[Array 14 (2022) 100135](https://doi.org/10.1016/j.array.2022.100135)

|  |  |  |
| --- | --- | --- |
|  | Contents lists available at [ScienceDirect](http://www.elsevier.com/locate/array) |  |
| Array |
| journal homepage: [www.elsevier.com/locate/array](http://www.elsevier.com/locate/array) |
|  | | |

Who watches the new watchmen? The challenges for drone digital forensics investigations

Evangelos Mantasa, Constantinos Patsakisb,c,∗

a *University of Oxford, OX1 2JD Oxford, United Kingdom*   
b *University of Piraeus, 80 Karaoli & Dimitriou str, 18534 Piraeus, Greece*   
c *Athena Research Center, Artemidos 6, Marousi 15125, Greece*

|  |  |  |
| --- | --- | --- |
| A R T I C L E | I N F O | A B S T R A C T |
| *Keywords:*  UAV  UAS  Drones  Digital forensics Investigation  Standardisation |  | The technological advance of drone technology has augmented the existing capabilities of flying vehicles rendering them a valuable asset of the modern society. As more drones are expected to occupy the airspace in the near future, security-related incidents, either malicious acts or accidents, will increase as well. The forensics analysis of a security incident is essential, as drones are flying above populated areas and have also been weaponised from radical forces and perpetrators. Thus, it is an imperative need to establish a Drone Digital Forensics Investigation Framework and standardise the processes of collecting and processing such evidence.  Although there are numerous drone platforms in the market, the same principles apply to all of them; just like mobile phones. Nevertheless, due to the nature of drones, standardised forensics procedures to date do not manage to address the required processes and challenges that such investigations pose. Acknowledging this need, we detail the unique characteristics of drones and the gaps in existing methodologies and standards, showcasing that there are fundamental issues in terms of their forensics analysis from various perspectives, ranging from operational and procedural ones, and escalate to manufacturers, as well as legal restrictions. The above creates a very complex environment where coordinated actions must be made among the key stakeholders. Therefore, this work paves the way to address these challenges by identifying the main issues, their origins, and the needs in the field by performing a thorough review of the literature and a gap analysis. |

**1. Introduction**

A few years ago, drones were exclusively used by government and military organisations, but the ever-evolving technology made them accessible to the public. What was labelled as a ‘‘technology of the fu-ture’’, quickly become a technology of today, as drones integrated to the needs of the market rapidly. Drones evolved from toy machines used by numerous flight enthusiasts to machines that can undertake operations on everyday tasks. From seemingly simple applications like high-level quality infrastructure inspections, and everyday goods deliveries to life-saving Search and Rescue (SAR) missions, drones have established their value to the society. The revolutionary use of drones comes with side effects as malicious actors have also evolved to incorporate drones in their *modus operandi* as they are cheap, reliable and easy to modify to carry payloads (e.g. drugs, explosive devices). Over the last five years, drones have been used to disrupt airport operations,1attempted

high-value persons assassinations,2and used in attacks against industry complexes3to name a few. The number of malicious acts is expected to rise since perpetrators are becoming more acquainted with this new technology.

The need to address this emerging technology has pushed Digital Forensics Science to further specialise in handling incidents involving drones and their supporting equipment or devices. Since this need is relatively new, there is a limited amount of information and specialisa-tion on the matter, and as there is no standardised practice to conduct a forensic investigation around drones, the investigator relies on already established procedures, relevant to other digital devices, that may not be applicable to a drone. Furthermore, the presence of a large number of different devices, that support the operation of a drone expands the complexity of the investigation, as the forensics expert will have to

∗ Corresponding au[thor at: University of Pir](mailto:emantas000@gmail.com)aeus, 80 Kara[oli & Dimitriou s](mailto:kpatsak@unipi.gr)tr, 18534 Piraeus, Greece.

*[E-mail addresses:](https://www.forbes.com/sites/grantmartin/2019/01/08/londons-heathrow-airport-briefly-closed-following-possible-drone-sighting/)* [emantas000@gmail.com](mailto:emantas000@gmail.com) [(E. Mantas),](https://www.forbes.com/sites/grantmartin/2019/01/08/londons-heathrow-airport-briefly-closed-following-possible-drone-sighting/) [kpatsak@unipi.gr (C. Patsakis).](https://www.forbes.com/sites/grantmartin/2019/01/08/londons-heathrow-airport-briefly-closed-following-possible-drone-sighting/)

1 [https://www.forb](https://www.forbes.com/sites/grantmartin/2019/01/08/londons-heathrow-airport-briefly-closed-following-possible-drone-sighting/)[es.com/sites/grantmartin](mailto:emantas000@gmail.com)[/2019/01/08/londons-heathrow-airport-briefly-closed-following-possible-drone-sighting/](https://www.forbes.com/sites/grantmartin/2019/01/08/londons-heathrow-airport-briefly-closed-following-possible-drone-sighting/). 2 [https://www.bbc.com/news/world-latin-america-45073385.](https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html)

3 <https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html>.

<https://doi.org/10.1016/j.array.2022.100135>

[Received 29 June 2021; Received in revised](https://doi.org/10.1016/j.array.2022.100135) form 3 October 2021; Accepted 22 February 2022

Available online 11 March 2022

[2590-0056](http://creativecommons.org/licenses/by-nc-nd/4.0/)/© 2022 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license ([http://creativecommons.org/licenses/by-](http://creativecommons.org/licenses/by-nc-nd/4.0/)

[nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*

handle the supporting devices as well as to find and correlate evidence regarding the drone operation.

This work focuses on explaining the reason behind the need for a standardised procedure by identifying the related devices needed to be examined and the evidence stored in them. Therefore, we review the related literature, highlighting key differences with traditional digital forensics operations and the challenges that these introduce. We argue that since both drone accidents and malicious acts will become in-creasingly frequent in the near future, a forensics framework to handle such incidents should be set in a timely manner. In this regard, our work performs a thorough literature review which covers the work in both academic and ‘gray’ literature as it spans to, e.g. international standards. Based on this, our gap analysis illustrates the needs in the field and serves as a guideline for both academic and practitioners in the field.

The rest of this manuscript is organised as follows. First, we present the related work by first providing an overview of the drone and the most relevant forensics tools for drones. Then, in Section 3, we discuss which are the primary sources for evidence in a drone and their types, to proceed with a generic overview of the cases that a forensics investigator would have to face. To facilitate her task, we accompany the latter with a comprehensive and prioritised list of evidence for each case. In Section 4.1, we first present the relevant forensic models and standards to discuss the primary challenges in the forensics investigation in the form of a gap analysis afterwards. The key differences of drones and their particularities indicate that we are currently missing not only the needed tools but also the procedures to address the upcoming forensics cases. The article then concludes and streamlines some key findings and open issues for the further development of the field.

**2. Related work**

The goal of this section is to acquaint the reader with the drone and the existing tools to collect forensic evidence from a drone. Therefore, we briefly provide an overview of a drone and proceed to present some relevant tools and their scope.

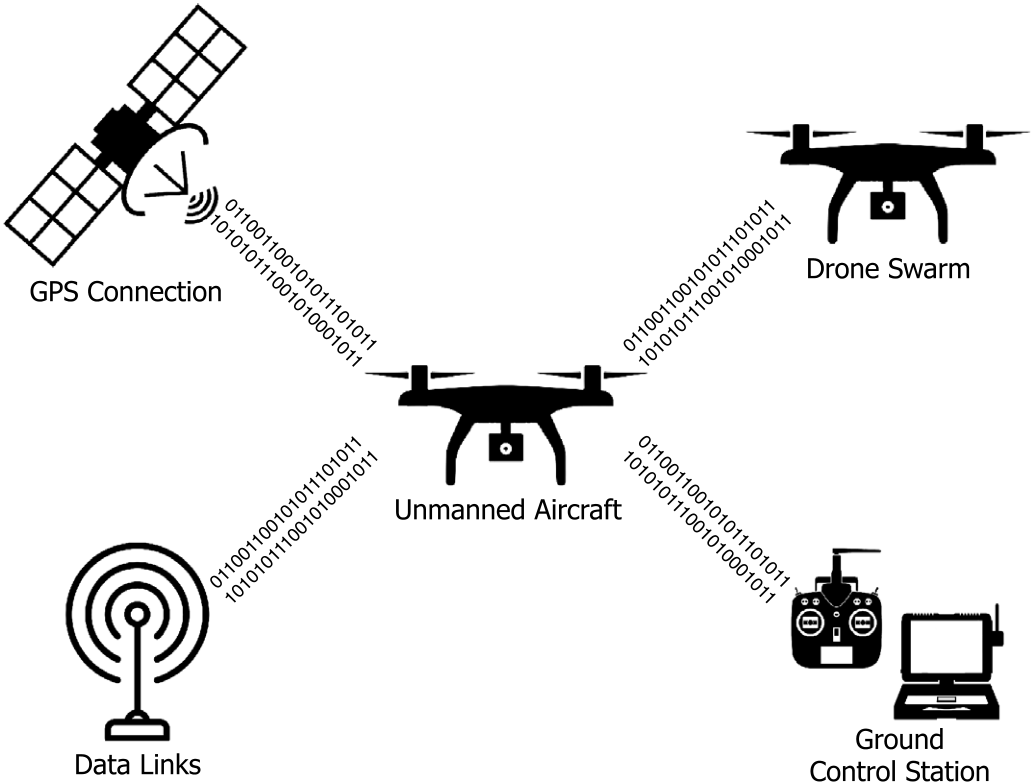
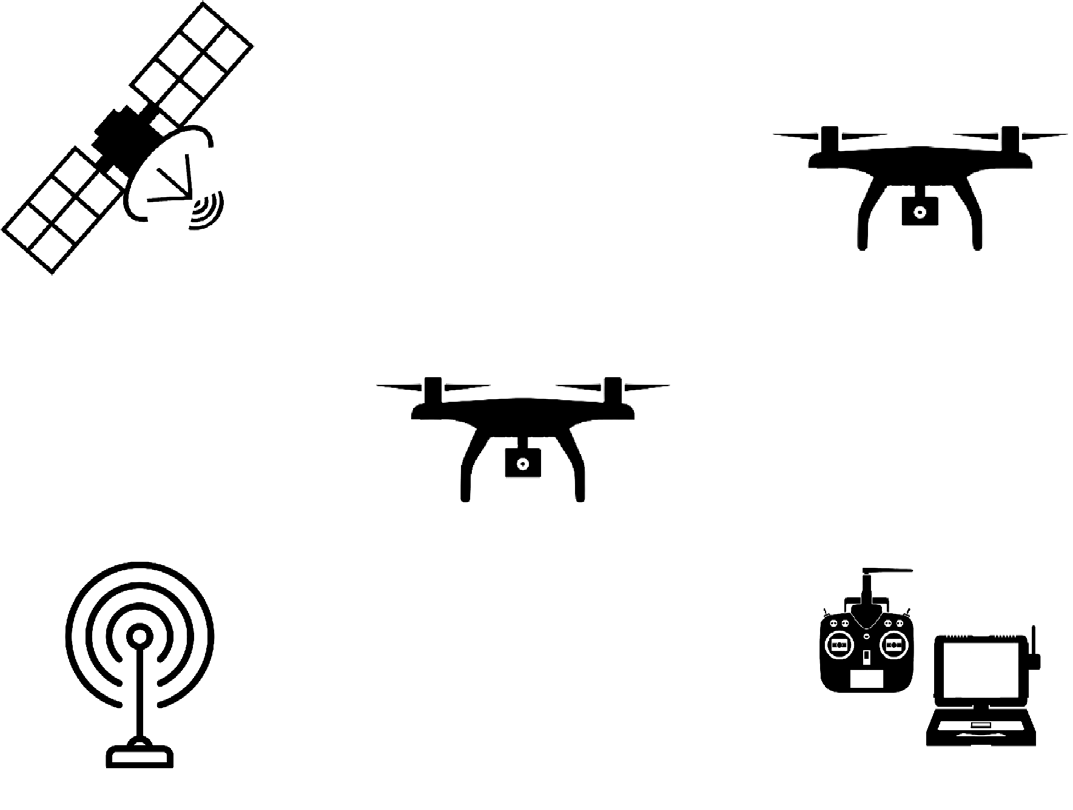
*2.1. Overview of a drone*

Unmanned Aerial Vehicles are commonly acknowledged as drones in everyday life. It is important to make a distinction between the sys-tems with autonomous capabilities and the hobbyist flying machines; the capabilities of which rely only on the pilot’s skills. Since these radio-controlled (RC) machines require minimal and basic hardware to fly, usually a ‘flight board‘ to receive and process the signal to spin the motors, they do not offer any tangible digital forensics. Therefore, this work focuses on drones with autonomous capabilities. The primary components of a drone are the following:

• **Flight Controller:** The most critical component of a drone since it contains a variety of sensors (e.g. accelerometer, gyroscope) and software, or as widely know as the autopilot, to allow the execution of autonomous commands and more complex flight scenarios. The flight controller can also receive input from sensors (e.g. lidar, infrared) and adjust the flight path to avoid collision with nearby objects without any human interaction.

• **Companion Computer:** The flight controller can be directly con-nected to a small on-board companion computer (e.g. Raspberry Pi, Asus Tinker-board) that augments the drones’ capabilities even further, running a real-time Operating System (OS). A task like an object avoidance can be executed by combining the on-board range-finding sensors connected on the companion computer and provide that feedback to the flight controller. Companion comput-ers are expected to be found on makeshift/DIY flying machines or very sophisticated commercial drones to handle demanding tasks, such as object avoidance and 3D object reconstruction.

2



*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*



**Fig. 1.** Components of an Unmanned Aerial System (UAS).

• **Unmanned Aircraft (UmA):** The flying vehicle as described in the previous section, is probably the most critical component since the whole system exists to assist the drone’s operation and its autonomous capabilities. It should also be noted that another or multiple flying vehicles may be part of the same UAS, which is described as a *swarm*.

• **Ground Control Station (GCS):** Ground Control Station is the ground-based software and hardware that provides communica-tion and enables the remote control of the drone. GCS software can be installed on systems on fixed locations (e.g. military air-bases) or in portable systems such as laptops and mobile phones. The acquisition of the GCS device is of great significance since it contains most of the flight data and can be linked with an individual. There are commercially available drones that come equipped with controllers with proprietary software to control the drone, a hybrid device combining the analogue RF control and the digital interface of a mobile platform, the acquisition of which can also contain considerable evidence.

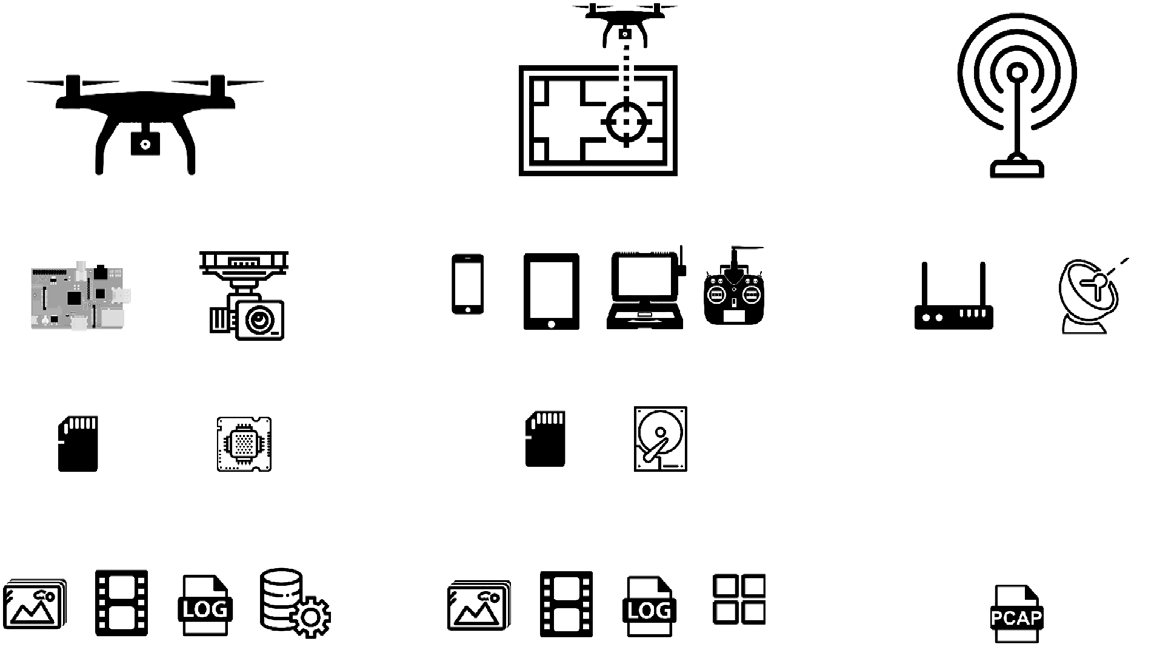
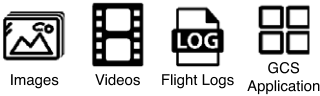
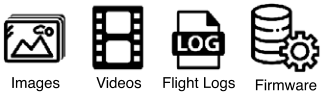
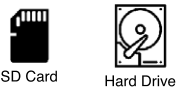
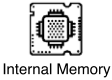
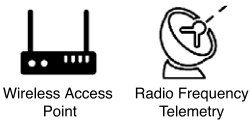
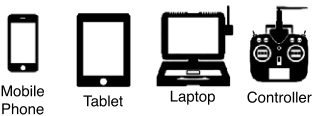
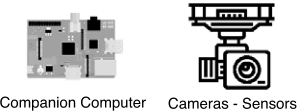
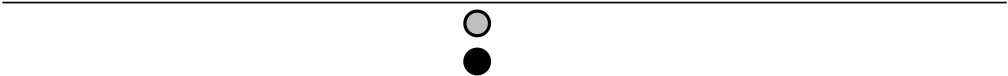
• **Communication Data-Link (CDL):** Data links are mainly used for UAV control, video transmission from the on-board camera and telemetry providing information on the location of the vehicle or other sensor values. Each data link broadcasts on a different radio-frequency (RF) wavelength with 4 GHz and 900 Mhz mainly being used for *UAV control*, 3-4–5 GHz for *video transmission* and 400–900 Mhz for *telemetry*.4Small UAVs (sUAV) may also use Bluetooth and WiFi communications to execute all the previous operations, but their flight radius is significantly reduced.

All these interconnected components store data related to the drone operation or serve them to other devices. These data can be classified in the following types:

• **Flight logs and predefined flight missions:** As mentioned be-fore, the *flight controller*, is responsible for the autonomous ca-pabilities, has another function during the flight. It generates a log that contains information about critical sensors like the GPS position and altitude, resulting in a reconstruction of the flight path, providing valuable information about the drone activity to the forensics investigator. Moreover, they contain key equipment data and error logs. For instance, battery and signal statistics

4 [https://www.911security.com/learn/airspace-security/drone-fundamentals/drone-communication-data-link.](https://www.911security.com/learn/airspace-security/drone-fundamentals/drone-communication-data-link)

3



*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*









**Fig. 2.** Evidence Distribution on UAS devices.

like the SD card. Provided with the fact that storage capacities of micro SD cards have exceeded the TB mark, the low price per byte ratio has established them as the dominant data storage solution in UAVs. Most of the drones have an SD card slot to save images and video footage recorded during the flight or even the ‘‘hard drive’’ of the companion computer.

• **Companion Computer Storage:** As mentioned before, compan-ion computers are running a real-time OS. This may contain digital evidence as ‘‘raw’’ information of drones activity, like the execution of flight-mission scripts and transmission of data to other devices.

• **Mobile Devices:** Mobile GCS applications provide the ability to control a drone or receive a payload (e.g. video stream of the drone’s on-board camera) via wireless connection (e.g. WiFi, Bluetooth) and should also be considered as a prospective data source that can be directly linked to the pilot.

• **Network Packets:** The monitoring and capturing of packets from the UAS network, can lead to the discovery of numerous payloads or devices and servers that the fight data are stored, as an addi-tional source of evidence that could not be otherwise obvious to the forensic investigator.

• **Cloud Storage:** There is a currently increasing trend in UAV technology, where manufacturers allow their clients to store their logs and images on their servers. Data storage outsourcing to third parties’ servers, internal UAS cloud, and backup servers, due to the demand to reduce local storage media, should also be considered during a UAS forensics investigation.

An indicative list of the devices and the evidence found on a typical UAS is illustrated in Fig. 2.

*3.2. Cases for forensics investigation*

It is deemed necessary to outline the cases that a digital forensic investigation would be required, to highlight which evidence might be available and which ones could be more more relevant for each case. The most ‘‘benign’’ cases involve accidents where the forensic in-vestigator should determine its causes. It is clear that even a small malfunction, due to the altitude that a drone may have and the dif-ficulty to balance once something starts falling from the sky, severe damages would be suffered by the drone. Moreover, while one may not care about the damage to the drone and its payload per se, insurance issues due to the caused damages may require the investigation of the accident. It should be noted that weather issues due to sudden and local phenomena or even collisions with a bird or another drone fall into the accident category and have to be investigated. In such cases, the most relevant evidence would be the flight logs and media captured, since

4

*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*

has to assess the actual impact as further damages may have been caused. The evidence will allow her to estimate when and where the incident occurred but also to extract some key locations of interest, e.g. from where the drone was launched and where it was heading to. The scheduled flight and the payload may also denote the drone’s purpose. For the attribution, the investigator also has to consider the stored data (images, videos), metadata (emails, registered accounts, stored WiFi), hardware tags, as well as wet evidence (fingerprints, DNA) to assess the possible owner and controller of the drone. Clearly, the above highlight the strong connection of the digital evidence with the physical ones which act rather complementary.

To summarise the evidence collection sources, in Table 1, we high-light and prioritise the most relevant evidence sources per case. The table clearly shows how the generic cases we discussed earlier differ as the investigator has to look for different evidence.

**4. Challenges and gaps for drone digital forensics**

There is a constant challenge to stay up to date with the rapid changes in the latest technologies. Drones are beginning to shape tomorrow’s society, used by many individuals for both personal and professional purposes. The challenge of carrying out digital forensics on drones and associated devices as part of the UAS, is to identify flight routes, possible malfunctions, collisions, and associated media (pictures and videos) contained within the system’s devices. These may facilitate the investigator to understand the mission of the drone, whether the operation was successfully performed, the people or assets that were affected by it, and the reasons behind possible damage or collision. The findings derived from electronic evidence must follow a standard set of guidelines to ensure that the investigation is not challenged in a court of law [10]. Moreover, the border-less nature should also be considered due to cloud storage (e.g. evidence on a server hosted in a third country). In fact, as indicated by NIST, cloud forensics are also facing many challenges [11] and a draft mapping of, e.g. ISO 27037 is not that simple.6Additionally, the provision of the evidence from a cloud provider or a third party, in general, is not necessarily granted, as shown in the case of Apple and the San Bernardino shooting case.7 Note that even if the cloud service provider is willing to cooperate the data may be stored across different servers and countries. The presence of multiple devices and various formats on a UAS requires a high level of expertise from the forensic’s experts that take part in the investigation since each device requires different acquisition and examination techniques.

*4.1. Relevant standards, practices and challenges*

Standards are a vital necessity to ensure conformance and mutual compliance across the geographical and jurisdictional border. There are currently numerous standards and established practices provided by organisations worldwide using accepted methods. The technical details on how to forensically approach the investigation differs, depending on the device. The analysis of electronic evidence is typically categorised into the following phases: *identification*, *collection*, *acquisition*, *preser-vation* and *disposal*, although the exact phases naming may vary due to the usage of different forensic model that each organisation finds appropriate for their needs.

Currently, there are several models and methodologies regarding the handling of evidence and digital forensic procedures during an in-vestigation. These include the DFRWS model [12], the Enhanced Digital Investigation Process Model (EDIP) [13], the Analytical Crime Scene

6 <https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf>[.](https://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html)

[7](https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf) [https://edition.cnn.com/2016/02/16/us/san-bernardino-s](https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf)[hooter-phone-apple/index.html.](https://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html)

5

*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*

• **ISO/IEC 27038:2014:** Describes the digital redaction of informa-tion that must not be disclosed, taking extreme care to ensure that removed information is permanently unrecoverable.

• **ISO/IEC 27040:2015:** Provides detailed technical guidance on how organisations can define an appropriate level of risk miti-gation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security.

• **ISO/IEC 27041:2015:** Describes other standards and documents to provide guidance, setting the fundamental principles ensuring that tools, techniques and methods, appropriately selected for the investigation.

• **ISO/IEC 27042:2015:** This standard describes how methods and processes to be used during an investigation can be designed and implemented to allow correct evaluation of potential digital evi-dence, interpretation of digital evidence, and effective reporting of findings.

• **ISO/IEC 27043:2015:** It defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

• **ISO/IEC 27050:** This recently revised standard guides non-technical and technical personnel to handle evidence on electron-ically stored information (ESI).

• **ISO/IEC 17025:2017:** This standard describes the general re-quirements for the competence of testing and calibration lab-oratories, applying to all organisations performing laboratory activities, regardless of the number of personnel.

• **ISO/IEC 30121:2015:** Provides a framework for organisations to strategically prepare for a digital investigation before an incident occurs, to maximise the effectiveness of the investigation.

ETSI is a European Standards Organization that produces standards for ICT systems and services that are used all around the world, collaborating with numerous organisations. In 2020 ETSI published TS 103 643 V1.1.1 (2020-01) [21], a set of techniques for assurance of digital material in a legal proceeding, to provide a set of tools to assist the legitimate presentation of digital evidence.8   
 The National Institute of Standards and Technology (NIST) has released guidelines for organisations to *develop forensic capability*, based on the principles of forensic science in the aspect of the application of science to the law but should not be used on digital forensic investi-gations due to subjection to different laws and regulations, as clearly stated on their manual. The scope on NIST guidelines is *incorporating forensics into the information system life cycle* of an organisation. The most relevant guidelines are 800-86 [22] for Integrating Forensic Tech-niques into Incident Response and 800-101 [23] for Mobile Device Forensics.

The Scientific Working Group on Digital Evidence (SWGDE) is an organisation engaged in the field of digital and multimedia evidence to *foster communication and cooperation as well as to ensure quality and consistency within the forensic community*. SWGDE has released a number of documents to provide the current best practices on a large variety of state of the art forensics subjects. Nonetheless, none of them is targeting nor addressing the particularities of drone forensics.

Nevertheless, in none of the aforementioned standards is there any reference to drones. While someone could oversee this omission as the procedures could cover the procedures needed for UAV forensic investigations. However, for the collection of forensic evidence from a UAV one cannot always access the data and may need to exploit the device to gain access to them. As will be discussed in the next paragraphs, such processes are not foreseen by any standard. Moreover, the contradicting records in the log files of the UAV and the GCS; also discussed in the following paragraphs, are not considered by any

8 <https://www.swgde.org/documents/published>.

6

*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*

The latter issue with encryption leads to another challenge. To collect the evidence from a drone that lacks accessible removable storage devices, or they are encrypted, similar to mobile devices, one may need to exploit a vulnerability to gain access to the data. This implies tampering of the digital evidence introducing issues for the chain of custody of the evidence. The nature of the exploit and the need to, e.g. ‘‘root’’ the device may significantly alter the stored information and careful examination of the tools and methods is necessary to allow the presentation of the findings in a court of law. Clearly, such practices violate the first principle of ACPO, which clearly states that:

‘‘*No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subse-quently be relied upon in court.*’’

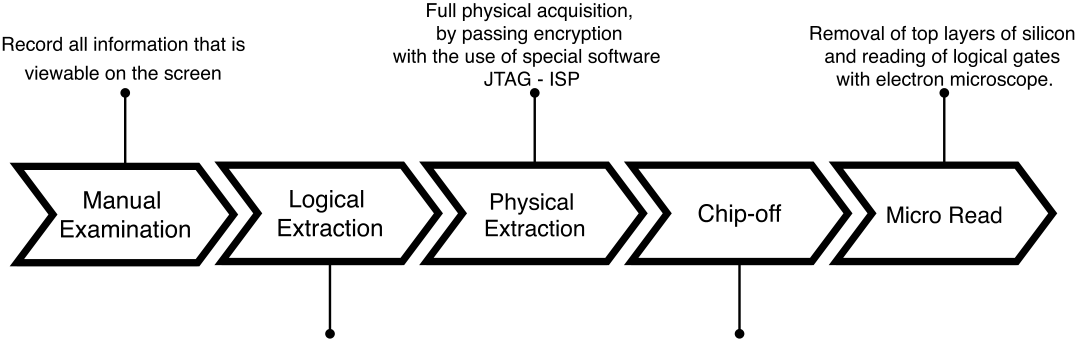
One has also to consider the diversity of the platforms. Unlike mobile phones where there are two main platforms, Android and iOS, and can be considered a well-established market the drone market might have a big player (DJI) which enjoys the biggest market share; more than 70%, nevertheless, the rest is significantly fragmented. Therefore, there are plenty of different platforms which imply the need for various forensics tools. Furthermore, the different scope of many of the drones as well as their big numbers suggest that despite the fragmentation this heterogeneity is expected to continue, so there is no foreseen interoperability of the forensics tools. It is worth noticing that the recent ban on Chinese manufactured drones may lead to significant market changes.10   
 One very challenging parameter for drone forensics has to do with live forensics. While Adelstein [29] stressed the need for live forensics, we have to acknowledge the additional difficulties and limitations of performing live digital forensics in a drone. Contrary to ‘‘traditionally’’compromised devices where the adversary will have integrated evasion, persistence and anti-analysis mechanisms, in a drone the adversary may have installed additional physical mechanisms, so the drone may physically react, e.g. consider it being armoured, or try to fly away. Beyond that, since the drone is remotely controlled; even via the cloud, kill switches or other such mechanisms are expected to continue being relevant during the investigation. To this end, to capture a drone, it is advised to approach it from a non-visible angle and use a non-tampering measure such as a coat or net. Next, the drone should be turned off without tampering any possible wet evidence on it.

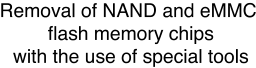
Since there is no standardised procedure to conduct a digital foren-sics investigation on drones, researchers have to resolve to already established practices that apply to similar devices. This raises the following question: What kind of device is a drone or relevant to, to select a method to proceed with the forensics triage. A valid argument would be that a drone has many similarities with a mobile phone regarding the hardware (e.g. processor architecture) and the sensors (e.g. GPS receiver, accelerometer). It should be noted here that there is also no standard for handling mobile digital forensics case, yet an initiative has recently started by the FORMOBILE H2020 project.11 To acquire the needed data, the investigator will have to resolve to the techniques illustrated in Fig. 4. Typically to *logically image* a mobile device, the investigator has to turn on the device. If this method is applied to a drone, there is a high risk to alter or erase the existing data of the UAV’s internal memory [30]. As stated in [6], turning on the drone will erase the previously recorded flight log, resulting in the loss of evidence and alteration of the investigation. Although the investigator followed the procedure correctly, the result may render the whole investigation useless due to misconceptions about the drone’s in-ternal operations. Since the storage of data on the drone itself is highly volatile, extreme caution and preparation for the acquisition should

10 [https://www.ainonline.com/aviation-news/aerospace/2020-08-17/us-near](https://www.ainonline.com/aviation-news/aerospace/2020-08-17/us-nears-law-banning-chinese-drones)[s-law-banning-chinese-drones](https://formobile-project.eu/)[.](https://www.ainonline.com/aviation-news/aerospace/2020-08-17/us-nears-law-banning-chinese-drones)   
[11](https://www.ainonline.com/aviation-news/aerospace/2020-08-17/us-nears-law-banning-chinese-drones) <https://formobile-project.eu/>[.](https://www.ainonline.com/aviation-news/aerospace/2020-08-17/us-nears-law-banning-chinese-drones)

7

*E. Mantas and C. Patsakis*  *Array 14 (2022) 100135*



**Fig. 4.** Data acquisition techniques.

per se and the established forensics procedures and more coordinated efforts towards this direction. To this end, we prioritise the harmonisa-tion of manufacturers with common best practices from other platforms that will pave the way for procedures and tools could be established and developed.

**Declaration of competing interest**

The authors declare that they have no known competing finan-cial interests or personal relationships that could have appeared to influence the work reported in this paper.

**Acknowledgements**

This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the projects *Cyber-Sec4Europe*, Greece (Grant Agreement no. 830929) and *LOCARD*, Greece (Grant Agreement no. 832735). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

**References**

[1] Kovar D, Dominguez G, Murphy C. UAV (aka drone) forensics. 2016, URL [https://integriography.files.wordpress.com/2016/06/uav-forensics-ts16-final-distribution.pdf.](https://integriography.files.wordpress.com/2016/06/uav-forensics-ts16-final-distribution.pdf)

[2] [Kao D-Y, Chen M-C, Wu W-Y, Lin J-S, Chen C-H, Tsai F. Drone foren-sic investigation: DJI spark drone as a case study. Procedia Comput Sci 2019;159:1890–9, Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 23rd International Conference KES2019.](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb2)

[3] [Yousef M, Iqbal F. Drone forensics: A case study on a DJI mavic ai](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb2)r. In: 2019 IEEE/ACS 16th international conference on computer systems and applications. 2019, p. 1–3. <http://dx.doi.org/10.1109/AICCSA47632.2019.9035365>.

[4] Yousef M, Iqb[al F, Hussain M. Drone forensics: A detailed analysis of](http://dx.doi.org/10.1109/AICCSA47632.2019.9035365) emerging DJI models. In: 2020 11th international conference on information and commu-nication systems. 2020, p. 066–71. [http://dx.doi.org/10.1109/ICICS49469.2020. 239530](http://dx.doi.org/10.1109/ICICS49469.2020.239530).

[5] Kamoun F, Bouafif H, Iqbal F. Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. Int J Digit Crime Forensics 2019;12:1–23. <http://dx.doi.org/10.4018/IJDCF.2020010103>.

[6] [Clark D, Meffert C, Baggili I, Breitinger F. DRO](http://dx.doi.org/10.4018/IJDCF.2020010103)P (drone open source parser) your drone: Forensic analysis of the DJI phantom III. Digit Investig 2017;22:S3–14. <http://dx.doi.org/10.1016/j.diin.2017.06.013>.

[7] [Mantas E, Patsakis C. GRYPHON: Drone fo](http://dx.doi.org/10.1016/j.diin.2017.06.013)[rensics in dataflash and telemetry logs. In: Attrapadung N, Yagi T, editors. Advances in information and computer security. Cham: Springer International Publishing; 2019, p. 377–90.](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb7)

[8] [Yaacoub J-P, Salman O. Security analysis of drones systems: Attacks, limitations,](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb8)  [and recommendations. Internet Things 2020;100218.](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb8)

[9] [Europol. Internet organised crime threat assessment. European Union Agency for](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb9)  [Law Enforcement Cooperation (Europol); 2020.](http://refhub.elsevier.com/S2590-0056(22)00006-6/sb9)

8