HADMÉRNÖK
BIZTONSÁGTECHNIKA

19. évfolyam (2024) 2. szám 17–28.
DOI: 10.32567/hm.2024.2.2

József Répás[1]

Examining the Application of Drone Forensics Methodology on Highly Automated Civil and Military Vehicles

Abstract

One of the aims of digital forensics investigations of modern civil and military vehicles traffic accidents or other crimes is to establish what kind of incident occurred, when, where, and under what circumstances. As the automation level of vehicles increases, connected solutions become more widespread (e.g. drone–vehicle cooperation), and an accurate timeline of events and credible evidence can be provided in vehicles and connected drones. The forensic examination of drones deals with the exploration, processing, interpretation, and analysis of data stored in drones and sent through the established communication channel, some of the examination steps of which may be applicable in the case of vehicle examination. This study aims to examine one of the areas of digital forensics, Drone forensics, to determine which of its steps or procedures can be applied in the expert examination of highly automated and increasingly autonomous vehicles (e.g. military vehicles).

Keywords: unmanned aerial vehicle, drone forensics, digital forensics, autonomous vehicles, autonomous vehicle forensics

Introduction

The increase in the level of vehicle automation means the collection, processing, and management of more and more data in both civilian and military applications. While in civilian use the protection of personal data is one of the key issues, in operational terms, the protection of operational information appears. In data storage units of vehicles, the information is retained for a longer or shorter period depending on the purpose of use. This can be data related to the operation, traffic, or environment of the vehicle,

[1] PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: repas.jozsef@uni-nke.hu

but it can also refer to the driver or passengers. The cooperative operation of vehicles in intelligent transport systems and advanced communication technologies allow them to coordinate their manoeuvres with nearby vehicles and gather a wide range of information about their surroundings. Direct or mobile communication is possible with infrastructure, vehicles, smart networks, devices, and pedestrians. This allows vehicles to extend their own perception and localisation. Another extension could be the addition of drones to the detection and navigation of vehicles, i.e., with a drone connected to the vehicles, additional information can be collected and processed by the vehicles. This could further expand the range of data generated, collected, stored, and processed in vehicles.

Drones, or Unmanned Aerial Vehicles (UAVs), are used for several purposes, including creating photos and videos of large areas, conducting military operations, and conducting environmental surveys. As a result of technological developments, UAVs now include many additional technologies, including high-performance cameras, thermal scanners, and even military weapons. As a result, from a military perspective, UAVs are now part of the Internet of Battlefield Things (IoBT) ecosystem. In addition to UAVs, the IoBT ecosystem includes components such as networks of sensors, wearable devices, and other Internet of Things (IoT) devices. This ecosystem is expected to generate large amounts of data, enabling military personnel to respond to various situations on the battlefield.

The use of drones extends beyond legal limits (e.g. recreational and corporate) to illegal and other violent operational applications. They are used in cyberattacks (e.g. unauthorised access and monitoring, surveillance, rouge access point, etc.), invasion of privacy, trespassing, damage, violation of no-fly zones, information gathering, international espionage, reconnaissance, smuggling, support for terrorism, or IED attack. The wide range application and functionality of UAVs increase the chances that forensics examination may be necessary to investigate an event (e.g. an accident or incident).[2]

Drone forensics

"Digital forensics is a significant domain that involves capturing and analyzing cybercrimes. It has many branches: database forensics, IoT forensics, cloud forensics, drone forensics, wireless forensics, malware forensics, mobile forensics, network forensics, and data forensics. These branches have numerous and redundant forensics models, frameworks, approaches, policies, procedures, and tasks."[3]

Regardless of the size, structure, and operation of drones, depending on their use, they collect and store large amounts of information about their users, as well as about the detected events and locations. Given that the use of drones may pose a threat to national safety and security, a post-mortem forensics examination of intercepted or crashed drones may be necessary. Their data, as vital pieces of evidence

[2] Hankó 2021; Studiawan et al. 2023; Krajnc 2018.
[3] Alotaibi et al. 2022.

during a forensics examination, can contribute to the achievement of the investigation goals and the answer to forensics questions. Digital forensics has several subdomains, drone forensics is the one. Drone forensics has a wide range of applications beyond law enforcement. It can be used in various fields, including:

- counter-terrorism (espionage or terrorist activities)
- accident investigations (determine the cause and prevent future incidents)
- privacy law compliance[4]

Figure 1: Drone forensics
Source: www.cyforce.in/images/Drone-Forensics-India.jpg

It is the responsibility of drone forensics to recover, obtain, process and analyse this information. Data generated by drones, such as ID's, geolocations, flight path and history, time, images, and videos greatly contribute to the reconstruction of the events.[5]

Drones operate on a principle similar to that of computers. They have a processor, a data storage unit, communication ports, sensors, a camera, and a unit that determines their geographical location. The control of the device, as well as the transmission of data, is carried out by wireless communication. Existing digital forensics methods and techniques can be used. The process steps for computer, IoT, or mobile forensics can also apply to drones.[6] Expert examination of drones serves three main purposes.

[4] Riaz 2023.
[5] Alotaibi et al. 2022; Gustafson 2024; https://qccglobal.com/drone-forensics-services/; Répás 2023; Répás et al. 2022; Tiwari 2022.
[6] Kovar–Bollö 2021.

- The first category is the identification of the affected persons (suspect, victim), which is primarily the user of the drone or the victim, so in this case the investigation is aimed at how the device was controlled. The method of control may vary from manufacturer to manufacturer. For example, a remote controller, a smartphone that transmits commands to the drone, or a smartphone that provides direct communication with the device via Wi-Fi or Bluetooth. Both control methods leave different traces of digital evidence.[7]
- The second category includes the analysis and interpretation of flight data. In such a case, information collected by the drone's sensors and navigation data is processed. By analysing this data, it is possible to find out where the drone took off from or calculate the time of the drone's failure from the battery level. The reconstruction and analysis of the flight path of the drone and the flight track may be important mainly in the investigation of crimes related to smuggling.
- The third category of the investigation is the extraction and processing of existing data on the drone's data carrier.

Figure 2: Future directions and main purposes

Source: https://media.licdn.com/dms/image/D4D12AQGjrcq6s2uFyg/article-inline_image-shrink_1500_2232/0/1700476063621?e=1720051200&v=beta&t=Yk5l4d-9BIGxjLAj6cFuQKJqjAM1CH6LpmR0WKYtzQ8

Drone forensics challenges

Millions of unmanned aerial vehicles (UAVs) are registered across the globe, with almost half of them being used for commercial purposes. Apart from the registered UAVs, there are a significant number of devices being used privately. These are used for various illegal activities such as smuggling of illegal drugs, unauthorised surveillance, potential attacks, carrying explosives, and disrupting aviation.

[7] Azhar et al. 2018.

Drones have become a popular technology because of their various uses. They store a lot of information about both the events they captured and their users. Drone forensics is responsible for recovering, obtaining, processing, and analysing this information. The data generated by UAVs, such as flight path, time, images, and videos, are extremely helpful in reconstructing the events.[8]

Although the examination of drones is carried out using a procedure and approach similar to that of computers, mobile phones, or IoT devices, there are still physical, legal, and technical challenges in investigating them.[9]

Due to the diverse drone manufacturers, standards, operating systems, and infrastructure-based networks, the forensic examination of drones is a complex and unclear field. Many drone forensics models and frameworks have been designed based on various peer-review processes and activities, as well as possible scenarios for drone-related incidents, and numerous models, frameworks, methods, approaches, tools, and algorithms have been offered in the literature to conduct investigations on different UAVs. However, there is still a lack of a structured and unified model for managing and facilitating forensics tasks and activities in digital forensics.

Due to the current drone expert examination procedures and the protection of assets, access to data is not easy. One of the challenges of trace recording that we are looking for answers to is drones as sources of evidence. In investigating a drone-related event, basic forensic questions[10] need to be answered:

- Who: the persons involved (suspect, victim, eyewitness), proof of use, linking the device and the person using it
- Why: the trigger, motivation of the event
- Where: the location of the event under investigation or related relevant locations
- When: date of the event under investigation and related events (flight history firmware, upgrade, maintenance, etc.)
- What: a compilation of a timeline of events, a description of the facts (what happened during the flight, what flights the drone made, what route it travelled, etc.)
- How: how the event occurred, how it was committed (how the drone was used)
- With whom: connecting to the stakeholders (who), and establishing the role of the participants or co-perpetrators (who, or what services are connected to the drone)

As usual, when examining drones, not all questions have answers, or they are not stored in one device, in one place, or in one way. While the images and videos taken by the camera are stored on the memory card, flight, navigation information and operating parameters are stored in the internal storage of the drone (sometimes with limited capacity), but the remote control also contains information about the connected/controlled drone, and the logically connected mobile device and the files

[8] Répás 2023; https://digitpol.com/drone-forensics/; Gustafson 2024; Singh 2022; www.qccglobal.com/drone-forensics

[9] Vízi 2019; Almusayli et al. 2024.

[10] Fenyvesi 2013.

related to the application running on it may also contain data related to the flight, communication or live broadcast by the drone.

A distinction should be made between known and unknown (constantly developing) factory- and custom-built devices. In the absence of standardisation, different manufacturers use different solutions (drone-specific hardware and databases) both technically and logically, and in the case of custom-built drones, additional individual solutions (data storage, data access, unknown communication, etc.). Some drones can be accessed via FTP and Telnet protocol, while others can be accessed via direct USB. In addition, access permissions to the drone are different. In most cases, access is limited to the media folder or system files only. That is, there are currently no consistent tools to carry out the process of obtaining data from drones.

The drone may be damaged during flight, landing, or interception. Storage may also be damaged, or (temporarily) stored flight data may be lost due to power failure. In the absence of off navigation, connection problems, and geographical coordinates, knowing the flight path of the drone becomes almost impossible. The linking of the unique identifiers of the drone, the remote control, the related services, and the identity of the owner also complicates the investigation. There may also be technical obstacles, such as incompatibility, lack of software, drivers, or appropriate cables, or failure to connect via the USB port. The encryption used by drones, and different file systems can cause incompatibility, even within the same device (different file systems are also used within the same drone).

The way in which data is extracted and analysed may also vary, taking into account the need to ensure data integrity and authenticity, or individual data storage solutions and logical access. The use of anti-forensics solutions (the use of solutions and procedures that make it difficult or impossible to perform the test effectively) can also be applied to drones, which pose an additional challenge for investigators. Various encryption and deletion solutions (e.g. remote or timed deletion), data hiding, and metadata modification make it difficult to obtain evidence. Determining the type of drone or its controller when the signal is scraped or removed can also be difficult.[11]

Extracting data from drones for forensic examinations presents a significant hurdle: creating a standardised and repeatable process that aligns with forensic peer-review principles while preserving data integrity. This issue parallels the challenges faced in expert examinations of highly automated civil and military vehicles, where a universal procedure has not yet been established.[12]

Drone data

The first step in answering the examinations questions is to identify the source of the data, the test object (in this case the drone), and the potential evidence (the

[11] Atkinson et al. 2020; Kovar–Bollö 2021; Kao et al. 2019; www.salvationdata.com/knowledge/what-is-drone-forensics

[12] Répás 2023; Al-Room et al. 2021.

data in the drone). In general, drone forensics has defined three main phases that fit into each step of digital forensics: preparation, data acquisition, and analysis phase.[13]

During the examination of the drone, the evidence can be divided into three categories:

- physical evidence, the device itself
- digital evidence, storage of drone data, data stored in the cloud or on other devices
- other/miscellaneous evidence, e.g. social media, purchase records, DNA, fingerprints

Compared to the examination of vehicles, it can be concluded that physical evidence can also be evaluated by the vehicle itself, since it can be both the target, object (contains evidence), and the means of the crime.

Digital and other categories of data can be stored in the internal memory of the drone, external memory card, remote controller, connected mobile device (e.g. mobile, tablet, notebook), cloud-based systems (social media, forums), or service providers (e.g. mobile phone company, web account). The data can be found on the drone's communication channel (in transit) for some examination. Compared to the examination of vehicles, it can be concluded that, similarly to drones, digital evidence connected to vehicles can be found in the vehicle itself (internal data storage, e.g. ECU, HDD, SSD, memory card, etc.), connected mobile device, manufacturer and service provider clouds, or in environmental and track elements.

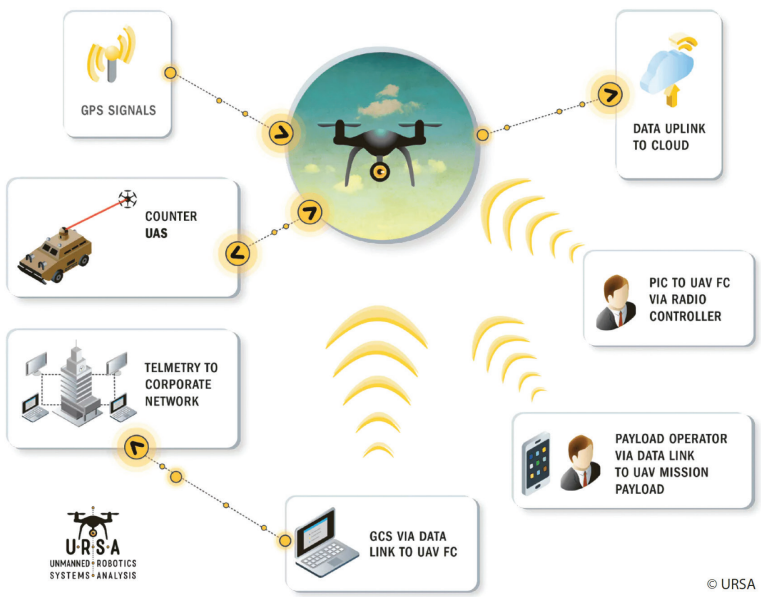

Figure 3: Drone connections
Source: www.japcc.org/wp-content/webp-express/webp-images/uploads/CUAS_Fig_19_1.png.webp

[13] Al-Dhaqm et al. 2021; Jain et al. 2017.

"Evidence from one source will lead you to evidence from other sources. Combined, they produce a compelling picture of the immediate flight, but also of operations, logistics and supply chain."[14] The stored data provides information about the identifiers of the drone and its components (e.g. remote controller, MAC, IMEI, IMSI), paired devices, software and firmware versions, and configurations. Flight track information includes landing, take-off, return locations (including frequent and preferred flight locations), and flight history (including known locations, home points, and routes travelled). Among operating parameters, GPS, telemetry, barometric data, state of the motor, and battery are recorded. The communication information about SSID, WiFi data, IP, and mobile communication (4G, 5G) connection. Information about payload, data recorded by sensors (photos, video recordings). In the case of vehicles, component identifiers, software, and firmware versions, or e.g., IMEI, IMSI numbers in connection with the Emergency call function are also stored. Flight track information in vehicles can be matched to track logs, and different flight parameters can be matched to the vehicle's operational and traffic parameters (see Figure 3).[15]

Drone forensics process

During the identification of evidence, if possible, the make, type, weight, and category of the drone should be determined, its individual characteristics (possible customisation, additional components) should be documented, and its physical condition assessed. For devices of well-known manufacturers, it is necessary to review the manufacturer's documentation, and in the case of drones developed individually and not known by expert software, obtaining and reviewing the controller manufacturer's documentation. Based on the documentation, the methods of accessing the data can be learned (e.g. API, interface, file system, operating system). If the device is unique or the control is not known and no information is available from documentation or other sources, physical or logical access to data can be achieved with individual solutions at considerable time and cost. Some manufacturers provide direct access to drone on-board logs via USB port, but there are also solutions where the information is stored on an SD card glued to the motherboard. Drone control applications can also provide an option for flight logs, however, this solution is not always stable, as the files can be corrupted, and do not contain all flight path information. In the case of a drone with severe electronic damage, data extraction can only be obtained by connecting to JTAG points or chip-off directly from the chip by removing the integrated media.[16]

The first step of the effective drone forensic process is preparation. In the preparation phase, data storage must be explored and identified, and the operability of devices must be checked. During a logical assessment, the drone's wireless network connections (Wi-Fi, Bluetooth, etc.), navigation, and data storage are checked.

[14] Kovar–Bollö 2021.
[15] Kovar–Bollö 2021; Tiwari 2022.
[16] Kovar–Bollö 2021.

In the acquisition phase, all steps, activities, and processes of obtaining and preserving relevant data from identified data sources should be documented. Create a Working Copy, or a physical or logical image of the data storage (in order to reduce the chance of damaging evidence, it should only be activated once).[17]

During the analysis phase, the data obtained should be examined and analysed to identify and uncover evidence. The analysis can be done manually or with the help of software using an automated method. In the practice of computer forensics, analysis is largely done with some kind of interactive tool, which must recognise and analyse the data structures and metadata embedded in the extracted data. In the case of drones, such solutions are implemented thanks to the expansion of the functionality of certain mobile forensics solutions. They have been supplemented with functions and options that make them suitable for examining drones as well. For example, the application can identify files by header or recover deleted files (in this case, it recovers individual entries in the file system and compiles the file afterward). It is extremely important to select and separate the wheat, i.e., relevant evidence.

If appropriate information is available about the device, such as a known factory device, some data can be accessed even with the help of free tools, which contribute to the achievement of the test purposes. During the compilation of the event itself and the timeline of the events, it is determined what kind of event occurred in which the investigated drone played a role.

The test shall ensure that subsequent remote manipulation of the data (erasing, modifying, or factory reset) is excluded. Therefore, if the drone is still operational, it must be switched off and data must be kept safe.

During the examination of drones, the interpretation of the extracted data also belongs to the analysis phase. There are several important aspects to evaluate, and interpret results, as well as elements that are likely to be overlooked, such as:

- the meaning of all relevant data has been properly interpreted
- whether the study was prevented (e.g. by anti-forensics solutions)
- timestamps are consistent
- how expert independence has been ensured

As a result of the analysis and interpretation, the answers appropriate to the purpose of the study, the event under investigation, and the supporting evidence are produced. The last phase of drone forensics is reporting.

Conclusions

Drones – unmanned aerial vehicles – are used for various purposes, including mapping, creating photos, and videos of large areas, managing environmental surveys, and conducting military operations. The increasing use and functionality of UAVs increase the chances that a digital forensics investigation may be required to examine the circumstances of an event. As a result, both industry and academia have issued

[17] Alhussan et al. 2022.

numerous guidelines and publications on expert testing of UAVs. However, survey results show the need for an enhanced digital forensic framework to support future expert investigations of these vehicles. In this study, the aim was to determine the common points of the investigation of UAVs and forensics for modern transport vehicles and to analyse which steps and elements of the drone forensics procedure can be applied during the examination of highly automated vehicles. In addition, data storage solutions for drones and vehicles and categories of stored data were compared. Reviewing the forensics examination of drones, it can be concluded that this is a continuously developing field with similar examination challenges. The devices, methods of use, and control show a mixed picture, therefore complex, flexible, easy-to-use solutions need to be applied. The test steps do not go beyond the general steps of digital forensics, they can be partially or fully applied to drones. The process steps listed in this study and their content are similar to those of vehicle-related tests, but in the case of vehicle testing, several process steps and specific characteristics need to be taken into account.

Acknowledgement

Prepared with the professional support of the Doctoral Student Scholarship Program of the Cooperative Doctoral Program of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund.

The author would like to especially thank the managing director and staff of Alverad Technology Focus Ltd. for their support for the research work.

References

Al-Dhaqm, Arafat – Ikuesan, Richard A. – Kebande, Victor R. – Razak, Shukor – Ghabban, Fahad M. (2021): Research Challenges and Opportunities in Drone Forensics Models. *Electronics,* 10(13), 1519. Online: https://doi.org/10.3390/electronics10131519

Al-Room, Khalifa – Iqbal, Farkhund – Baker, Thar (2021): Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. *International Journal of Digital Crime and Forensics,* 13(1), 1–25. Online: https://doi.org/10.4018/IJDCF.2021010101

Alhussan, Amel A. – Al-Dhaqm, Arafat – Yafooz, Wael M. S. – Razak, Shukor Bin Abd – Emara, Abdel-Hamid M. – Khafaga, Doaa S. (2022): Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics,* 11(8), 1168. Online: https://doi.org/10.3390/electronics11081168

Almusayli, Asma – Zia, Tanveer – Qazi, Emad-ul-Haq (2024): Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. *Technologies,* 12(1), 11. Online: https://doi.org/10.3390/technologies12010011

Alotaibi, Fahad Mazaed – Al-Dhaqm, Arafat – Al-Otaibi, Yasser D. (2022): A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Computational Intelligence and Neuroscience,* (1), 1–13. Online: https://doi.org/10.1155%2F2022%2F8002963

Atkinson, S. – Carr, G. – Shaw, C. – Zargari, Shahrzad (2020): Drone Forensics: The Impact and Challenges. In Montasari, Reza – Jahankhani, Hmaid – Hill, Richard – Parkinson, Simon (eds.): *Advanced Sciences and Technologies for Security Applications.* Springer, 65–124. Online: https://doi.org/10.1007/978-3-030-60425-7_4

Azhar, M. A. Hannan Bin – Barton, Thomas Edward – Islam, Tasmina (2018): Drone Forensic Analysis Using Open Source Tools. *Journal of Digital Forensics, Security and Law,* 13(1), 7–30. Online: https://doi.org/10.15394/jdfsl.2018.1513

Fenyvesi, Csaba (2013): A kriminalisztika alapkérdései. In Gaál, Gyula – Hautzinger, Zoltán (eds.): *Pécsi Határőr Tudományos Közlemények XIV.* Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 341–349. Online: www.pecshor.hu/periodika/XIV/fenyvesics.pdf

Gustafson, Kimmy (2024): Modern Forensic Science Technologies. *Forensics Colleges,* 9 February 2024. Online: www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

Hankó, Viktória (2021): A drónokkal kapcsolatos kockázatok és kezelési lehetőségeik. *Hadmérnök,* 16(3), 189–202. Online: https://doi.org/10.32567/hm.2021.3.11

Jain, Upasita – Rogers, Marcus – Matson, Eric T. (2017): Drone Forensic Framework: Sensor and Data Identification and Verification. In *2017 IEEE Sensors Applications Symposium* (SAS), Glassboro, NJ, USA, 1–6. Online: https://doi.org/10.1109/SAS.2017.7894059

Kao, Da-Yu – Chen, Min-Ching – Wu, Wen-Ying – Lin, Jsen-Shung – Chen, Chien-Hung – Tsai, Fuching (2019): Drone Forensic Investigation: DJI Spark Drone as A Case Study. *Procedia Computer Science,* 159, 1890–1899. Online: https://doi.org/10.1016/j.procs.2019.09.361

Kovar, David – Bollö, Joel (2021): Drone Forensics. *JAPCC.org,* January 2021. Online: www.japcc.org/chapters/c-uas-drone-forensics/

Krajnc, Zoltán (2018): Drónok, hibrid fenyegetés, terrorizmus a légtérből: A légi hadviselés privatizálása. *Hadmérnök,* 13(4), 358–369. Online: https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/3705

Riaz, Talha (2023): Digital Forensics on Drones: Tools, Techniques, and Real-World Applications. *Linkedin,* 20 November 2023. www.linkedin.com/pulse/digital-forensics-drones-tools-techniques-real-world-talha-riaz-qrilf/

Répás, József (2023): Definition of Forensic Methodologies for Autonomous Vehicles. *Hadmérnök,* 18(1), 125–141. Online: https://doi.org/10.32567/hm.2023.1.9

Répás, József – Schmidt, Miklós – Vitai, Miklós – Berek, Lajos (2022): *Mit árul el rólunk az autónk? – Modern járművek IT szakértői vizsgálatának kérdései és lehetőségei* [What Does Our Car Tell about Us? – Questions and Possibilities of Digital Forensic Analysis of Modern Vehicles]. Pécs: Szentágothai János Szakkollégiumi Egyesület.

Studiawan, Hudan – Grispos, George – Choo, Kim-Kwang Raymond (2023): Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unadd-

ressed. *Computers & Security,* 132, 103340. Online: https://doi.org/10.1016/j.cose.2023.103340

Tiwari, Ashwani (2022): Drone Forensics: An Unrevealed Dome. *Data Forensics,* 19 April 2022. Online: www.dataforensics.org/drone-forensics/

Vízi, Linda (2019): *A Computer Forensics jogi vonzata.* Online: https://netacademia.hu/courses/take/computer-jog/multimedia/8481853-figyelem-ez-egy-classic-tanfolyam