	0	0	0	0
[68]	1	1	1	1	1	1	1	1	1	1	1	1
[69]	1	1	1	1	1	1	1	1	1	1	1	1
[7]	1	1	1	1	1	1	1	1	1	1	1	1
[113]	1	1	1	1	1	1	1	1	1	1	1	1
[72]	1	0	0	0	0	0	0	1	0	0	0	0
[8]	1	1	1	1	1	1	1	0	1	1	1	1
[6]	1	1	1	1	1	1	1	0	1	1	1	1
[114]	0	0	0	0	1	1	1	0	0	0	0	0

Table 4.19 shows the populated data entered manually for each criterion. The evaluation for each article indicates if that particular article has any issues related to the soundness of the recovered digital evidence. To support the evaluation metrics and to minimize bias, the author conducted a regression analysis to determine if the count of citations predicts the total score of each article. The results indicate that there were eight articles out of the fourteen that are not forensically sound. The determined reasons will aid in the proposed taxonomy of this research, which improves future technical analysis presented in court. The reasons were very obvious and here the author is not criticizing the scholarly published articles because there are no technical requirements on scholarly articles. This means that the eight peer-reviewed articles hold valid contributions in the field; however, when following the techniques and approaches presented in these articles, the author highlights an issue that might lead to the inadmissibility of the recovered digital evidence. Most of the peer-reviewed articles that are not forensically sound share a common technical issue: the utilization of an open source tool to conduct the whole experiment. Two scholarly articles acquired data from the drone while it was on. For research purposes that could be understandable; however, it is not recommended to do live acquisition when dealing with real UAV forensic cases as this can lead to alterations to data.

The P-P plot illustrated in Figure 4.16 indicates that the data is normally distributed. This confirms the proximity of observed and expected quantities of the distributions indicating that the data were normally distributed.

A simple linear regression (SLR) was carried out to test hypothesis three. The analysis shows a significant regression ($F\ (1, 13) = 4.847$, $p = .048$), with an $R2$ of 0.288; hence, 28.8% of the variance in the probability of the citation count may be explained by the total score of the evaluation metrics (see Table 4.20). As a result, the null hypothesis was rejected for $H3$, indicating that the number of citations for each article is a significant predictor for the total score of the conducted evaluation that measures forensically sound UAV digital evidence. This implies that the outcome of this result will aid the proposed taxonomy.

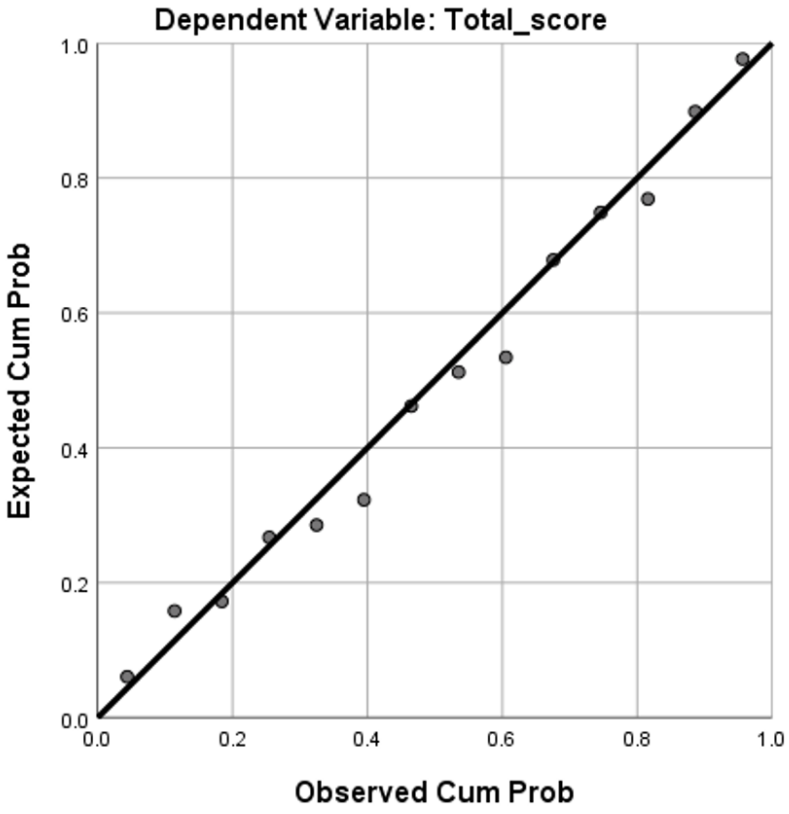


Figure 4.16. The normal P-P plot of regression standardized residual

Table 4.20.
Summary of simple regression analyses for the citation count and the total score of the evaluation metrics

Predictor	B	$SE\ B$	β
Citation Count	0.202	0.092	0.54
R^2		0.288*	
F		4.85*	

*$p < 0.05$. **$p < 0.01$.

4.4 Three Dimensional UAS Forensic Intelligence-Led Taxonomy

This research examined the importance of three important dimensions that could enhance complex forensic investigation such as UAV forensics. Since the proposed hypotheses in this research were significant by rejecting the null hypotheses, the author incorporates all findings coming from the three hypotheses to address the main research question **(How can evaluating the behavioral characteristics of UAS threat actors, self-reported techniques, and forensically sound digital evidence supplement the proposed UAS Forensic Intelligence-Led taxonomy?)**. This section introduces the reader to the proposed taxonomy and elaborates on all stages of this taxonomy.

The UAS forensic intelligence-led taxonomy illustrated in Figure 4.17 shows the classification of the three selected dimensions in this research. Behavioral analyses were conducted on the self-reported survey leading to a conclusion that categorizes each group with certain levels of personality. For instance, the tendency for UAV smugglers was predicted by antagonism and disinhibition. Also, there were significant individual differences among drone smugglers and normal drone users in neuroticism and extraversion. The results showed a significant difference between the two groups indicating that drone smugglers had a lower level of extraversion, suggesting an introverted personality trait. Looking at drone users who performed deviant activities the results indicated that users who flew around governmental buildings were predicted by antagonism, disinhibition, neuroticism, and emotional stability. Finally, the tendency for individuals who were involved in drone collision and flew in controlled airspace were predicted with the same personality traits with some differences in the level. Both groups were associated with antagonism, disinhibition, and neuroticism; whereas, the tendency for individuals who flew at high altitudes was predicted by the same traits as the two groups with an extroverted personality trait.

The second dimension (i.e., forensic investigation) deals with the technical investigative components. The important entities in this dimension were 1) the forensic layers, 2) source of evidence, 3) type of evidence, 4) forensic tools, 5) forensic models, 6) technical challenges, and 7) integrity and admissibility of evidence. This classification highlights the important components of a complete investigative approach. Also, with consideration to the current

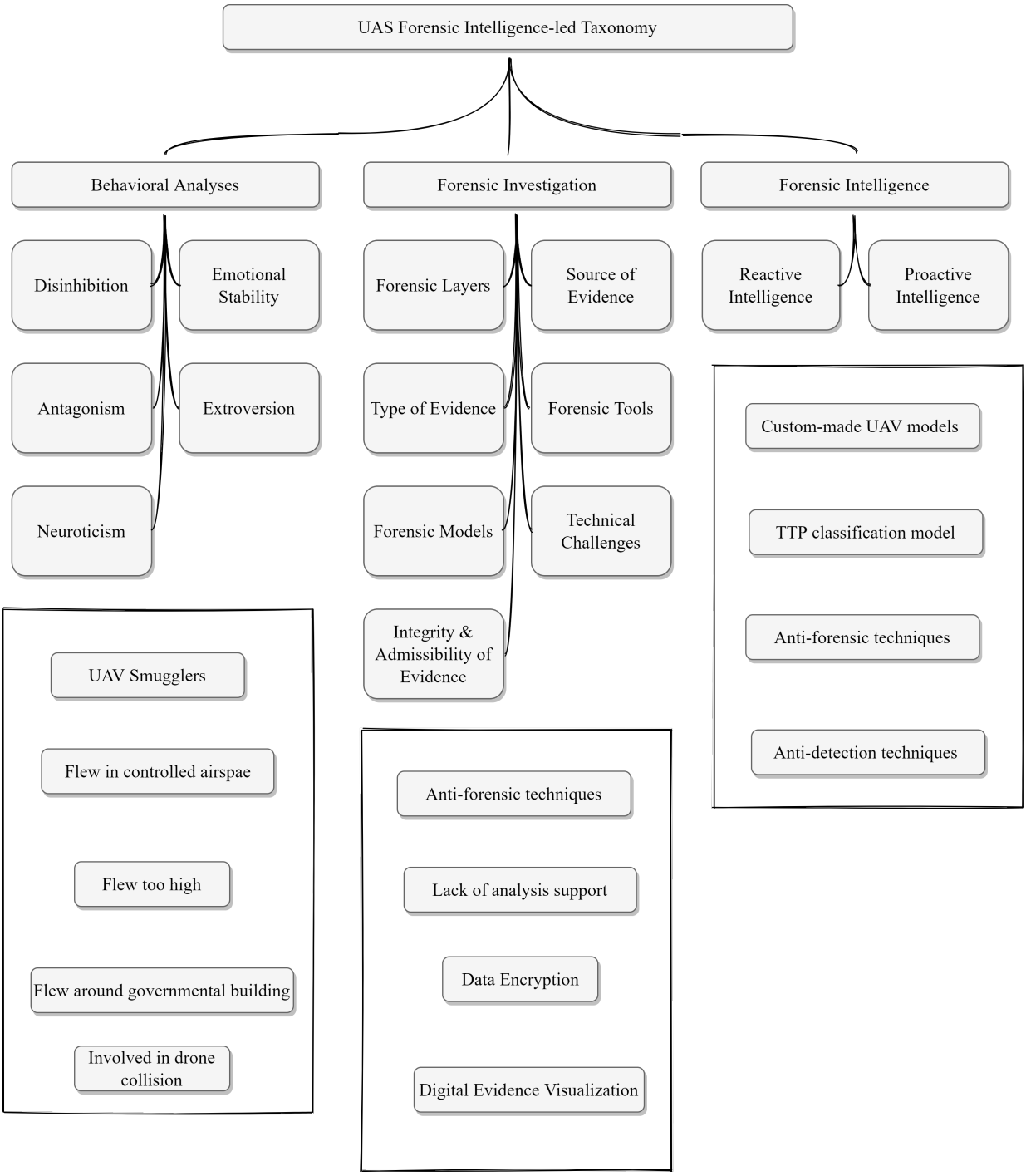


Figure 4.17. UAS forensic intelligence-led taxonomy

research in this area, the author discusses very crucial elements that are missing from a forensically sound UAV forensic investigation. For instance, technical challenges that impact the integrity of collected UAV forensic evidence were presented in this research. In addition, revisiting the currently available investigative framework was essential to highlight all of these gaps.

The final dimension deals with the intelligence component which links between the behavioral, self-reported information, and technical challenges. There are two categories of this dimension (i.e., reactive and proactive intelligence). The reactive approach involves information collected before the incident and/or during the incident, at the crime scene (see Figure 4.9). The proactive approach involves the examination of TTPs and operational behavior. The taxonomy classifies custom-made UAV models, anti-forensic techniques, and anti-detection techniques as the main pillars of the proactive approach (see Figures 4.13 and 4.16)

5. DISCUSSION AND CONCLUSION

This chapter discusses the overall results of the three hypotheses and how the conducted analyses helped to answer the main research question. The collected self-reported data helped achieve the goal of this study. The pilot study enhanced the feasibility of the full-scale study by tuning the collected information and cleaning the dataset.

The null hypotheses that were included in this study were rejected. Results from hypothesis one support the research question as to the examination of whether personality patterns of UAV smugglers and users who were involved in deviant behaviors highlight specific traits for each group that explain the variance of that particular group. Hypothesis two also supports this study by highlighting the technical challenges in the UAV forensic investigation process, which enhances the forensic soundness approach. The highlighted technical issues that were reported in this study indicate that the field has no well-defined structure because UAVs have easy accessibility, operate on different architecture and operating systems, and deploy different technologies. This is a result of the lack of tool support by the digital forensic vendors posing challenges to investigators. Finally, there is no standard reporting and visualizing of extracted evidence from UAVs. All these highlighted technical issues should help practitioners and researchers in the field. For instance, this research indicates that using the DatCon tool to decrypt flight logs extracted from a DJI model may lead to inadmissibility issues. The last hypothesis dealt with the forensic intelligence dimension. Forensic intelligence is a good enabler for complicated issues in the cyber forensic field and not only UAV forensics. Results from hypothesis three led to evaluating the self-reported information for intelligence purposes. This included a complete TTP related to UAV threat actors.

5.1 Overview Summary

This research incorporates three important dimensions by examining each dimension to supplement the proposed UAS forensic intelligence-led taxonomy. Studying the behavioral characteristics of cyber deviants is crucial to strengthen countermeasures and investigative techniques. The UAV forensics field poses many challenges to traditional digital forensics procedures. For instance, the identification of a drone pilot, the examination of the extracted

black-box, the visualization, reporting, and admissibility of recovered and analyzed digital evidence. Not only challenges related to the digital forensics field, but also cyber attack vectors, which pose another challenge to the integrity of data being analyzed. To this end, this study focuses on incorporating the three mentioned dimensions aiming to reduce complexity and empower both forensic investigation and counter UAV techniques. The anonymous self-reported study helped in learning more about different groups of actors making sure to validate their responses through a validation question. The collected data and the proposed hypothesis for the behavioral and the intelligence dimensions supported the main research question in a way that could aid the cyber threat intelligence field. The level of personality traits indicates certain emotions such as anger, embarrassment, temptation, and helplessness leading to the motivation for a crime and/or deviant action. Additionally, investigating goals, tactics, techniques, and procedures is another essential element of building a robust intelligence-led approach. Finally, highlighting technical issues pertaining to the inadmissibility of digital evidence plays a major role in advancing the field. This study successfully incorporated all three dimensions to supplement the UAV forensics field from all angles: monitoring, detection, and mitigation.

5.2 Conclusion

There exists a paucity of research in the examination of reasoning related to the use of Unmanned Aerial Vehicles among drone smugglers and deviant actions. This study incorporated three dimensions (behavioral characteristics, UAV forensics investigation, and forensic intelligence). The three selected dimensions successfully support complex cyber forensics crimes and/or deviant actions. In addition, the results of these dimensions supported the proposed UAS forensic intelligence-led taxonomy by demystifying the predicted personality traits to deviant actions and drone smugglers. The score obtained in this study was effective in distinguishing individuals based on certain personality traits. Further, a significant association between personality patterns and UAV deviant actions was found. These novel, highly distinguishing features in the behavioral personality of drone users may be of particular importance not only in the field of behavioral psychology but also in law enforcement

and intelligence. Highlighting current technical issues to the UAV forensics field contributes to the standards and procedures. Also, discussing potential TTPs related to UAV deviant actions is valuable to the field.

5.2.1 Recommendations, Limitations, and Future Work

The presented results for the behavioral dimension aid investigators, law enforcement agencies, and researchers to feed their systems with such information and make better decisions regarding threat assessment, countermeasures, and investigative plans. Taking the highlighted personality patterns into consideration of intelligence analysts is highly recommended to help in identifying unknown suspects. The results show that drone smugglers have an increased level of antagonism compared to drone deviant actions. This implies that drone smugglers could be real drug dealers who are just using a drone. By doing so, a shortlisting strategy could be followed to reduce the number of potential suspects in a given region. UAVs are remotely controlled meaning that one could pilot a drone from miles away. Also, self-reported TTPs should help counter UAV system engineers and researchers to enhance the current monitoring, detection, and mitigation algorithms and communication protocols by considering these TTPs. Deploying machine learning techniques considering the features highlighted in this research should increase the response accuracy of the counter UAV systems.

This study is not without limitations. First, participants who declined to respond to questions related to the hypotheses were excluded, reducing the sample size. Second, several biases, including selection bias and confirmation bias, may exist in this study that are not addressed. However, the sample obtained should be seen as representative of the intended population. Third, the validity of the responses was based on answering the validation question. However, the veracity and truthfulness of the responses will have to be acknowledged. Fourth, the proposed UAV digital evidence metrics do not cover legal and expert witness perspectives and can not measure the admissibility of digital evidence. Fifth, there might be other unknown UAS deviant actions that were not part of this study.

Future works could include advancing artificial intelligence counter UAV systems by deploying the highlighted challenges, TTPs, and personality patterns. The author aims to expand the targeted population by conducting the same study on normal UAV pilots to identify their level of personality traits compared to this study. Another future research study enhances the visualization, reporting, and interpretation of collected digital evidence from UAVs. In addition, the author considers building an investigative model that standardizes software tools that do not pose inadmissibility issues during an investigation. Lastly, the author would like to expand the proposed research methodology and apply it to other challenging and complex digital crimes.

REFERENCES

[1] V. Prisacariu *et al.*, "The history and the evolution of uavs from the beginning till the 70s," *Journal of Defense Resources Management (JoDRM)*, vol. 8, no. 1, pp. 181–189, 2017.

[2] P. Law, "112-95. available online at https://www. congress. gov/112/plaws/publ95/plaw-112publ95. pdf," Accessed 1/31, Tech. Rep., 2017.

[3] *Dedrone, inc.* https://www.dedrone.com/resources/incidents/all., (Accessed on 04/09/2021).

[4] *Resources & other topics*, https://www.faa.gov/uas/resources/, (Accessed on 04/09/2021).

[5] UN, *Criminal intelligence: manual for analysts*. 2011.

[6] F. E. Salamh, U. Karabiyik, and M. K. Rogers, "Rpas forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon h," *Sensors*, vol. 19, no. 15, p. 3246, 2019.

[7] A. Roder, K.-K. R. Choo, and N.-A. Le-Khac, "Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study," *arXiv preprint arXiv:1804.08649*, 2018.

[8] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "Drop (drone open source parser) your drone: Forensic analysis of the dji phantom iii," *Digital Investigation*, vol. 22, S3–S14, 2017.

[9] S. Atkinson, G. Carr, C. Shaw, and S. Zargari, "Drone forensics: The impact and challenges," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*, Springer, 2021, pp. 65–124.

[10] *Nodis library*. [Online]. Available: https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR.

[11] M. K. Rogers, K. Seigfried, and K. Tidke, "Self-reported computer criminal behavior: A psychological analysis," *digital investigation*, vol. 3, pp. 116–120, 2006.

[12] D. A. Cobb-Clark and S. Schurer, "The stability of big-five personality traits," *Economics Letters*, vol. 115, no. 1, pp. 11–15, 2012.

[13] A. Oshio, K. Taku, M. Hirano, and G. Saeed, "Resilience and big five personality traits: A meta-analysis," *Personality and Individual Differences*, vol. 127, pp. 54–60, 2018.

[14] F. Şahin, H. Karadağ, and B. Tuncer, "Big five personality traits, entrepreneurial self-efficacy and entrepreneurial intention: A configurational approach," *International Journal of Entrepreneurial Behavior & Research*, 2019.

[15] F. Leutner, G. Ahmetoglu, R. Akhtar, and T. Chamorro-Premuzic, "The relationship between the entrepreneurial personality and the big five personality traits," *Personality and individual differences*, vol. 63, pp. 58–63, 2014.

[16] K. Eriksson, P. Strimling, M. Gelfand, J. Wu, J. Abernathy, C. S. Akotia, A. Aldashev, P. A. Andersson, G. Andrighetto, A. Anum, *et al.*, "Perceptions of the appropriate response to norm violation in 57 societies," *Nature communications*, vol. 12, no. 1, pp. 1–11, 2021.

[17] E. Goode, *Deviant behavior*. Routledge, 2019.

[18] K. M. Wilson and B. F. Codding, "The marginal utility of inequality," *Human Nature*, vol. 31, no. 4, pp. 361–386, 2020.

[19] J. Dippong and C. Fitch, "Emotions in criminological theory: Insights from social psychology," *Sociology compass*, vol. 11, no. 4, e12473, 2017.

[20] O. P. Stepanova, S. V. Gridneva, P. V. Menshikov, G. . Kassymova, O. V. Tokar, A. P. Merezhnikov, and M. R. Arpentieva, "Value-motivational sphere and prospects of the deviant behavior," *International journal of education and information technologies. ISSN*, pp. 2074–1316, 2018.

[21] N. V. Vist, "Psychological and pedagogical conditions for the prevention of deviant behavior among adolescents.," *International Journal of Environmental and Science Education*, vol. 11, no. 15, pp. 8536–8551, 2016.

[22] J. R. Lilly, F. T. Cullen, and R. A. Ball, *Criminological theory: Context and consequences*. Sage publications, 2018.

[23] A. Ronaldi, "Criminological theories introduction, evaluation and application," *Los Angeles, CA: Roxbury Publication*, vol. 129, 2004.

[24] K. C. Seigfried-Spellar, N. Villacís-Vukadinović, and D. R. Lynam, "Computer criminal behavior is related to psychopathy and other antisocial behavior," *Journal of Criminal Justice*, vol. 51, pp. 67–73, 2017.

[25] K. C. Seigfried-Spellar and M. K. Rogers, "Low neuroticism and high hedonistic traits for female internet child pornography consumers," *Cyberpsychology, Behavior, And Social Networking*, vol. 13, no. 6, pp. 629–635, 2010.

[26] F. Sudzina and A. Pavlicek, "Virtual offenses: Role of demographic factors and personality traits," *Information*, vol. 11, no. 4, p. 188, 2020.

[27] S. M. Albladi and G. R. Weir, "Personality traits and cyber-attack victimisation: Multiple mediation analysis," in *2017 Internet of Things Business Models, Users, and Networks*, IEEE, 2017, pp. 1–6.

[28] M. J. Turner, "An investigation of big five personality and propensity to commit white-collar crime," in *Advances in accounting behavioral research*, Emerald Group Publishing Limited, 2014.

[29] D. R. Lynam and T. A. Widiger, "Using a general model of personality to identify the basic elements of psychopathy," *Journal of personality disorders*, vol. 21, no. 2, pp. 160–178, 2007.

[30] T. Widiger, "Five factor model rating form (ffmrf)," *Retrieved May*, vol. 19, p. 2009, 2004.

[31] R. D. Hare, "Hare psychopathy checklist (pcl-r)," MHS, 2003.

[32] S. Lilienfeld and M. Widows, "Professional manual for the psychopathic personality inventory-revised (ppi-r)," *Lutz, FL: Psychological Assessment Resources*, 2005.

[33] M. R. Levenson, K. A. Kiehl, and C. M. Fitzpatrick, "Assessing psychopathic attributes in a noninstitutionalized population.," *Journal of personality and social psychology*, vol. 68, no. 1, p. 151, 1995.

[34] R. D. Hare, "Comparison of procedures for the assessment of psychopathy.," *Journal of Consulting and Clinical psychology*, vol. 53, no. 1, p. 7, 1985.

[35] J. Suler, "The online disinhibition effect," *Cyberpsychology & behavior*, vol. 7, no. 3, pp. 321–326, 2004.

[36] T. A. Widiger and D. R. Lynam, "Development and validation of the super-short form of the elemental psychopathy assessment katherine l. collison joshua d. miller b eric t. gaughan c,"

[37] S. J. Semple, S. A. Strathdee, T. Volkmann, J. Zians, and T. L. Patterson, ""high on my own supply": Correlates of drug dealing among heterosexually identified methamphetamine users," *The American Journal on Addictions*, vol. 20, no. 6, pp. 516–524, 2011.

[38] T. A. Widiger and P. T. Costa Jr, *Personality disorders and the five-factor model of personality*. American Psychological Association, 2013.

[39] B. P. O'Connor, "A quantitative review of the comprehensiveness of the five-factor model in relation to popular personality inventories," *Assessment*, vol. 9, no. 2, pp. 188–203, 2002.

[40] K. C. Seigfried-Spellar, C. L. O'Quinn, and K. N. Treadway, "Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students," *Behaviour & Information Technology*, vol. 34, no. 5, pp. 533–542, 2015.

[41] E. Abdalla-Filho and B. Völlm, "Does every psychopath have an antisocial personality disorder?" *Brazilian Journal of Psychiatry*, vol. 42, no. 3, pp. 241–242, 2020.

[42] R. J. R. Blair, "Neurobiological basis of psychopathy," *The British Journal of Psychiatry*, vol. 182, no. 1, pp. 5–7, 2003.

[43] K. Schneider, "Clinical psychopathology.(trans. by mw hamilton)," 1959.

[44] R. Blackburn, "Personality disorder and antisocial deviance: Comments on the debate on the structure of the psychopathy checklist-revised," *Journal of personality disorders*, vol. 21, no. 2, pp. 142–159, 2007.

[45] D. T. Lykken, *The antisocial personalities*. Psychology Press, 1995.

[46] J. R. Ogloff, R. E. Campbell, and S. M. Shepherd, "Disentangling psychopathy from antisocial personality disorder: An australian analysis," *Journal of Forensic Psychology Practice*, vol. 16, no. 3, pp. 198–215, 2016.

[47] R. D. Hare, "Psychopathy and antisocial personality disorder: A case of diagnostic confusion," *Psychiatric times*, vol. 13, no. 2, pp. 39–40, 1996.

[48] R. L. Craig, N. S. Gray, and R. J. Snowden, "Recalled parental bonding, current attachment, and the triarchic conceptualisation of psychopathy," *Personality and Individual Differences*, vol. 55, no. 4, pp. 345–350, 2013.

[49] A. Diagnostic, "Statistical manual of mental disorders,(dsm-5) washington," *DC: Author*, 2013.

[50] D. J. Simourd and R. D. Hoge, "Criminal psychopathy: A risk-and-need perspective," *Criminal Justice and Behavior*, vol. 27, no. 2, pp. 256–272, 2000.

[51] V. M. Gonsalves, M. J. Scalora, and M. T. Huss, "Prediction of recidivism using the psychopathy checklist—revised and the psychological inventory of criminal thinking styles within a forensic sample," *Criminal Justice and Behavior*, vol. 36, no. 7, pp. 741–756, 2009.

[52] D. Mitchell and R. C. Tafrate, "Conceptualization and measurement of criminal thinking: Initial validation of the criminogenic thinking profile," *International Journal of Offender Therapy and Comparative Criminology*, vol. 56, no. 7, pp. 1080–1102, 2012.

[53] S. J. Riopka, R. Coupland, and M. E. Olver, "Self-reported psychopathy and its association with criminal cognition and antisocial behavior in a sample of university undergraduates.," *Canadian Journal of Behavioural Science/Revue canadienne des sciences du comportement*, vol. 47, no. 3, p. 216, 2015.

[54] J. D. Miller, S. E. Jones, and D. R. Lynam, "Psychopathic traits from the perspective of self and informant reports: Is there evidence for a lack of insight?" *Journal of Abnormal Psychology*, vol. 120, no. 3, p. 758, 2011.

[55] G. Oatley, B. Chapman, and J. Speers, "Forensic intelligence and the analytical process," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 3, e1354, 2020.

[56] R. Milne, *Forensic intelligence*. CRC Press, 2012.

[57] J. Tang, J. Ostrander, R. Wickenheiser, and A. Hall, "Touch dna in forensic science: The use of laboratory-created eccrine fingerprints to quantify dna loss," *Forensic Science International: Synergy*, vol. 2, pp. 1–16, 2020.

[58] W. Parson, "Age estimation with dna: From forensic dna fingerprinting to forensic (epi) genomics: A mini-review," *Gerontology*, vol. 64, no. 4, pp. 326–332, 2018.

[59] W. C. Thompson and N. Scurich, "How cross-examination on subjectivity and bias affects jurors' evaluations of forensic science evidence," *Journal of forensic sciences*, vol. 64, no. 5, pp. 1379–1388, 2019.

[60] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Generation Computer Systems*, vol. 110, pp. 758–771, 2020.

[61] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The future of digital forensics: Challenges and the road ahead," *IEEE Security & Privacy*, vol. 15, no. 6, pp. 12–17, 2017.

[62] O. Ribaux, S. J. Walsh, and P. Margot, "The contribution of forensic science to crime analysis and investigation: Forensic intelligence," *Forensic science international*, vol. 156, no. 2-3, pp. 171–181, 2006.

[63] M. K. Rogers, "Psychological profiling as an investigative tool for digital forensics," in *Digital Forensics*, Elsevier, 2016, pp. 45–58.

[64] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2016.

[65] T. E. A. Barton and M. H. B. Azhar, "Open source forensics for a multi-platform drone system," in *International Conference on Digital Forensics and Cyber Crime*, Springer, 2017, pp. 83–96.

[66] A. Irons and H. S. Lallie, "Digital forensics to intelligent forensics," *Future Internet*, vol. 6, no. 3, pp. 584–596, 2014.

[67] INTERPOL, *FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT*. 2020. [Online]. Available: https://www.interpol.int/en.

[68] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *2017 IEEE Sensors Applications Symposium (SAS)*, IEEE, 2017, pp. 1–6.

[69] F. E. Salamh, U. Karabiyik, M. Rogers, and F. Al-Hazemi, "Drone disrupted denial of service attack (3dos): Towards an incident response and forensic analysis of remotely piloted aerial systems (rpass)," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, 2019, pp. 704–710.

[70] M. K. Rogers and K. Seigfried, "The future of computer forensics: A needs analysis survey," *Computers & Security*, vol. 23, no. 1, pp. 12–16, 2004.

[71] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro air vehicle link (mavlink) in a nutshell: A survey," *IEEE Access*, vol. 7, pp. 87 658–87 680, 2019.

[72] M. Azhar, T. E. A. Barton, and T. Islam, "Drone forensic analysis using open source tools," *Journal of Digital Forensics, Security and Law*, vol. 13, no. 1, p. 6, 2018.

[73] F. E. Salamh, U. Karabiyik, and M. Rogers, "A constructive direst security threat modeling for drone as a service," *Journal of Digital Forensics, Security and Law*, vol. 16, no. 1, p. 2, 2021.

[74] A. Tăbuşcă and G.-E. Garais, "Iot and the flying answer to covid-19," *Journal of Information Systems & Operations Management*, pp. 162–173, 2020.

[75] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 218–223, 2017.

[76] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 619–641, 2013.

[77] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Radionavigation laboratory conference proceedings*, 2008.

[78] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza, and V. Guizilini, "The impact of dos attacks on the ar. drone 2.0," in *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)*, IEEE, 2016, pp. 127–132.

[79] G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: A survey," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, 2018, pp. 560–565.

[80] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for aodv," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, 2003, pp. 125–134.

[81] V. Vaidya, *Dynamic signature inspection-based network intrusion detection*, US Patent 6,279,113, 2001.

[82] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[83] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, "A hybrid intrusion detection system design for computer network security," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 517–526, 2009.

[84] A. L. S. Renduchintala, A. Albehadili, and A. Y. Javaid, "Drone forensics: Digital flight log examination framework for micro drones," in *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, 2017, pp. 91–96.

[85] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (uav/drone) forensic framework," *Digital Investigation*, vol. 30, pp. 52–72, 2019.

[86] F. Iqbal, B. Yankson, M. A. AlYammahi, N. AlMansoori, S. M. Qayed, B. Shah, and T. Baker, "Drone forensics: Examination and analysis," *International Journal of Electronic Security and Digital Forensics*, vol. 11, no. 3, pp. 245–264, 2019.

[87] İ. Gülataş and S. Baktır, "Unmanned aerial vehicle digital forensic investigation framework," *Journal of Naval Sciences and Engineering*, vol. 14, no. 1, pp. 32–53, 2018.

[88] A. Antwi-Boasiako and H. Venter, "A model for digital evidence admissibility assessment," in *IFIP International Conference on Digital Forensics*, Springer, 2017, pp. 23–38.

[89] B. Carrier *et al.*, "Defining digital forensic examination and analysis tools using abstraction layers," *International Journal of digital evidence*, vol. 1, no. 4, pp. 1–12, 2003.

[90] M. Hannan, S. Frings, V. Broucek, and P. Turner, "Forensic computing theory and practice: Towards developing a methodology for a standardised approach to computer misuse," PhD thesis, Edith Cowan University, 2003.

[91] S. McCombie and M. Warren, "Computer forensic: An issue of definitions," in *Australian Computer, Network & Information Forensics Conference (1st: 2003)*, 2003.

[92] R. McKemmish, "When is digital evidence forensically sound?" In *IFIP international conference on digital forensics*, Springer, 2008, pp. 3–15.

[93] B. Smith, "Ontology," in *The furniture of the world*, Brill Rodopi, 2012, pp. 47–68.

[94] T. Gruber, "Ontology.," *Encyclopedia of database systems*, vol. 5, p. 3748, 2009.

[95] K. D. Bailey, *Typologies and taxonomies: An introduction to classification techniques*, 102. Sage, 1994.

[96] J. Hair, W. Black, B. Babin, and R. Anderson, "Multivariate data analysis: A global perspective . new jersey: Pearson prentice hall," 2010.

[97] N. Cliff, *Analyzing multivariate data.* Harcourt Brace Jovanovich, 1987.

[98] J. Pallant, "Spss survival guide," *Crow's Nest, NSW: Allen & Unwin*, 2005.

[99] V. Patil, S. Singh, S. Mishra, and D. Donavan, *Parallel analysis engine to aid in determining number of factors to retain using r [computer software]*, 2017.

[100] S. E. Jones, J. D. Miller, and D. R. Lynam, "Personality, antisocial behavior, and aggression: A meta-analytic review," *Journal of Criminal Justice*, vol. 39, no. 4, pp. 329–337, 2011.

[101] K. W. Reardon, J. L. Tackett, and D. Lynam, "The personality context of relational aggression: A five-factor model profile analysis.," *Personality Disorders: Theory, Research, and Treatment*, vol. 9, no. 3, p. 228, 2018.

[102] C. E. Vize, K. L. Collison, J. D. Miller, and D. R. Lynam, "Using bayesian methods to update and expand the meta-analytic evidence of the five-factor model's relation to antisocial behavior," *Clinical psychology review*, vol. 67, pp. 61–77, 2019.

[103] S. Maghsoodloo, A. Ghodousi, and T. Karimzadeh, "The relationship of antisocial personality disorder and history of conduct disorder with crime incidence in schizophrenia," *Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences*, vol. 17, no. 6, p. 566, 2012.

[104] P. Moran and S. Hodgins, "The correlates of comorbid antisocial personality disorder in schizophrenia," *Schizophrenia bulletin*, vol. 30, no. 4, pp. 791–802, 2004.

[105] D. B. Garrie, "Digital forensic evidence in the courtroom: Understanding content and quality," *Nw. J. Tech. & Intell. Prop.*, vol. 12, p. i, 2014.

[106] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "A comparative uav forensic analysis: Static and live digital evidence traceability challenges," *Drones*, vol. 5, no. 2, 2021, ISSN: 2504-446X. DOI: 10.3390/drones5020042. [Online]. Available: https://www.mdpi.com/2504-446X/5/2/42.

[107] E. Casey, "Digital evidence in the courtroom," *Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet*, 2011.

[108] V. Mitova, *Believable evidence*. Cambridge University Press, 2017.

[109] E. Mantas and C. Patsakis, "Gryphon: Drone forensics in dataflash and telemetry logs," in *International Workshop on Security*, Springer, 2019, pp. 377–390.

[110] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone forensics: Challenges and new insights," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2018, pp. 1–6.

[111] M. Yousef and F. Iqbal, "Drone forensics: A case study on a dji mavic air," in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, 2019, pp. 1–3.

[112] F. Iqbal, S. Alam, A. Kazim, Á. MacDermott, *et al.*, "Drone forensics: A case study on dji phantom 4," in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, 2019, pp. 1–6.

[113] D.-Y. Kao, M.-C. Chen, W.-Y. Wu, J.-S. Lin, C.-H. Chen, and F. Tsai, "Drone forensic investigation: Dji spark drone as a case study," *Procedia Computer Science*, vol. 159, pp. 1890–1899, 2019.

[114] S. E. Prastya, I. Riadi, and A. Luthfi, "Forensic analysis of unmanned aerial vehicle to obtain gps log data as digital evidence," *IJCSIS*, vol. 15, no. 3, 2017.

A. APPENDICES

]

PURDUE
UNIVERSITY

This Memo is Generated From the Purdue University Human Research Protection Program System, Cayuse IRB **.**

Date: January 21, 2020
PI: KATHRYN SEIGFRIED-SPELLAR
Department: PWL COMPUTER INFO & TECH
Re: Initial - IRB-2019-787
Survey of Drone Operators' Attitudes

The Purdue University HRPP/IRB has approved an exemption for your study " *Survey of Drone Operators' Attitudes*" via limited IRB review. The administrative check-in date is **January 20, 2023**. The IRB must be notified when this study is closed.
If a study closure request has not been initiated by this date, the HRPP will request study status update for the record.

Specific notes related to your study are below.
Decision: Exempt - Limited IRB
Category: Category 3.(i). Research involving benign behavioral interventions in conjunction with the collection of information from an adult subject through verbal or written responses (including data entry) or audiovisual recording if the subject prospectively agrees to the intervention and information collection and at least one of the following criteria is met:

(C) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review to make the determination required by §46.111(a)(7).

"**Attitudes Towards Drone Users Behavior**"

Fahad E Salamh, PhD student
Dr. Kathryn Seigfried-Spellar
Dr. Marcus Rogers
Computer & Information Technology, Purdue University

Key Information

Please take time to review this information carefully. This is a research study. Your participation in this study is voluntary, which means that you may choose not to participate at any time without penalty or loss of benefits to which you are otherwise entitled. You may ask questions to the researchers about the study whenever you would like. If you decide to take part in the study, you will be asked to sign this form. Be sure you understand what you will do and any possible risks or benefits.

What is the purpose of this study? The purpose of this study is to examine individual differences among drone users.

What will I do if I choose to be in this study? The anonymous online survey will be administered using a secure website. Once you have read this consent form, and agree to voluntarily participate, you will be taken to a secure website to complete the online survey. You may withdraw from the survey at any time and you may skip or decline any questions that you do not wish to answer. There will be a validation question that requires a force response from participants; therefore, entering an incorrect response will result in preventing you from completing the survey, and result in no compensation.

How long will I be in the study? Most people take about 30 minutes to complete the survey.

What are the possible risks or discomforts? The risks to you are minimal. They are not greater than those ordinarily encountered in daily life. Please know that this is an anonymous survey that uses a secure link.

The survey is anonymous because we will not be able to link your responses back to you – we do not ask for any identifiable information (Ex. name). While completing the survey, the only risk to you might be if someone were to see your responses to the survey, so we recommend that you take this survey when you have complete privacy. Since the survey is anonymous, no one will know that you completed this survey unless you personally tell him or her, so breach of confidentiality is a risk and the safeguards used to minimize this risk can be found in the confidential section below.

This survey has a number of questions embedded in it as validity checks to insure that you are not a robot and are in fact fully reading and answering each question. A unique combination of answers to those questions may result in your survey being rejected.

Are there any potential benefits? There are no direct benefits to you. Eventually, we hope to publish the research results, and if you want to see them, you should send an email requesting information to the Principal Investigator at kspellar@purdue.edu.

Will I receive payment or other incentive? After completing the study, you will be compensated $.50 for your time via the anonymous payment system set up through Mechanical Turk. Participants will not be compensated if they are screened out during the early on in the survey.

Will information about me and my participation be kept confidential? We do not ask for your name or any other information that could be used to identify you at any time before, during, or after the survey. No IP addresses will be recorded. There will be no way to determine where the survey was taken or by whom. Instead, the survey software will randomly assign an ID number to your responses. This means that the responses to the questionnaires cannot be linked or matched to you, which means your responses will remain completely

anonymous. Only researchers associated with this study will have access to the data. In addition to the data being anonymous, it will be stored electronically in an encrypted format. The encrypted data will be kept indefinitely and will be used only for research purposes.

What are my rights if I take part in this study? Your participation in this study is voluntary. You may choose not to participate or, if you agree to participate, you can withdraw your participation at any time without penalty or loss of benefits to which you are otherwise entitled.

Who can I contact if I have questions about the study? If you have questions, comments or concerns about this research project, you can talk to one of the researchers. Please contact Dr. Kathryn Seigfried-Spellar at 765-494-2439. If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to:
Human Research Protection Program - Purdue University
Ernest C. Young Hall, Room 1032
155 S. Grant St.,
West Lafayette, IN 47907-2114

Documentation of Informed Consent. I have had the opportunity to read this consent form and have the research study explained. I have had the opportunity to ask questions about the research study, and my questions have been answered. I am prepared to participate in the research study described above. If I wish, I may print this form for my records. If you agree, please click on the "Agree" button below. Otherwise, we thank you for your time and ask that you click on the "Disagree" button.

Agree | Disagree

Demographic

What is your gender?

- ○ Male
- ○ Female
- ○ Non-Binary
- ○ Decline to respond

What is your current age?

Ethnic origin: Please specify your ethnicity.

- ○ African American
- ○ Asian
- ○ Hispanic or Latino
- ○ Native American
- ○ Native Hawaiian or Pacific Islander
- ○ Middle Eastern
- ○ White
- ○ Other
- ○ Decline to answer

What is the highest degree or level of school you have completed?

- ○ Less than high school diploma/GED

- ○ High school diploma or GED
- ○ Associate degree
- ○ Bachelor's degree
- ○ Master's degree
- ○ Doctorate degree
- ○ Decline to answer

- ☐ A student
- ☐ Employed (Full Time)
- ☐ Employed (Part Time)
- ☐ Looking for work
- ☐ Retired
- ☐ Self-employed
- ☐ Decline to answer

DroneQuestions

I am currently a .....

- ○ Drone user
- ○ Non-drone user
- ○ Decline to answer

Are you a certified drone pilot? (For example, FAA PART 107 certificate)

- ○ No
- ○ Yes
- ○ I do not need certification to fly. Please explain..

- ○ Decline to answer

Do you own a registered drone?

- ○ Yes, my drone is registered through the FAA for Commercial use
- ○ Yes, my drone is registered through the FAA for Recreational use
- ○ Yes, my drone is registered but not through FAA. Please explain..

- ○ No, I do not need to register my drone. Please explain..

- ○ Decline to answer

I use drones for ..... [check all that apply]

- ☐ Aerial Photography
- ☐ Agriculture & Farming
- ☐ Aerial Delivery & Shipping
- ☐ Commercial, Industrial & Construction
- ☐ Entertainment & Light Shows
- ☐ Filming and Movies
- ☐ Fire Fighting
- ☐ Hunting
- ☐ Medical & Emergency
- ☐ News & Journalism
- ☐ Racing & Sports
- ☐ Recreational, Hobby & Fun
- ☐ Search and Rescue Operations
- ☐ Sensory & Inspection
- ☐ Surveying
- ☐ Other (please specify)

How would you describe yourself in terms of drone use? [check all that apply]

- ☐ FPV Racer
- ☐ Gear Nerd
- ☐ Legal Nerd
- ☐ Newbie
- ☐ Photographer
- ☐ Scientist
- ☐ Tech Nerd
- ☐ Veteran
- ☐ Decline to answer
- ☐ Other (please specify)

I use .....

- ○ Customized drones
- ○ Commercial drones
- ○ Both (Customized & Commercial) drones
- ○ Decline to answer
- ○ Other (please specify)

I know how to disable the functionality of No Drone Zone (NFZ) restrictions.

- ○ No
- ○ Yes
- ○ Decline to answer

- ○ Other (please specify)

Have you ever been involved in a drone incident (For example, operating an aircraft non-compliant with safety laws)?

- ○ No
- ○ Yes
- ○ Decline to answer
- ○ Other (please specify)

Which of the following best describes your incidents relating to the use of drones? [check all that apply]

- ☐ Flew a drone over the airfield
- ☐ Flew a drone too high (e.g: above 300 feet or 400 feet) [note: this depends on regulatory by country]
- ☐ Flew a drone up close to government buildings
- ☐ Drone collision (e.g: personal injuries, plan crashes, or property damage)
- ☐ Decline to answer
- ☐ Other (please specify)

- ○ No
- ○ Yes
- ○ Decline to answer

Have you ever used drone for smuggling activities? (For example, transport drugs or prison contraband)

- ○ No
- ○ Yes
- ○ Decline to answer

What is the make/model of the drone you fly?

Neuroticism versus Emotional Stability

Please describe yourself on a 1 to 5 scale on each of the following traits, where 1 is extremely low (i.e., extremely lower than the average person), 2 is low, 3 is neither high nor low (i.e., does not differ from the average person), 4 is high and 5 is extremely high. Use any number from 1 to 5.

1= Extremely Low **2**= Low **3** = Neither high nor low **4** = High **5**= Extremely high

	1	2	3	4	5	
(relaxed, unconcerned, cool)	○	○	○	○	○	(fearful, apprehensive)
(even-tempered)	○	○	○	○	○	(angry, bitter)
(optimistic)	○	○	○	○	○	(pessimistic, glum)
(self-assured, glib, shameless)	○	○	○	○	○	(timid, embarrassed)
(controlled, restrained)	○	○	○	○	○	(tempted, urgency)
(clear-thinking, fearless, unflappable)	○	○	○	○	○	(helpless, fragile)

Extraversion versus Introversion

Please describe yourself on a 1 to 5 scale on each of the following traits, where 1 is extremely low (i.e., extremely lower than the average person), 2 is low, 3 is neither high nor low (i.e., does not differ from the average person), 4 is high and 5 is extremely high. Use any number from 1 to 5.

1=Extremely Low **2** = Low **3** = Neither high nor low **4** = High **5**= Extremely high

	1	2	3	4	5	
(cold, aloof, indifferent)	○	○	○	○	○	(cordial, affectionate, attached)
(withdrawn, isolated)	○	○	○	○	○	(sociable, outgoing)
(unassuming, quiet, resigned)	○	○	○	○	○	(dominant, forceful)
(passive, lethargic)	○	○	○	○	○	(vigorous, energetic, active)
(cautious, monotonous, dull)	○	○	○	○	○	(reckless, daring)
(placid, anhedonic)	○	○	○	○	○	(high-spirited)

Openness versus Closeness

Please describe yourself on a 1 to 5 scale on each of the following traits, where 1 is extremely low (i.e., extremely lower than the average person), 2 is low, 3 is neither high nor low (i.e., does not differ from the average person), 4 is high and 5 is extremely high. Use any number from 1 to 5.

1=Extremely Low **2** = Low **3** = Neither high nor low **4** = High **5**= Extremely high

	1	2	3	4	5	
(practical, concrete)	○	○	○	○	○	(dreamer, unrealistic, imaginative)
(uninvolved, no aesthetic interests)	○	○	○	○	○	(aberrant interests, aesthetic)
(constricted, unaware, alexythymic)	○	○	○	○	○	(self-aware)
(routine, predictable, habitual, stubborn)	○	○	○	○	○	(unconventional, eccentric)
(pragmatic, rigid)	○	○	○	○	○	(strange, odd, peculiar, creative)
(traditional, inflexible, dogmatic)	○	○	○	○	○	(permissive, broad-minded)

Agreeableness versus Antagonism

Please describe yourself on a 1 to 5 scale on each of the following traits, where 1 is extremely low (i.e., extremely lower than the average person), 2 is low, 3 is neither high nor low (i.e., does not differ from the average person), 4 is high and 5 is extremely high. Use any number from 1 to 5.

1=Extremely Low **2** = Low **3** = Neither high nor low **4** = High **5**= Extremely high

	1	2	3	4	5	
(skeptical, cynical, suspicious, paranoid)	○	○	○	○	○	(gullible, naïve, trusting)
(cunning, manipulative, deceptive)	○	○	○	○	○	(confiding, honest)
(stingy, selfish, greedy, exploitative)	○	○	○	○	○	(sacrificial, giving)

(oppositional, combative, aggressive)	○ ○ ○ ○ ○	(docile, cooperative)
(confident, boastful, arrogant)	○ ○ ○ ○ ○	(meek, self-effacing, humble)
(tough, callous, ruthless)	○ ○ ○ ○ ○	(soft, empathetic)

Validation

Below are a number of items related to activities involving your free time. Please select only the fourth item ("knitting"), despite whatever activities you might favor most. This is to verify that you are a human and not a test-taking robot.

Incorrect responses will result in the survey exiting and you will not receive a payment code for Mechanical Turk. Random responses will also exit you from the study.

What activity do you engage in the most in your free time?

- ○ Playing sports
- ○ Reading
- ○ Shopping
- ○ Knitting
- ○ Swimming
- ○ Traveling

Conscientiousness versus Undependability

Please describe yourself on a 1 to 5 scale on each of the following traits, where 1 is extremely low (i.e., extremely lower than the average person), 2 is low, 3 is neither high nor low (i.e., does not differ from the average person), 4 is high and 5 is extremely high. Use any number from 1 to 5.

1=Extremely Low **2** = Low **3** = Neither high nor low **4** = High **5**= Extremely high

	1 2 3 4 5	
(lax, negligent)	○ ○ ○ ○ ○	(perfectionistic, efficient)
(haphazard, disorganized, sloppy)	○ ○ ○ ○ ○	(ordered, methodical, organized)
(casual, undependable, unethical)	○ ○ ○ ○ ○	(rigid, reliable, dependable)
(aimless, desultory)	○ ○ ○ ○ ○	(workaholic, ambitious)
(hedonistic, negligent)	○ ○ ○ ○ ○	(dogged, devoted)

(hasty, careless, rash) ○ ○ ○ ○ ○ (cautious, ruminative, reflective)

Antagonism

Please read each item carefully and select the answer that best corresponds to your agreement or disagreement. If you strongly disagree select **1**, if you disagree selects **2**, if you neither agree nor disagree select **3**, if you agree select **4**, and if you strongly agree select **5**.

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
I deserve special treatment.	○	○	○	○	○
I care a lot about my relationships with others.	○	○	○	○	○
Feeling sorry for others is a sign of weakness.	○	○	○	○	○
When someone does something nice for me, I wonder what they want from me.	○	○	○	○	○
People would say I am a reliable and dependable person.	○	○	○	○	○
I quit things pretty easily.	○	○	○	○	○
I could make a living as a con artist.	○	○	○	○	○
I have more important things to worry about than other people's feelings.	○	○	○	○	○

Disinhibition

Please read each item carefully and select the answer that best corresponds to your agreement or disagreement. If you strongly disagree select **1**, if you disagree selects **2**, if you neither agree nor disagree select **3**, if you agree select **4**, and if you strongly agree select **5**.

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
My temper has gotten me into trouble.	○	○	○	○	○
I am known as a bit of a rebel.	○	○	○	○	○
"Act first, think later," describes me well.	○	○	○	○	○
I like doing things that are risky or dangerous.	○	○	○	○	○
When I'm upset, I will do things I later regret.	○	○	○	○	○

Emotional Stability

Please read each item carefully and select the answer that best corresponds to your agreement or disagreement. If you strongly disagree select **1**, if you disagree selects **2**, if you neither agree nor disagree select **3**, if you agree select **4**, and if you strongly agree select **5**.

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
I am a bit of a worrier.	○	○	○	○	○
I'm not the type to get depressed about the things I've done wrong.	○	○	○	○	○
I remain cool, calm, and collected when things get stressful.	○	○	○	○	○
I often emerge as the leader in a group.	○	○	○	○	○
I'm pretty comfortable when meeting new people.	○	○	○	○	○

DS3-Mach

Please read each item carefully and select the answer that best corresponds to your agreement or disagreement. If you strongly disagree select **1**, if you disagree selects **2**, if you neither agree nor disagree select **3**, if you agree select **4**, and if you strongly agree select **5**.

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
It's not wise to tell your secrets.	○	○	○	○	○
Generally speaking, people won't work hard unless they have to.	○	○	○	○	○
Whatever it takes, you must get the important people on your side.	○	○	○	○	○
Avoid direct conflict with others because they may be useful in the future.	○	○	○	○	○
It's wise to keep track of information that you can use against people later.	○	○	○	○	○
You should wait for the right time to get back at people.	○	○	○	○	○
There are things you should hide from other people because they don't need to know.	○	○	○	○	○

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
Make sure your plans benefit you, not others.	○	○	○	○	○
Most people can be manipulated.	○	○	○	○	○

DS3-Narcissism

Please read each item carefully and select the answer that best corresponds to your agreement or disagreement. If you strongly disagree select **1**, if you disagree selects **2**, if you neither agree nor disagree select **3**, if you agree select **4**, and if you strongly agree select **5**.

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
People see me as a natural leader.	○	○	○	○	○
Many group activities tend to be dull without me.	○	○	○	○	○
I hate being the center of attention.	○	○	○	○	○
I know that I am special because everyone keeps telling me so.	○	○	○	○	○
I like to get acquainted with important people	○	○	○	○	○
I feel embarrassed if someone compliments me.	○	○	○	○	○
I have been compared to famous people.	○	○	○	○	○
I am an average person.	○	○	○	○	○
I insist on getting the respect I deserve	○	○	○	○	○

DS3-Psy

Please read each item carefully and select the answer that best corresponds to your agreement or disagreement. If you strongly disagree select **1**, if you disagree selects **2**, if you neither agree nor disagree select **3**, if you agree select **4**, and if you strongly agree select **5**.

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
I like to get revenge on authorities	○	○	○	○	○

	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
I avoid dangerous situations.	O	O	O	O	O
Payback needs to be quick and nasty.	O	O	O	O	O
People often say I'm out of control.	O	O	O	O	O
It's true that I can be mean to others.(or I enjoy having sex with people I hardly know.)	O	O	O	O	O
People who mess with me always regret it.	O	O	O	O	O
I have never gotten into trouble with the law.	O	O	O	O	O
I like to pick on losers.	O	O	O	O	O
I'll say anything to get what I want	O	O	O	O	O

VITA

Fahad E. Salamh

EDUCATION

- Doctor of Philosophy in Technology (Cyber Forensics) Purdue University, West Lafayette, IN, Graduated in 2021
- Master's degree in Digital Forensics and Incident Response, University of Central Florida, FL, Graduated in 2015
- Bachelor's Degree in Cyber Defense and Information Security, Tiffin University, OH, Graduated in 2014

ACADEMIC EMPLOYMENT

- Graduate Research Assistant, Department of Computer and Information Technology, Purdue University, August 2019 - present. Research activities include cybersecurtiy, C-UAS and DFIR projects.
- Graduate Teaching Assistant, Department of Computer and Information Technology, Purdue University, Jan 2021 - May 2021. Responsibilities include: assisting professors with the preparation and presentation of graduate courses, grading, and tutoring.

PUBLICATION

- RPAS forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon H FE Salamh, U Karabiyik, MK Rogers Sensors 19 (15), 3246
- Drone disrupted denial of service attack (3DOS): Towards an incident response and forensic analysis of remotely piloted aerial systems (RPASs) FE Salamh, U Karabiyik, M Rogers, F Al-Hazemi 2019 15th International Wireless Communications Mobile Computing

- An Android Case Study on Technical Anti-Forensic Challenges of WhatsApp Application MM Mirza, FE Salamh, U Karabiyik 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1-6
- Asynchronous forensic investigative approach to recover deleted data from instant messaging applications FE Salamh, U Karabiyik, MK Rogers 2020 International Symposium on Networks, Computers and Communications
- A Constructive DIREST Security Threat Modeling for Drone as a Service FE Salamh, U Karabiyik, M Rogers Journal of Digital Forensics, Security and Law 16 (1), 2
- UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies FE Salamh, MM Mirza, U Karabiyik Electronics 10 (6), 733
- UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. Electronics 2021, 10, 733 FE Salamh, MM Mirza, U Karabiyik
- Unmanned Aerial Vehicle Kill Chain: Purple Teaming Tactics FE Salamh, U Karabiyik, MK Rogers, ET Matson 2021 IEEE 11th Annual Computing and Communication Workshop and Conference
- A Forensic Analysis of Home Automation Devices (FAHAD) Model: Kasa Smart Light Bulb and Eufy Floodlight Camera as Case Studies FE Salamh International Journal of Cyber Forensics and Advanced Threat Investigations
- Automating digital forensic evidence collection MK Rogers, FE Salamh, U Karabiyik US Patent App. 17/006,154
- A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges FE Salamh, U Karabiyik, MK Rogers, ET Matson Drones 5 (2), 42

PROFESSIONAL MEMBERSHIP

- AAFS Member Affiliate – The American Academy of Forensic Science
- TC Affiliate Member of IEEE - Information Forensics and Security

- TPC Member of ISDFS – The International Symposium on Digital Forensics and Security
- TPC Member of IWUAS – The International Workshop on Unmanned Aircraft Systems
- Production co-editor- The Journal of Digital Forensics, Security, and Law (JDFSL).
- Member, Quality Teaching committee, 2017 — 2018
- Member, Job Hiring committee, 2017 — 2018
- Member, Computer Forensics Certifications Committee, 2017 — 2018

AWARDS and ACHIEVEMENTS

- My team was awarded 1" among five hundred cyber security specialists in a National Cyber Security Contest March 2017. (Best defended report on Shaman analysis)