drones

MDPI

Article

A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges †

Fahad E. Salamh *, Umit Karabiyik, Marcus K. Rogers and Eric T. Matson

Department of Computer and Information Technology, Purdue University, West Lafayette, IN 47907, USA; umit@purdue.edu (U.K.); rogersmk@purdue.edu (M.K.R.); ematson@purdue.edu (E.T.M.)

* Correspondence: fsalamh@purdue.edu

† This paper is an extended version of our paper published in Salamh, F. E., Karabiyik, U., Rogers, M. K. and Matson, E. T. (2021, January). Unmanned Aerial Vehicle Kill Chain: Purple-Teaming Tactics. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1081–1087). IEEE.

Abstract: The raising accessibility of Unmanned Aerial Vehicles (UAVs), colloquially known as drones, is rapidly increasing. Recent studies have discussed challenges that may come in tow with the growing use of this technology. These studies note that in-depth examination is required, especially when addressing challenges that carry a high volume of software data between sensors, actuators, and control commands. This work underlines static and live digital evidence traceability challenges to further enhance the UAV incident response plan. To study the live UAV forensic traceability issues, we apply the 'purple-teaming' exercise on small UAVs while conducting UAV forensic examination to determine technical challenges related to data integrity and repeatability. In addition, this research highlights current static technical challenges that could pose more challenges in justifying the discovered digital evidence. Additionally, this study discusses potential drone anti-forensic techniques and their association with the type of use, environment, attack vector, and level of expertise. To this end, we propose the UAV Kill Chain and categorize the impact and complexity of all highlighted challenges based on the conducted examination and the presented scientific contribution in this work. To the best of our knowledge, there has not been any contribution that incorporates 'Purple-Teaming' tactics to evaluate UAV-related research in cybersecurity and digital forensics. This work also proposes a categorization model that classifies the discovered UAV static and live digital evidence challenges based on their complexity and impact levels.

Keywords: UAV forensic; Kill Chain; digital evidence traceability; data integrity; technical issues; comparative model

Citation: Salamh, F.E.; Karabiyik, U.; Rogers, M.K.; Matson, E.T. A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges. *Drones* **2021**, *5*, 42. https://doi.org/10.3390/drones5020042

Academic Editor: Diego González-Aguilera

Received: 29 April 2021
Accepted: 18 May 2021
Published: 21 May 2021

1. Introduction

The future uses of UAVs include border security, coastguard, forest fires, emergency rescue, oil industry, environmental monitoring, aerial photography, and surveying [1]. UAVs' safety functionality is considered an essential factor to the principles of cybersecurity (i.e., Confidentiality, Integrity, Availability, and Safety). The use of flying devices has created challenges to many countries, including challenges relating to policies and regulation, software development, security issues, and a lack of detection and monitoring technologies.

Adversarial tactics related to the use of UAVs have created more challenges to the drone Incident Response (IR) process. There are several detection systems to counter UAVs, and the lessons learned from UAV incidents allow for continuous improvement on the detection and prevention measures. Critical infrastructures such as airfields, prisons, and borders have encountered a massive number of UAV incidents during the past three years. The UK Airprox Board has conducted an assessment on a Small Unmanned Air System (SUAS), including drones, balloons, model aircraft, and unknown objects (e.g., birds). As illustrated in Figure 1, it is estimated that the number of publicly reported drone incidents in 2019 was about 91 incidents [2]. These incidents are limited to the description provided

by airplane pilots. Drone incidents count for about more than 80% compared to the other three classified categories (i.e., balloons, model craft, and unknown objects).

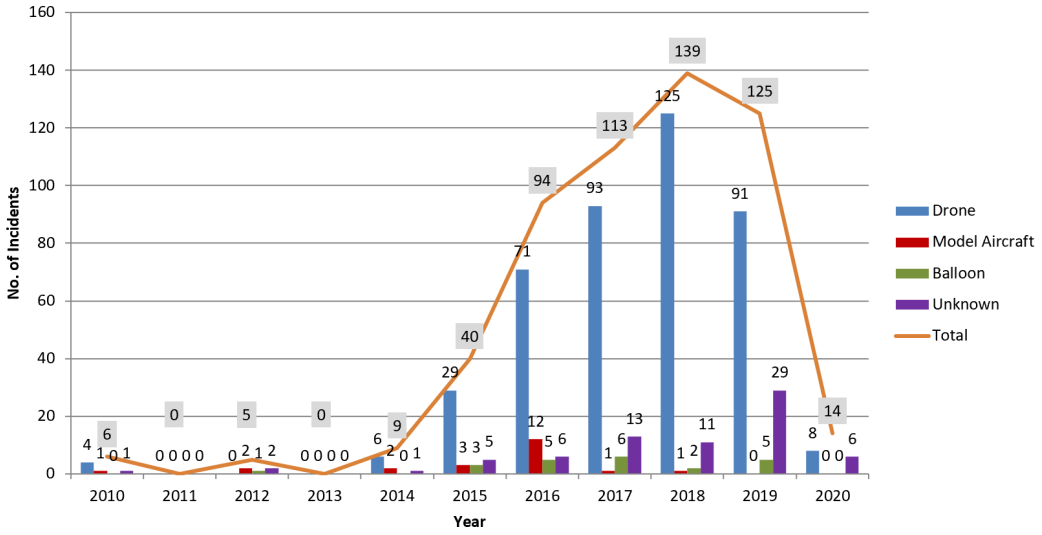

Figure 1. UK Airprox board assessment on a Small Unmanned Air System (SUAS) [2].

Some Commercial off the shelf (COTS) drones deploy a software restriction based on the No Fly Zone (NFZ) policy; however, unlocking the NFZ restriction has become an online service. This attack vector poses many challenges not only to the drone forensic process and examination, but also the detection, monitoring, and mitigation of attacks. Researchers in [3] proposed a fully autonomous system as a counter UAV solution supported with a net designed to safely capture the targeted UAS. Alternatively, lateral movement of drone attack can impact both the detection and IR processes if Command and Control (C&C) sent customized requests to erase or alter all digital evidence from Unmanned Aerial System (UAS). A new approach is therefore needed to address the following questions:

1. What type of challenges are present in the forensic discovery process that depend on the method of attack or intrusion?
2. How do technical forensic challenges impact the forensic soundness of digital evidence recovered from UAVs?
3. How do different attack scenarios change the potential ability to discover tractability or evidence?
4. What are the main identifiable factors of evidence and how can this be simulated in a red team or blue team scenario?

In this paper, security challenges related to the use of drones and digital evidence traceability challenges are discussed. The contributions of this paper include:

- A 'Purple-Teaming' exercise performed on a commercial off-the-shelf UAV.
- Discussing possible Anti-UAV forensic techniques based on the conducted experiments.
- Proposing a Kill Chain for UAVs.
- Highlighting the technical challenges pertaining to the decryption of digital evidence recovered from UAVs.

This paper is structured as follows: Section 2 discusses the earlier studies regarding UAVs cyber threats, IDS, and IR. Section 3 explores the methodology used in this paper. Section 4 presents the 'Purple-Team' scenario and UAV forensic challenges (i.e., this includes static and live approaches). Section 5 discusses the overall contributions and limitations of this work. Finally, Section 6 concludes this paper with directions of future research .

2. Literature Review

Drone cyber threats were categorized into four classes including confidentiality and privacy, integrity, availability, and authenticity, while each class contains a certain type of attack [4]. For instance, confidentiality and privacy of data transmitted via UAVs are essential to avoid traffic analysis, data alteration, and eavesdropping. Simultaneously, Denial of Service (DoS) and jamming attacks impact the drone operations.

In a recent work [5], researchers have proposed a threat model for UAVs. The proposed model consists of application and link risks, accessibility risks, perceptional risks, and data security risks. The model highlights the important factors in this research. For instance, identifying the accessibility risks (i.e., insecure file systems, weak credentials, and network services) are very crucial when operating a UAV. In addition, researchers [5] discussed the importance of securing live data streaming and communication protocols to minimize the intrusion risk.

Alternatively, an operational overview of the UAV Intrusion Detection System (IDS) has been proposed to enhance security requirements [6]. The proposed IDS is based on specifications [7], signatures [8], anomaly behaviors [9], and hybrid [10]. The selection method is based on specific rules generated to monitor the UAS behavior, while the signature method is executed on known cryptographic hash functions. The hybrid mechanism requires incorporating at least two of the aforementioned methods, for instance, combining anomaly detection and signature based IDS. These methods are identical to the traditional IDS; however, UASs consist of a large number of components (i.e., sensors and communication links).

Automating security assessment is vital for the advancement of drone technology, especially with the rapidly increasing use of drones and the implementation of Drone as a Service (DaaS). A Hierarchical Context Aware Aspect-Oriented Petri Net (HCAPN) model was proposed by researchers in [11]. The model's objective is to detect potential vulnerabilities based on drone behavior evaluation. Alternatively, the deployment of onboard and external IDSs to prevent attacks on the security principals of cybersecurity, namely, confidentiality, integrity, and availability, has been presented in [12–14]. Prior researchers [12,13] concentrated more on detecting abnormal flight patterns indicating an unauthorized change of flight trajectory such as GPS spoofing, and structural failure, while the work presented in [14] deployed a combination of IDS techniques combining both rule and anomaly-based detection.

Drones connected to the Internet are transforming the fourth industrial revolution to meet the requirements of the cyber physical system revolution. The development and deployment of the Internet of Drones (IoD) enhance smart mobility, public safety communications, air traffic control, logistics tracking, along with medical, military, and environmental applications [15]. Securing the implementation of IoD requires extensive risk assessment and continuous traffic monitoring, as the operation will mostly depend on network communication. This would increase the number of cyber threats because enabling long-range wireless connectivity results in more chances to perform a reconnaissance attack. Authors in [15] introduce a new type of attack to the IoD taxonomy called the firmware replacement attack. This is not the case with off-the-shelf drones as they operate on multiple low range communication protocols (i.e., Radio Frequency and Wireless Local Area Network (WLAN)); however, a firmware replacement attack is considered as a cyber threat to small drones when manufacturers make firmware publicly available. This may lead to potential malware injection and the distribution of the fake version of the firmware to drone users.

Maldrone (known as hijacking attack) is another potential security threat to UAVs [16], which may be performed by executing a malicious code into the drone to take over control. This indicates the necessity of revisiting traditional security measures as the maldrone attack has been successful for the AR Parrot type drone. Therefore, comprehensive security measures need to be addressed based on a threat's level of priority [17].

It has been identified that there are three types of cyber-physical attackers with different capabilities, including revelation, knowledge, and disruption [18]. Researchers claim that any attack-targeted UAVs should accomplish one or more of the three capabilities because revelation deals with intercepting unencrypted data, knowledge refers to the reconnaissance technique (i.e., information gathering and fingerprinting), and disruption signifies the ability of an adversary to deny the UAS operation [19]. Researchers in [19] also claim that the process of UAV forensic investigations is unclear due to the complexity of data flow and UAS architecture. While there has been a fair amount of recent work in the area of UAV forensic investigations [20,21], challenges related to drone forensics are still ongoing. One major factor is system architecture, related software components, and data flow mechanisms. Researchers in [5] developed a DIREST threat assessment model to enhance the security of flying devices through the consideration of three layers of data flow. These emphasize the importance of amending the firmware update mechanism.

On the other hand, researchers have demonstrated technical issues related to the traceability of digital evidence [22]. The highlighted issues are associated with current forensic software tools and their capability in performing the analysis without compromising the forensic soundness of the recovered digital evidence. One example claimed by the researchers is that some forensic software tools do not meet the minimum technical requirements (i.e., do not guarantee reproducibility). In this work, we dig deep into investigating the technical issues by examining the outcome of the well-known flight log extractor (DatCon [23]). Examining DatCon will aid in clarifying any technical issues and bring them to the attention of UAV forensic investigators. Our concerns center around what could happen if a drone is hacked and its data are altered, or if two investigators work on the same case and fail to uphold their integrity of the collected digital evidence. Furthermore, it is important to mention that the DatCon app is widely used on most digital forensic tools. For this reason, it is important to evaluate and report any technical issues linked to the app to improve the forensic soundness of UAV related investigations.

An interesting work by [24] compared the architecture of five selected commercial drones to highlight software incompatibility when replacing certain pieces of hardware component (e.g., gimbal, LED, propellers, etc.). This work holds a valuable contribution to UAV forensic investigators to identify anti-forensic techniques; however, there are several other advanced techniques through software and/or network protocols that pose complicated challenges in the field of UAV forensics.

3. Methodology

We aim to address the research questions presented in Section 1 by performing a Proof of Concept (POC). The first selected methodology in this work is the 'purple-teaming' technique, which is a combination of *'red'* and 'blue' activities by performing processes such as planning, assessment, collaboration, remediation, and reporting [25]. These actions include penetration testing (i.e., vulnerability assessment), risk mitigation measures, and IR. However, our approach in this paper is considered as a 'Non-Traditional Purple-Teaming' (NTPT) technique due to the complexity of UAS architecture and data flow. To this end, the proposed UAV Kill Chain can be deployed and expanded on other emerging technologies. In addition, the second approach is to investigate the technical issues related to the traceability of digital evidence and evaluate the integrity of current digital forensic tools when dealing with UAV forensic analysis. Discussing the performance of digital forensic tools is out of the scope of this research, since we are only concerned with the decryption process of recovered flight logs in the '.DAT' format.

Our research aims to address the research questions by investigating the consequences resulting from the conducted investigation on UAVs. The selected scenario for the 'purple-teaming' exercise includes a Windows 10 laptop running Kali Linux subsystem, Vivitar VTI Phoenix drone, encrypted flight logs from DJI Matrice 210 [26]. We performed an indoor simulation and analysis of VTI Phoenix by scanning the network of the drone and fingerprinting its system. Table 1 shows the details about the selected tools to perform

the analysis. Eighteen encrypted flight logs were selected from the DJI Matrice 210 to test and evaluate forensic tools in performing the analysis. As a side note, small UAVs do not usually deploy any encryption on flight logs and they have smaller flight endurance compared to the DJI Matrice 210. Our goal is to present a POC of the selected attack vectors which can be performed on any other small UAVs that deploy the same technology and specs (i.e., WLAN pairing). This research investigated the encrypted flight logs that are usually recovered from mid-size drones. This is a crucial intersection that aids in enhancing the UAV forensic investigation tools and techniques. Therefore, this paper discusses the association, impact, and complexity of the highlighted technical forensic issues and the presented POC.

Table 1. A set of tools used to conduct the 'purple-teaming exercises'.

Purpose	Software Tool	Version
Fingerprinting	Nmap	7.80
Network Sniffing	Wireshark	3.2.4
Gain Access	Metasploit Framework	5.0
Escalation of Privilege (install and modify data)	Kali Linux Commands	2020.2

The main purpose of the scenario was to eavesdrop the unsecured WLAN and intercept the network connection, then commence the fingerprinting phase to discover weaknesses related to the system that can move us to the next phase. A demonstration of the general setup of the experiment is illustrated in Figure 2.

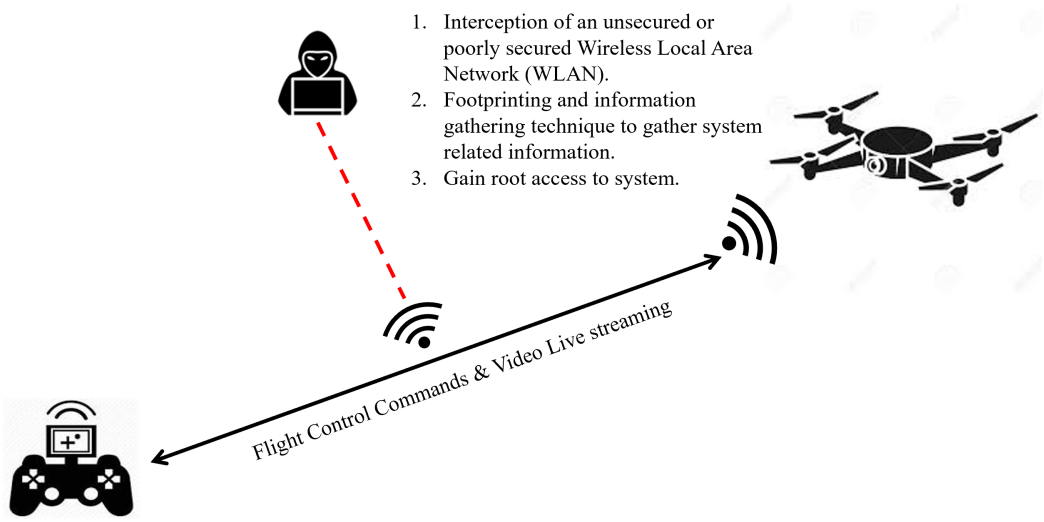

Figure 2. Scenario layout.

In our experiment, different stages of penetrating testing were performed; starting with:

- Reconnaissance and Scanning,
- Gaining Access,
- Maintaining Access, and
- Clearing Tracks

These are the traditional phases of hacking; however, a slight modification to the procedure might be different regarding UAVs due to the lack of proper security measures.

The process involves connecting the laptop with the unsecured WLAN Phoenix Dronexxxx of the drone and monitoring generated traffic between the drone and remote control. Connecting to a WiFi signal with no authentication is considered a major security issue,

in addition to the use of unencrypted communication protocols. As a result, the Network Mapper (Nmap) scan was performed to get further details about open protocols. Exploiting a vulnerability in the system is the next step using the Metasploit framework to gain access to the system as a root user. All traffic was monitored in the hopes of detecting the abnormal behavior on the network.

4. Findings

During the course of our research, our experiment was successful as a POC to the current security status of UAVs. Not all available drones share common security weaknesses; however, the work presented here illustrates the comprehensible impact of drone security.

4.1. 'Purple-Teaming' Exercise

In this work, the Nmap scan provided more details about the network communication protocols. Several insecure network services were discovered leading to insecure transmission of data between the drone and its remote control. Figure 3 shows open protocols and services related to drone IP Cameras.

```
Nmap scan report for 192.168.99.1
Host is up (0.015s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 21.48 seconds
```

Figure 3. Drone Nmap network scanning output.

The IP Camera reveals a number of vulnerabilities that can be simply exploited and result in a lateral movement attack. Accordingly, the Metasploit framework available in Kali Linux was used to perform the exploitation via open services, such as Telnet `port 23` and `File Transfer Protocol (FTP), port 21`. Telnet is an application protocol that provides a bidirectional interactive test communication, while FTP is responsible for file transmission. The connection to FTP did not require any form of authentication (i.e., username and password) allowing access to data and creating the opportunity for uploading malicious files. The attempt to basically telnet into the server requires authentication. In this case, a *Brute Force* attack was performed to get the login conditionals through telnet. Figures 4 and 5 show the payload creation and the successful BF attack that were able to crack the login username and password.

```
msf5 auxiliary(scanner/telnet/telnet_version) > use auxiliary/scanner/telnet/telnet_version
msf5 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.99.1
rhosts => 192.168.99.1
msf5 auxiliary(scanner/telnet/telnet_version) > set rport 23
rport => 23
msf5 auxiliary(scanner/telnet/telnet_version) > set threads 5
threads => 5
msf5 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.99.1:23       - 192.168.99.1:23 TELNET anyka login:
[*] 192.168.99.1:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 4. Msfconsole payload generator.

```
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat1111 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat1110 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat110dog624 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat1108 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat110788 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat110682 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat1105 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat10b (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat109 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat106 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat1051990 (Incorrect: )
[-] 192.168.99.1:23       - 192.168.99.1:23 - LOGIN FAILED: root:cat103020 (Incorrect: )
[+] 192.168.99.1:23       - 192.168.99.1:23 - Login Successful: root:cat1029
[*] 192.168.99.1:23       - Attempting to start session 192.168.99.1:23 with root:cat1029
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.99.1:23) at 2020-07-31 03:46:13 -0400
```

Figure 5. Telnet brute force attack.

Telnet login conditionals were login: root and password: cat1029. Network traffic during these phases was captured and not encrypted. The captured traffic provided synchronous digital evidence related to the payload and BF attacks, but the question remains, What about an asynchronous approach to responding to such an attack? Logging into telnet revealed data related to the system and escalation of privileges would not be an issue to the attacker. Stealing and tampering with data would be another issue as well. Root access leads to many system files such as mounted USB devices, script updates, WiFi connections, and configuration files. Protocols such as Telnet and FTP should be replaced with more secure protocols such as Secure SHell (SSH).

Another interesting open network service was the `Real Time Streaming Protocol (RTSP)`, which is used to control streaming media in an unencrypted format. It is recommended to use the `Secure RTP (SRTP)` over `Transport Layer Security (TLS)`, which minimize the chance for cyber threats such as replay and DoS attacks.

The proposed IoD framework [15] is essential to keep live monitoring of network intrusions between the RC and UAV. Moreover, techniques such as the proposed IDS are based on specifications [7], signatures [8], anomaly behaviors [9], and hybrid [10] would enhance the overall detection system when it comes to DaaS development.

As mentioned earlier, UASs operate based on different technologies and specifications. This results in a serious problem regarding generating a unified security framework. Therefore, this problem was tackled by applying the 'purple-teaming' technique (i.e., combining 'red team' and 'blue team' techniques. The presented techniques resulted in a slight modification to the traditional Cyber Kill Chain. The proposed UAV Kill Chain should be applicable to other types of drones that use the same technology of the UAV models covered in this research.

Network communication-based intrusions require pre-configured sensors to perform anomaly detection for prevention purposes. Consequently, there are other security threats related to drone use that need to be appropriately researched. During our experiment, network packets related to the brute force attack were captured as shown in Figure 6.

This type of attack is mostly prevented with advanced network intrusion detection. In regard to the UAV network, intrusion attacks require live monitoring of traffic, including automated detection systems. The captured traffic did not report any traceable evidence that identify the suspect because the captured TCP packets during all attacking phases show hosts related to the drone subnet (e.g., **192.168.99.xxx**). Flying devices should be equipped with IDS that can log and capture communication traffic and software events. Evidence traceability is a critical feature as it requires 'live data acquisition' and 'live monitoring.' These functions would even enhance the reliability and integrity of digital evidence.

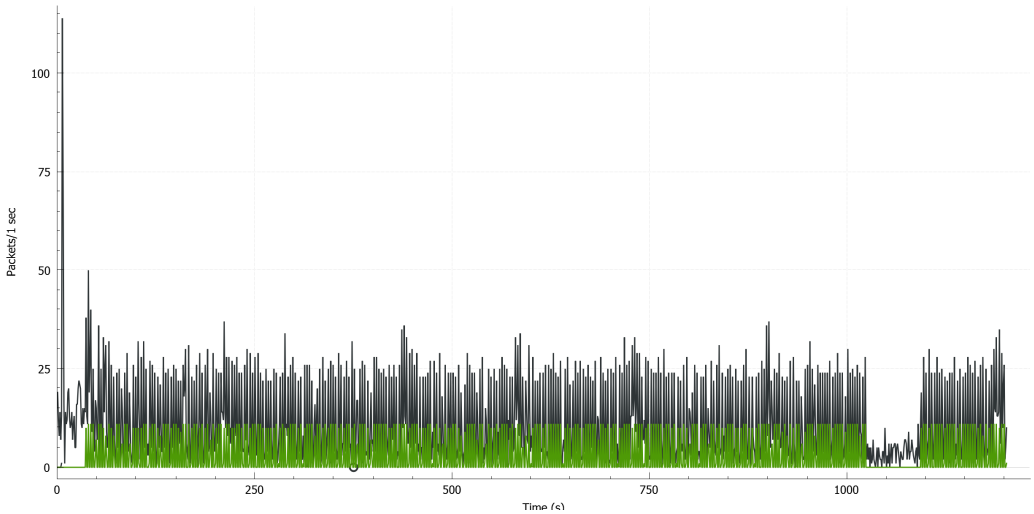

Figure 6. Brute force attempts showing packet dropping at 1000 s.

In addition, a new folder was created on the drone file system (see Figure 7). This means that escalating privileges would enable an attacker to read, create, and modify system files.

```
ftp> mkdir ThisIsAnewFolder
257 Operation successful
ftp> ls
200 Operation successful
150 Directory listing
drwxr-xr-x    2 root     root            0 Jan  1 00:08 ThisIsAnewFolder
drwxr-xr-x    2 1001     1003            0 Dec 10  2019 bin
drwxr-xr-x    2 1001     1003            0 Dec 10  2019 lib
drwxr-xr-x    2 1001     1003            0 Dec 10  2019 local
drwxr-xr-x    2 1001     1003            0 Dec 10  2019 modules
drwxr-xr-x    2 1001     1003            0 Dec 10  2019 sbin
drwxr-xr-x    3 1001     1003            0 Dec 10  2019 share
226 Operation successful
```

Figure 7. Access and create files and/or folders without permission.

This research demonstrates the importance of securing data at rest, in motion, and in use. Communication links are another security concern that should be ciphered to bolster the integrity of data. Firmware is an example of a lower level software that needs to be secured and encrypted. The firmware update mechanism should follow best practices to avoid software related threats during the UAV's operation. In general, it is highly recommend to log communication, traffic and software events to determine the cause of an incident. After the root cause of an attack is discovered, the defensive technique becomes much more effective and durable.

The results of our experiments have led us to propose a UAV Kill Chain model, as shown in Figure 8. Martin's Cyber kill chain is a restructured model that best fits cyber attacks [27]. A slight modification to the model was considered to best fit the UAV's attack structure. The UAV Kill Chain consists of eight important phases. These phases are essential to UAV security operations, especially when defining each phase based on the purpose and use of drones. However, the proposed kill chain should be a minimum UAV security practice.

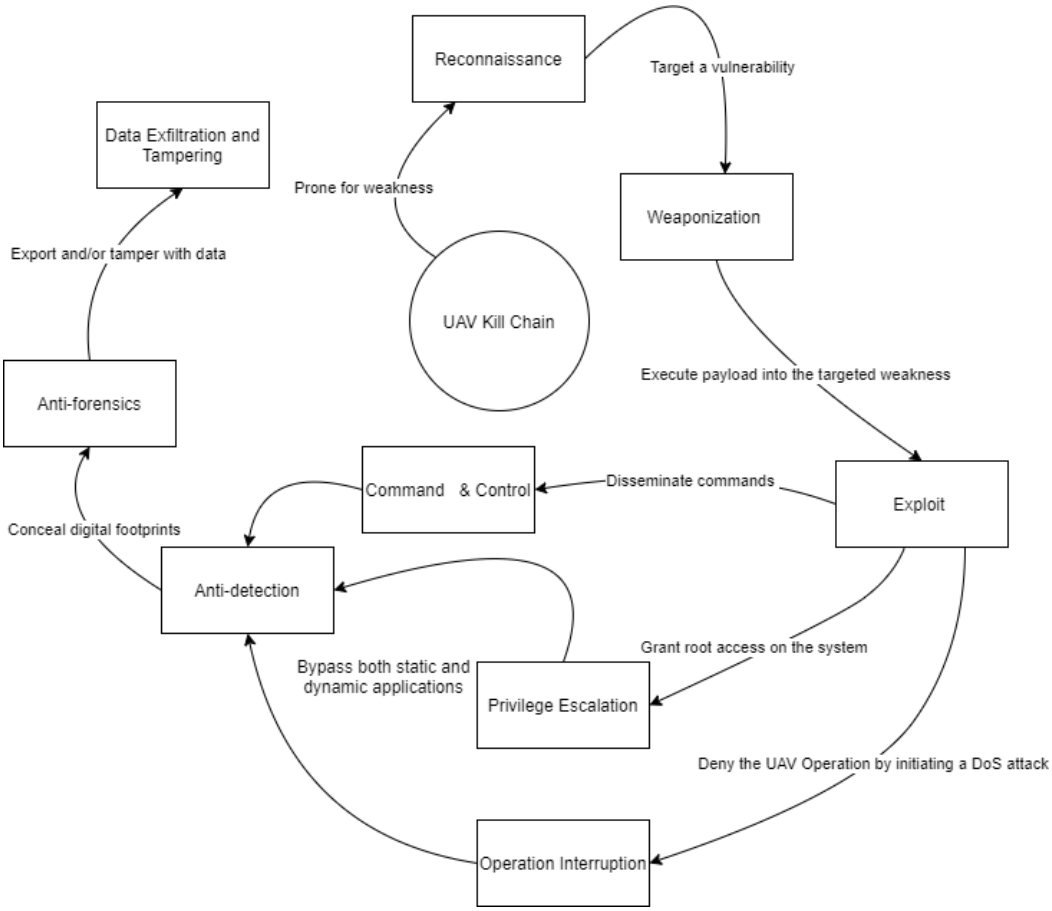

Figure 8. UAV Kill Chain.

As illustrated in Figure 8, the UAV Kill Chain goes through the following phases:

- **R**econnaissance to probe for weakness.
- **W**eaponization to target a vulnerability that can be exploited.
- **E**xploit to execute the payload into the targeted weakness.
- **P**rivilege escalation to grant root access to the systems.
- **O**peration Interruption to deny the service by initiating DoS or buffer overflow attacks.
- **A**nti-detection to bypass both static and dynamic applications
- **A**nti-forensics to conceal digital footprints and mislead forensic investigators in recovering the true digital evidence.
- **D**ata Exfiltration & tampering to export data or attempt to alter metadata.
- **C**ommand & **C**ontrol: to disseminate commands for different purposes (i.e., DDoS and Botnet).

The 'Purple-Teaming' technique was the selected approach in this research, which is why an evaluation based on security metrics is illustrated in Table 2 to clarify potential gaps in the UAV attack life-cycle. Our research findings suggest that detection of Operation Interruption and Command & Control is considered as a major challenge to UAV security. The admissibility of digital evidence requires certain elements and standards to be met, such as the validity and integrity of the recovered evidence. UAS data flow does not trace identifiable evidence due to the following factors:

- Communication protocols transmit data in motion, which keeps software related logs with no identifiable information.
- Physical factors might lead to a better discovery of evidence because the current use of commercial drones is digitally semi-anonymous.
- The investment battle and cheap development in an emerging technology result in less secure systems where they do not meet minimum security requirements.

- Lack of third party monitoring services for UAVs.
- Challenges related to UAS customization.

All of these factors play a major challenge in the field of UAV security and forensics; therefore, nontraditional solutions must be considered. For instance, the laptop used in this experiment can lead to admissible evidence, yet there were zero trace routes from the drone components that could identify the device that originated these attacks.

Mapping attack vectors with software generated data could enhance the automated detection methodology for UAVs. There are many recorded operating system and sensor events such as satellite signals and the three axes of flight (i.e., yaw, roll, and pitch). These system events could identify and distinguish unexpected software failures from suspicious behavior. In addition, an adaptive security for UAV flight management is another vital layer in responding to some attack vectors, such as GPS spoofing. The deployment of adaptive and automated mapping of software events might aid in automating the IR process.

Table 2. Attack life-cycle and purple-teaming evaluation.

Evaluation/Attack Lifecycle	Detection	Prevention	Response
Reconnaissance	✓	✓	✓
Weaponization	✓	N/A	✓
Delivery	✓	✓	✓
Exploitation	✓	N/A	✓
Privilege Escalation	✓	N/A	✓
Operation Interruption	X	✓	✓
Anti-detection & Anti-forensic	✓	✓	✓
Data Exfiltration & Tempering	✓	✓	✓
Command & Control	X	✓	✓

4.2. Discovery and Evaluation of UAV Forensic Technical Issues

This research categorizes the identified technical issues from both cyber security and digital forensics' perspectives. The technical challenges presented in Figure 9 illustrate the level of complexity and impact that each technical issue has on digital evidence traceability. The selected approach in highlighting these technical challenges is based on the validation and testing of the impact that each technical challenge poses to the field. For instance, blue colored challenges represent technical issues that directly impact the digital evidence traceability, whereas red colored challenges signify the impact and complexity of digital evidence traceability from a cybersecurity perspective. Technical issues might result from an attack vector [28], insecure communication protocols [5,28], data tampering [20], and data encryption [21]. On the contrary, the technical challenges associated with digital evidence traceability are related to software tools that do not fully support certain UAV models [22], meet the forensic soundness standards, report digital evidence [22], examine the file structure with high accuracy, and do not clearly interpret data and labeling. Although measuring the impact level of each technical challenge is important, the scale in categorizing each technical challenge is either high impact and high complexity, high impact and low complexity, high complexity and low impact, or low complexity and low impact. This research does not measure the variability of the highlighted technical challenges as it requires an in-depth examination that include surveying experts in the field.

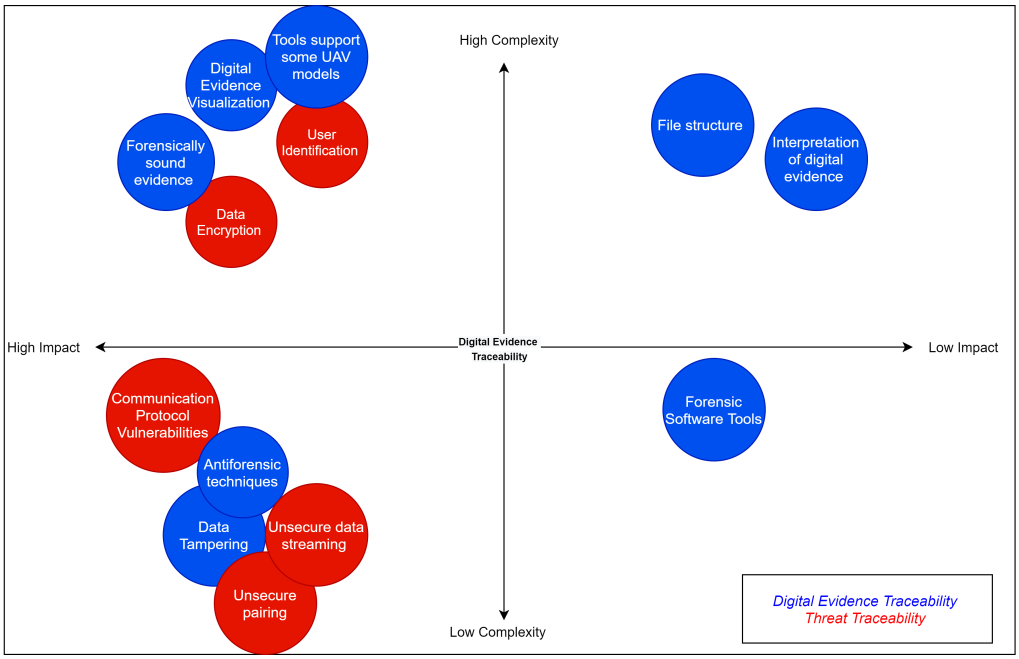

Figure 9. Categorization of UAV static and live digital evidence traceability challenges.

The concentration of this research is to better understand the technical issues related to the forensic soundness of UAV digital evidence. The most important piece of digital evidence pertaining to UAV forensic analysis is the flight log. Some small UAVs deploy encryption on flight log data, but some do not have this security feature. It is also important to note that some UAVs have different file structures of their flight logs, software, and sensor event logs. The most common flight log type is the '.DAT' file, and the DatCon software tool is the only available tool to decrypt '.DAT' files, which can be a limiting factor in some situations. Forensic software tools, such as Autopsy and Magnet Axiom, utilize the DatCon decryption algorithm to generate '.CSV' and/or '.KML' files to help investigators in visualizing a scenario. The DROP tool developed by [29] has reverse engineered the decryption algorithm of DatCon so that it can process encrypted data recovered from UAVs. This is a useful feature to the decryption process (e.g., generating MD5 and SHA256 hash values), but the generated hash values were only for the original '.DAT' files. This means that most of these tools have not been calculating the cryptographic hash values of the generated output (i.e., the decrypted flight log). Therefore, we concentrate on the multiplicity of the decryption process by decrypting the same flight log twice. This is crucial for two reasons: (1) the decrypted file should have the same cryptographic hash value during the second attempt, and (2) failure in having the same cryptographic hash value in both attempts results in no forensically sound digital evidence and leaves the door wide open to data integrity issues from various angles. In other words, this issue does not assure the quality of the recovered data, making it challenging to end up with secure and unaltered data. Note that tampering with encrypted data is out of the scope of this research. The presented technical issue is linked to the forensic soundness of UAV digital evidence.

To further illustrate our findings, we performed analysis on some flight logs using the DatCon software. Our analysis started with decrypting 'FLY000.DAT' with a size of *71 megabytes* and MD5 hash of *42b005dface6031b26a254c351e2b166*. We made sure that the DatCon tool does not impact the original '.DAT' file during the decryption process. The first decryption attempt has generated a file (FLY000.CSV) with a size of *32,978,802 bytes* and MD5 hash of *2601969f36bd0d59d1cc3624361c5730*. In comparison, the second decryption attempt resulted in a FLY000.CSV file with a size of *32,908,703 bytes* and MD5 hash value of *ee36a352c4052c080796096dc470406e*. The identified technical issue was carefully investigated because generating two different results from the same file (i.e., source of digital evidence) is a serious issue that might lead to uncertainty, hence technical and

legal problems. To ensure the legitimacy of our discovery, we made sure that all software settings and preferences were the same during each decryption process. Regardless of the similarities in processes, the problem was still occurring. Eventually, we found that the difference was minimal between the files, and it is either a rounding of the last number, replacement of a number, or the removal of a number. The occurrence of rounding numbers was the most likely cause. Next, we dug deep into the comparison between the bugs associated with the float point calculations performed by the Java virtual machine (VM). To test this hypothesis, we had to run the file decryption on OpenJDK to validate if the issue is associated with the Java compiler. Our analysis indicated that the OpenJDK does not produce the same results, hence using DatCon on Java VM will result in specific technical issues that affect data integrity. Although the difference between the files has a low significance in digital forensics, the data integrity is a very important factor.

During our analysis, we wanted to further investigate the significance of the changes between files from a digital forensic prospective. We based our research lens around a basic question: Would the difference between the files impact the results of the investigation? The answer ended up being "no". The technical issue has an insignificant impact on the final results but does increase the chance for a lack of data integrity. When we investigated the first byte change, we found that it occurred under the `IMU\_ATTI(0):tiltInclination` field. This field contains signals of the angle inclination. In addition, while there were different float rounding calculations in the tilt inclination, the two files are not forensically identical either. This means that the decryption process via DatCon Java vm could result in technical issues. Since the issue is tied to the Java vm calculation, we suggest UAV forensic investigators to decrypt '.DAT' files using the Openjdk vm to retain data integrity and prevent unforeseen issues. The Openjdk vm has been tested with multiple files, and no issues were reported.

4.3. Cross-Validation Analysis

To enhance our findings, it is crucial to test other '.DAT' files and report any differences. Figure 10 shows the steps taken to validate the integrity of the selected flight logs and highlight associated issues.

We performed the test again on a randomly selected file (FLY010.DAT). The first decrypted file (FLY010.CSV) has a size of *59,781,557 bytes* and MD5 hash value of *49dd94e6c3bf5c2e353255817c4641b0*. The second decrypted file (FLY010.CSV) has a size of *51,680,480 bytes* and MD5 hash value of *671ef418fd30485807a7838285574723*. The differences between the two files were noticeable as the DatCon tool added a '.' next to the version number of the tool when the file was decrypted. However, we performed the same test by analyzing 18 '.DAT' files and the technical issue appeared in only three files. Table 3 illustrates the MD5 hash values of all 18 decrypted files. Since files 0, 6, and 10 were not identical after the second decryption attempt, we therefore investigated the files to find out where the data changed. In comparison to 'FLY000.CSV', the first data that got changed in 'FLY006.CSV' was in the `IMU\_ATTI(0):directionOfTravel[mag]:c` field. According to the DatCon decryption [30], this field is responsible for degrees computed from successive latitude/longitude coordinates. The first data change between the two files is illustrated in Figure 11. Since there are slight differences between the the first and second attempts of decrypting the 'FLY006.DAT', we represented the content of both files in a scatter plot to visually compare them and flag any major differences. As shown in Figure 12, the scatter plot does not show a major visual difference, signifying that the files are nearly identical; however, from a digital forensic perspective, these files are not the same. The calculated MD5 hash values are different, and we observed a slight drop in the file size during the second decryption attempt.

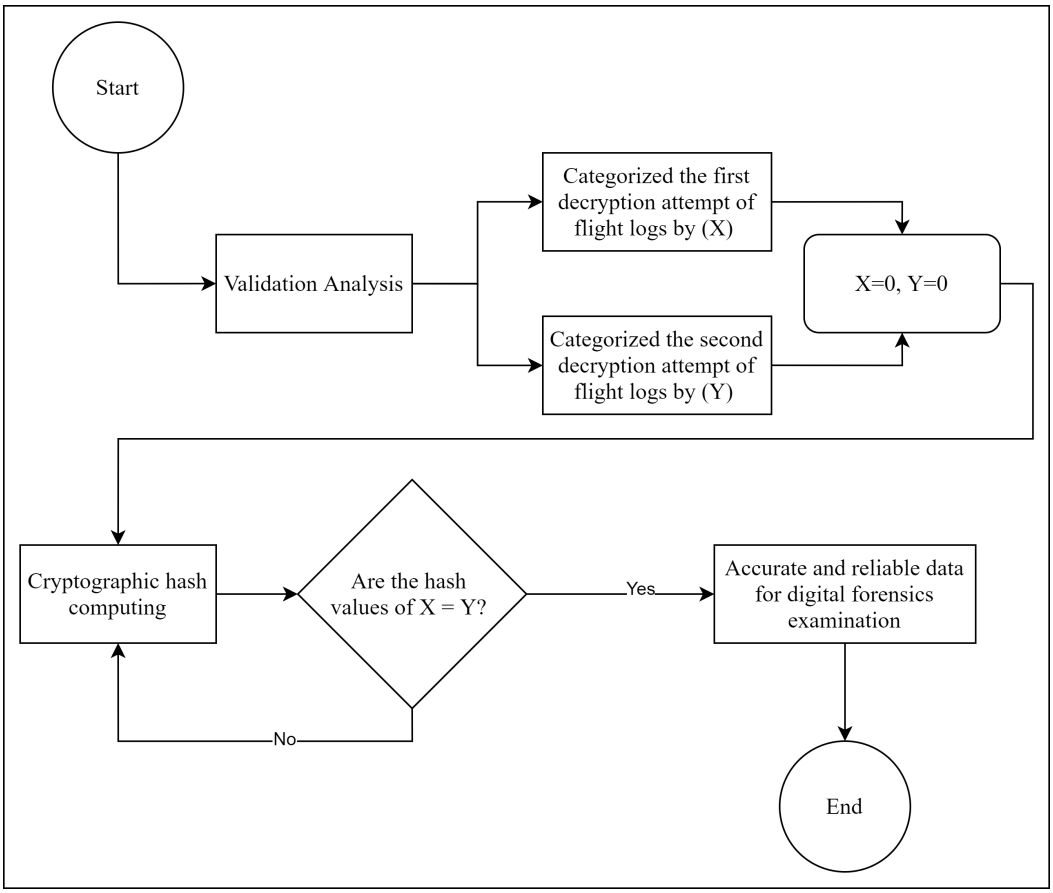

Figure 10. Flight logs' decryption procedure.

Table 3. Cross-validation of the DatCon decryption process.

File Name	MD5 Hash Value (1st Attempt)	MD5 Hash Value (2nd Attempt)
0	2601969f36bd0d59d1cc3624361c5730	2b36f21fcfced76ca36e9fe87ec8b08b
1	741f5bda2f425fc925e3fda798718e63	741f5bda2f425fc925e3fda798718e63
2	ccc366d53cda2507ef3ae7e0a4568462	ccc366d53cda2507ef3ae7e0a4568462
3	6b53a66e3ada5a9cd9ca491be48676ea	6b53a66e3ada5a9cd9ca491be48676ea
4	ded81b528dd9cd38d11e0a6955a95301	ded81b528dd9cd38d11e0a6955a95301
6	328265e3df38aef88a02c88276c35965	2a63b5ea110a9eb52e01ac821c153ed3
7	72f861e485392b1baeebccb4352bdfa3	72f861e485392b1baeebccb4352bdfa3
8	72adbc023cdda648da869b4f2c259072	72adbc023cdda648da869b4f2c259072
9	b200e480194e2f85b2ce6b8553fbceb2	b200e480194e2f85b2ce6b8553fbceb2
10	49dd94e6c3bf5c2e353255817c4641b0	671ef418fd30485807a7838285574723
11	d79f99896fe5f6c36d904802189b7605	d79f99896fe5f6c36d904802189b7605
12	42ce82bc1924724a8adefbf6e63c23d7	42ce82bc1924724a8adefbf6e63c23d7
13	7126cef458de088d62bcc6051b22d7d7	7126cef458de088d62bcc6051b22d7d7
14	496edcd1ea228fa97f1efe029ebba860	496edcd1ea228fa97f1efe029ebba860
15	4496fb7a4d63b2fa7fbf01940b2d0d93	4496fb7a4d63b2fa7fbf01940b2d0d93
16	44b03594b87089979033f9044155d77e	44b03594b87089979033f9044155d77e
17	8a5348afdca2ffc90f1dd50bdeef7820	8a5348afdca2ffc90f1dd50bdeef7820
18	a441434fbecb87e451b134a606831120	a441434fbecb87e451b134a606831120

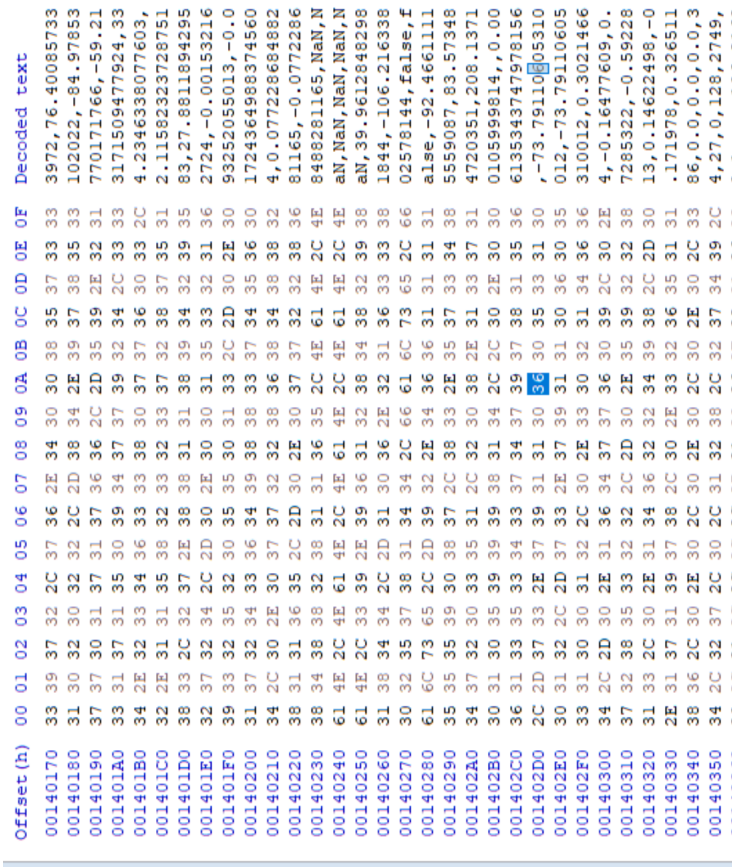

Figure 11. The first byte of data change.

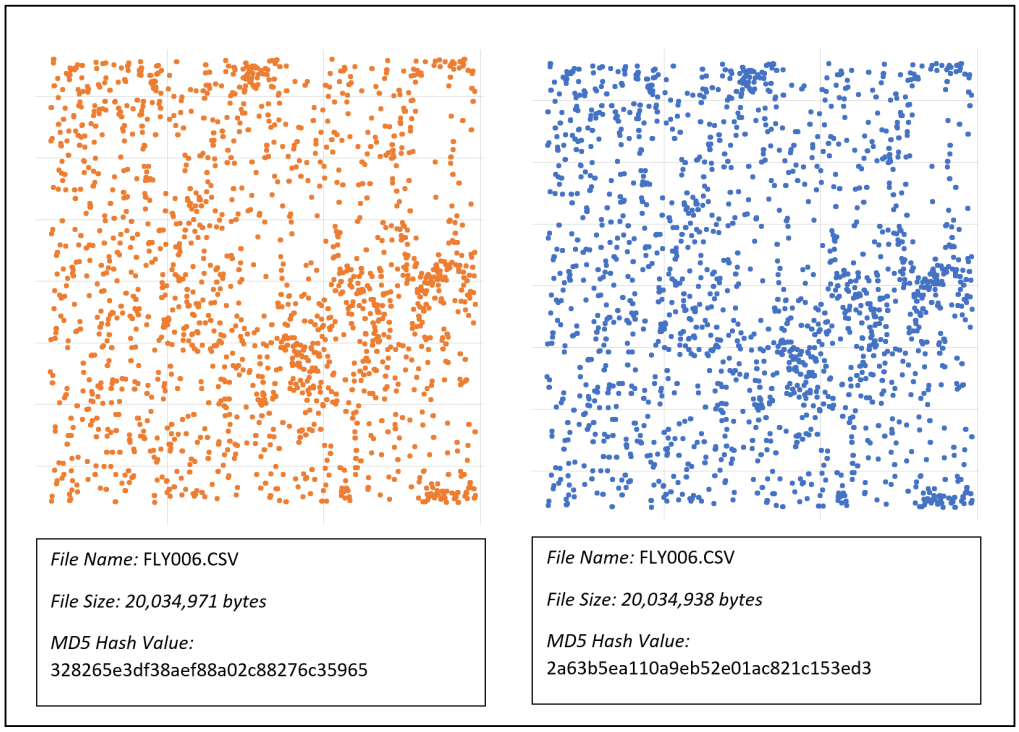

Figure 12. Scatter Plot showing the data comparison between the two decryption attempts of FLY06.

5. Discussion

In this research, we performed several 'purple-teaming' exercises that led to the proposal of the UAV Kill Chain, which incorporates both 'red' and 'blue' teaming techniques. The proposed UAV Kill Chain can help solve important challenges to UAV security and forensics. UAV anti-detection and anti-forensics techniques are complex topics due to the UAS's architecture and flow of data. We claim that data flow and UAS architecture influence the tendency of UAV anti-detection and anti-forensic techniques.

On the other hand, our forensic investigation on the recovered flight logs has led us to the discovery of a technical issue during the decryption process via the DatCon software tool. After a comprehensive analysis, we recognize that this technical issue has the least significant impact on the content of the decrypted file. With this in mind, we urge UAV forensic investigators to remain aware of the possible implications. Eventually, we discovered that the issue is linked to the Java compiler after comparing the analysis between Java and Openjdk virtual machines.

We recognize that this study has limitations. The most obvious limitations are open space and gaining authorized flying clearance, even when using lightweight drones like we did. The second limitation includes having to gather more tools, equipment, and lab space to perform further investigations on other types of drones. Lastly, highlighting technical issues related to the reporting phase is a time-consuming task.

The purpose of this research was to address the proposed research questions. Digital evidence points to how attack intrusions need live monitoring sensors to detect abnormal behaviors, and we know certain intrusions could leave traceable footprints, depending on the UAS architecture. In addition, when considering security threats to UAVs, there are indicators that security was omitted from, or at least a low priority on, the system components array.

6. Conclusions

The use of UAVs is becoming more ubiquitous, with user groups ranging from businesses and governments to individuals. Challenges coming from drones require an in-depth experimental study that aids engineers in implementing more secure systems at

every level. In this paper, 'Purple-teaming' techniques have been utilized in the presented scenario to illustrate potential live digital evidence traceability challenges. This work compared the forensic analysis and traceability of digital evidence in static and live modes. Then, it highlighted the complexity and impact of each technical challenge associated with digital evidence traceability. Throughout this research, we discussed static and live digital evidence traceability challenges in UAV forensics, presented several UAV attack scenarios, proposed new techniques related to the UAS architecture that would streamline the evidence identification process, and presented a categorization model that classifies the discovered traceability challenges.

In the future, we plan on expanding this work by reviewing the percentage of UAVs using a non-encrypted link, exploring different controls, data channels, and frequencies. In addition, we will consider different scenarios such as attack vectors related to UAV flying in non-tethered modes (autonomous waypoints, etc.). Finally, we will consider technical challenges related to data integrity and propose a forensically sound approach to the UAV forensic investigations.

Author Contributions: The authors of this paper have contributed to this work in the following ways. Conceptualization, F.E.S.; methodology, F.E.S.; validation, F.E.S. and U.K. and M.K.R. and E.T.M.; formal analysis, F.E.S.; Project administration, F.E.S.; Resources, F.E.S.; investigation, F.E.S.; writing—original draft preparation, F.E.S.; writing—review and editing, F.E.S. and U.K. and M.K.R. and E.T.M.; visualization, F.E.S.; supervision, U.K. and M.K.R. and E.T.M.; project administration, F.E.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Frost, S. Study Analysing the Current Activities in the Field of UAV. Technical Report, ENTR/2007/065. 2007. Available online: https://ec.europa.eu/home-affairs (accessed on 20 March 2021).
2. Small Unmanned Air System (SUAS) Assessment. Available online: https://www.airproxboard.org.uk/Reports-and-analysis/Airprox-reports-2018/ (accessed on 18 March 2021).
3. Goppert, J.M.; Wagoner, A.R.; Schrader, D.K.; Ghose, S.; Kim, Y.; Park, S.; Gomez, M.; Matson, E.T.; Hopmeier, M.J. Realization of an autonomous, air-to-air Counter Unmanned Aerial System (CUAS). In Proceedings of the 2017 First IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan, 10–12 April 2017; pp. 235–240.
4. Koubaa, A.; Allouch, A.; Alajlan, M.; Javed, Y.; Belghith, A.; Khalgui, M. Micro air vehicle link (mavlink) in a nutshell: A survey. *IEEE Access* **2019**, *7*, 87658–87680. [CrossRef]
5. Salamh, F.E.; Karabiyik, U.; Rogers, M. A Constructive DIREST Security Threat Modeling for Drone as a Service. *J. Digit. Forensics Secur. Law* **2021**, *16*, 2.
6. Choudhary, G.; Sharma, V.; You, I.; Yim, K.; Chen, R.; Cho, J.H. Intrusion detection systems for networked unmanned aerial vehicles: A survey. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 560–565.
7. Tseng, C.Y.; Balasubramanyam, P.; Ko, C.; Limprasittiporn, R.; Rowe, J.; Levitt, K. A specification-based intrusion detection system for AODV. In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Fairfax, VA, USA, 2003; pp. 125–134.
8. Vaidya, V. Dynamic Signature Inspection-Based Network Intrusion Detection. U.S. Patent 6,279,113, 21 August 2001.
9. Patcha, A.; Park, J.M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Comput. Netw.* **2007**, *51*, 3448–3470. [CrossRef]
10. Aydın, M.A.; Zaim, A.H.; Ceylan, K.G. A hybrid intrusion detection system design for computer network security. *Comput. Electr. Eng.* **2009**, *35*, 517–526. [CrossRef]
11. Sharma, V.; Choudhary, G.; Ko, Y.; You, I. Behavior and vulnerability assessment of drones-enabled industrial internet of things (iiot). *IEEE Access* **2018**, *6*, 43368–43383. [CrossRef]
12. Birnbaum, Z.; Dolgikh, A.; Skormin, V.; O'Brien, E.; Muller, D.; Stracquodaine, C. Unmanned aerial vehicle security using behavioral profiling. In Proceedings of the 2015 International Conference on Unmanned Aircraft Systems (ICUAS), Denver, CO, USA, 9–12 June 2015; pp. 1310–1319.
13. Birnbaum, Z.; Dolgikh, A.; Skormin, V.; O'Brien, E.; Muller, D.; Stracquodaine, C. Unmanned aerial vehicle security using recursive parameter estimation. *J. Intell. Robot. Syst.* **2016**, *84*, 107–120. [CrossRef]
14. Sedjelmaci, H.; Senouci, S.M.; Ansari, N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *48*, 1594–1606. [CrossRef]

15. Choudhary, G.; Sharma, V.; Gupta, T.; Kim, J.; You, I. Internet of drones (iod): Threats, vulnerability, and security perspectives. *arXiv* **2018**, arXiv:1808.00203
16. Fox-Brewster, T. Maldrone: Watch Malware That Wants To Spread Its Wings Kill A Drone Mid-Flight. Forbes Magazine. Available online: http://www.forbes.com/sites/bernardmarr/2015/09/01/7-technologytrends-that-will-make-or-break-many-careers/ (accessed on 22 March 2021).
17. Javaid, A.Y.; Sun, W.; Devabhaktuni, V.K.; Alam, M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 585–590.
18. Chabukswar, R. Secure Detection in Cyberphysical Control Systems. Available online: https://chabukswar.in/projects/thesis.pdf (accessed on 10 March 2021).
19. Altawy, R.; Youssef, A.M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber Phys. Syst.* **2016**, *1*, 1–25. [CrossRef]
20. Salamh, F.E.; Karabiyik, U.; Rogers, M.; Al-Hazemi, F. Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs). In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 704–710.
21. Salamh, F.E.; Karabiyik, U.; Rogers, M.K. RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H. *Sensors* **2019**, *19*, 3246. [CrossRef] [PubMed]
22. Salamh, F.E.; Mirza, M.M.; Karabiyik, U. UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. *Electronics* **2021**, *10*, 733. [CrossRef]
23. DatCon Downloads. Available online: https://datfile.net/DatCon/downloads.html (accessed on 18 March 2021).
24. Jain, U.; Rogers, M.; Matson, E.T. Drone forensic framework: Sensor and data identification and verification. In Proceedings of the 2017 IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, USA, 13–15 March 2017; pp. 1–6.
25. Armando, A.; Henauer, M.; Rigoni, A. *Next, Generation CERTs*; IOS Press: Amsterdam, The Netherlands, 2019; Volume 54.
26. Watson, S. Drone Forensic Program. Available online: https://dfrws.org/wp-content/uploads/2019/06/pres_drone_forensics_program.pdf (accessed on 1 March 2021).
27. Martin, L. Cyber Kill Chain®. Available online: http://cyber.lockheedmartin.com/hubfs/GainingtheAdvantageCyberKillChain.pdf (accessed on 3 May 2021).
28. Salamh, F.E.; Karabiyik, U.; Rogers, M.K.; Matson, E.T. Unmanned Aerial Vehicle Kill Chain: Purple-Teaming Tactics. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Virtual Conference, 27–30 January 2021; pp. 1081–1087.
29. Clark, D.R.; Meffert, C.; Baggili, I.; Breitinger, F. DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digit. Investig.* **2017**, *22*, S3–S14. [CrossRef]
30. V3.CSV Column Descriptions. Available online: http://www.datfile.net/DatCon/fieldsV3.html (accessed on 16 March 2021).