Digital Forensic in 2023

Tri Dai Ho

School of Cyber Education, UMGC-Global

CCJS 321-7382: Digital Forensics in the Criminal Justice System

Professor Maurice Hicks

7th May 2023

Describe ethical dilemmas that a digital forensic practitioner may encounter and what steps they should take to ensure their integrity is not called into question.

The job of a digital forensic practitioner (DFP) is to extract relevant data, analyze and present the findings in their purest state but in a readable format. As Boddington (2016) brilliantly states, “Evidence is blind and cannot speak for itself” the digital practitioner will often need to offer their expert opinion on what a particular piece of digital evidence means. The co-existence of both suspect-based and evidence-based investigation approaches can often put the DFP in an entanglement of the process of elimination logic. On the one hand, the DFP can purposely seek evidence that can prove or disprove the accusation of one suspect. This approach is much more in favor of the rest of the investigation team since they can start honing into a suspect or looking elsewhere. The DFP also benefit from it since they could consider that their findings help establish a case and move on to a long list of other devices waiting to be analyzed. However, this approach can potentially leave many stones unturned and biased toward the suspect and not captivate the entire essence of the evidence. According to Johannesson & Persons (2014), grounded theory does not start with a hypothesis to be tested but with data from which a theory can be generated. In this spirit, a case must be established strictly on the foundation of evidence and to the extent that said evidence remains unquestionable.

Secondly, the DFP also frequently comes across encrypted devices or locked devices. One way to solve this challenge is by checking the vulnerability database and exploiting them to access the interest data, according to Servida & Casey (2019). However, there is also an ethical dilemma that exists in this practice. Should the DFP report the vulnerability to

the manufacturer to improve the device security, which also makes the job of the DFP more complicated and demanding when the vulnerability receives a patch?

Moreover, digital forensics is still in its infancy compared to others in the IT sector, and this field is so new that no universal data extraction and interpretation standards exist. Additionally, many toolkits used by DFP are commercially developed elsewhere and have yet to be reviewed or field tested by any forensic or legal entities. As Sharevski (2015) claims, this is due to a need for a general governance body in digital forensics. For this reason, the findings often face great scrutiny from both the jury and attorney, which in turn places the DFP in a position of having no defined way to verify the evidence. Boddington (2016) also points to the inferiority of digital forensic equipment, further explaining the instability of the work. On the one hand, it is nearly impossible to recheck the findings using every possible methodology and available technique. On the other hand, DFP has no reliable way to tell if the hardware or their toolkit might contain a default false positive or negative, let alone the range of these errors.

When facing surmounting ethical challenges, as mentioned above, the DFP can still rely on proven best practices as guidance to carry out their work. The key is documenting every step, tool, finding, and chain of custody. Maratsi et al. (2022) suggest the following sequence to increase the soundness of evidence and its admissibility in court:

For offline forensic acquisitions

• Save the original material as it is.

• Take photos of physical evidence and a screenshot of evidence content.

• Document temporal information, date, time, etc.

• Inject the bit-by-bit copy into the forensic computer.

• Implement an Access Control List (ACL) only to allow certain people to access specific data according to their role in the investigation in the particular case. This will help increase accountability and decrease the chance of accidental mistakes by unauthorized people accessing this data. (Fewer people have hands on the data without absolutely needing to). The forensic system could operate on a reference monitor architecture where every operation (read, write, etc.) by subjects on the data is monitored to prevent unauthorized modification.

• Document everything.

<u>For live forensic acquisition</u>

• Freeze the current state of the computer to image RAM. This helps ensure that there have been no modifications during the acquisition (although not bulletproof).

• Swap the hard disk with forensic hardware in the principle of a shadow drive (place a drive between the motherboard and hard disk).

• Take the shadow drive and inject it into the forensic computer.

• Follow the same last three steps of offline forensics.

Maratsi et al. (2022) also suggest using an external reviewer to examine the data pseudonymously. Since the true identities of the person are omitted, the external reviewer can still follow the steps taken by DFP and preserve the unlinkability property of evidence.

Research and describe IoT devices. What are their functions, and what problems are they designed to solve for the user? What data valuable to an investigation is created by each

device? Besides the device, where might data from the IoT device be stored, and how can it be acquired?

QBee multi-sensor camera is a multifunctional camera designed for monitoring and surveillance that can be used at home, work, and in public areas. According to Axis Communication (2023), multisensor cameras produce high-resolution images and footage with a broad range of coverage. They are ideal for perimeter monitoring around critical infrastructure and public or private buildings. The forensic value of the multisensor camera is extraordinary. These cameras typically locate in very strategic areas and high up, which increases their surveillance footprint and away from the most destructive factor, making them ideal for evidence gathering. The sensor can be triggered by audio, image, or motion. This aids the investigation tremendously since it has a high chance of having a record of the incident, and the officers can look through the sensor-detected records. The ample storage on the camera and cloud allow for more extended recording and more space. This means the memory potential for the camera is more significant and can store the evidence for an extended period before it gets deleted. According to Servida and Casey (2019), even though the QBee camera's local data is encrypted, the cloud credential of Qbee can be cracked using the Python decryption function and a plugin using the Autopsy framework. Qbee cloud credentials allow access to its cloud storage, where data are in a readable format and can be analyzed.

Arlo Pro from Netgear is another IoT device in the surveillance camera family. Unlike Qbee, Arlo Pro possesses a wide lens of 130 degrees, which makes up for a lesser range of movement. Arlo Pro is very user-friendly and weatherproof. According to Passingham (2017), Arlo Pro is ideal for monitoring large properties and outdoor activities, thanks to its

night vision capability. The camera can be controlled through an app on a smartphone. Like most surveillance cameras, Arlo Pro is typically installed in a strategic location that allows a broad view and recording of activities that are going on. Arlo Pro is compact, completely wireless, and with night vision. These features appeal to investigators since they make the camera very hard to detect and potentially yield critical evidence to the case. Arlo Pro does not have internal storage, as Passingham (2017) explains, to conserve the space for processing power. This means all recordings and images are stored externally or uploaded to the cloud or USB drive. This is particularly important to the digital investigator since they must retrieve the external hard drive or the cloud storage credential to access the data. Servida and Casey (2019) were able to access the memory dump of the Arlo system by interfering with its bootloader. The researcher succeeded in establishing telnet access to Arlo station and obtained a partial file system copy of the device through root access. Servida & Casey (2019) discovered traces collected from the Arlo provide details about cameras connected to the station and their last settings, to all the logs from the device's last factory reset, including timestamps of the motion detection events from the connected camera.

Amazon Echo is an intelligent interface delivering commands to the IoT infrastructure. The user can activate the connected light bulbs with a voice command. According to Bouchaud et al. (2021), Amazon Echo can contain information about the user, the network, and a set of activity logs related to the system, current operation, events, and exchanges with the network. The mobile application also concentrates on the history of interactions and requests from the voice assistant. Bouchard et al. (2021) further emphasize the importance of the event logs notifying the action of capturing a sound at the time of the event.

However, the sound recordings are stored on the Amazon cloud. In this case, cloud forensic techniques might need to be employed to access the sound recording. However, it can be done with assistance from Amazon Cloud Administrator and through the legal process. One vital benefit of storing the record in the Cloud is that it can preserve the integrity of the evidence and will not get tampered with even with device destruction.

Wink Hub is one of the earliest intelligent home hubs, boasting many radios, including Z-Wave, Zigbee, Lutron Clear Connect, Thread, Wi-Fi, and Bluetooth. It is the only hub to work with Kidde's connected smoke alarms and supports Amazon Alexa voice control (Tuohy, 2022). Wink has broad device support for door locks, lights, thermostats, and sensors, allowing users to control remotely from a smartphone app. Wink hub data is relevant to understanding the local network's architecture, according to Bouchard et al. (2021). This gateway contains all the network events and the identifiers of the connected equipment. It identifies and maps the path and the ascent of the data through the connected infrastructure to the Internet. Analyzing the dependency link with the iPhone is appropriate for digital investigations. This connection informs the geographical proximity of the smartphone (Bouchard et al., 2021). Since Wink Hub is an internal bridge that links all the IoT devices on one network, direct device access will yield more potential evidence in this case. Servida & Casey (2019) were able to obtain a root shell on the Linux system, which was used to acquire an entire filesystem via SSH protocol. According to the author, Wink Hub filesystem includes the station's configuration settings and connected device and system log. One thing worth noticing is that this information concerns only the device directly connected to Wink Hub and not only the ones in the Wink Hub account (Servida & Casey, 2019).

The Terraillon Dot is developed to encounter insomnia and promote general health and well-being through good sleep. The device is equipped with 16 possible ambient light modes and six external sound speakers to help the user to f as asleep and wake up naturally. Its environment and sleep analysis tracks temperature, humidity, noise level, brightness, sleep duration, cycle, and body movement. Bouchard et al. (2021) point out that the Terraillon dot contains the latest measurements, network configuration, and synchronization information. The uploading of data is triggered manually from the mobile application. It contains data on the user (numerical user profile and health information), the network, synchronization events, and all health measurements over the last 30 days (sleep duration, lift/bed rest, body movement, etc.) (Bouchard et al., 2021).

How do criminals and terrorists use drones, and what can law enforcement do to combat using drones in illegal activities?

Drone technology upscales the battle between law enforcement and criminal activities. There is no longer a time when only government entities and travel agencies can access aerial space. Drone technology helps to keep the pilot secure in a remote location while performing air surveillance. Both state and private parties are significantly leveraging this technology.

<u>Drone usage:</u>

The drone can be used to smuggle contraband across the border or to deliver illegal substances. According to Tarantola (2017), in 2015, there were two records of illegal substances transport and delivery using drones. Tarantola (2017) points to the fact that

drones are easy to fly and difficult to spot as the primary reasons why criminals are in favor of this technology.

The drone can be used to spy on the authorities and alert the criminal of law presence. Australian law enforcement captured seven suspects in smuggling $30 million worth of cocaine into the country in 2017, according to Tarantola (2017). In this case, the criminal used the drone to monitor the police and serve as an early warning system.

The drone can be used to shoulder surfing ATM patrons. Crawford and Frater (2018) note an incident in Northern Ireland where a drone was used to monitor ATM patrons with the potential to steal their PIN and banking credentials.

The Islamic State militant group (ISIS) also has an army of drones in its arsenal. According to Crawford and Frater (2018), ISIS drones are inexpensive and portable, which belong to two classes. Class I drones are carriers to drop explosives on counterinsurgency forces, and class II drones will fly toward the target and self-detonate.

Counter drone:

Law enforcement can use a 12-gauge shotgun with a specific drone munition to shoot down the drone. One of which is the SKYNET Mi-5 shell, a modified 12 gauge that shoots out a 5-foot-wide capture net to entangle the propeller of most drones causing it to fail (*12 Gauge: SKYNET™ Mi-5*, n.d.).

On the other hand, the Navy Special Warfare Command decided to use a radio frequency jammer that can be mounted on a vehicle, according to Tarantola (2017). This device is designed to identify, track, and disable enemy UAVs that can come too close to friendly

forces. Another less bulky and cost-effective option is DroneGun, developed by DroneShield. This handheld rifle style sends radio frequency down the drone or back to its starting point (*DroneGun Tactical Counterdrone (C-UAS) Protection*, n.d.). The most significant advantage of this method is that it allows the targeted drone to land control manner and preserve the hardware component for forensics.

Besides shooting down the drone with a unique weapon, drone virus is a more sophisticated, elegant, and practical option. According to Tarantola (2017), as early as 2015, software engineers started to join the anti-drone domain with drone malware. Tarantola (2017) noted that software like Maldrone is Python-based scripts designed to override the drone driver and sensor using a Wi-Fi network.

Another approach to combat illegal drone operations is establishing a no-fly zone for drones. The authorities can also contact well-known drone manufacturers as a request for make and model using the serial ID of the drone for better monitoring the drone and tracking the pilot as needed.

Where do drones store their data, and what types of valuable information can be found?

A drone can come in multiple sizes and shapes with different features. In many ways, a drone functions like a computer with a data storage unit such as an SD card, USB ports, and CPU (*What Is Drone Forensics? - Salvation DATA*, 2023). Some drones can have cameras and sensors. Sometimes to lighten the design, the manufacturer can store the storage externally from the device, for example, in the cloud or a private server. Salvation DATA (2023) states that a drone is a data-rich device that can uncover information. Refer to Table 1 for types of data that can be extracted from a drone (*What Is Drone Forensics? - Salvation DATA*, 2023).

Captured data	Technical detail
Data about the drone's operator Photos taken Video footage captured Landing, launch, returning, and home locations (including common and preferred flying locations) Flight history (including the exact locations and the routes taken) Flight plans and purpose The altitude of the unit at every point of its travel Payload weights Protected zone activity logs Paired devices Atmospheric conditions that were in effect during each stage of the flight	Dates and timestamps (geo locations, photos, and videos) Controller ID EXIF Metadata GPS status during flight Drone's serial number Internal components (MAC, IMEI, IMSI) SSID WiFi data IP Bluetooth 3G and 4G connectivity status Firmware version Pilot control input Pilot-configured settings

	File system data Registry entries

Research new and developing technologies to determine what devices, software, or capabilities are emerging. Select two. Describe this new technology, how criminal or terrorist networks can use it, and how authorities can combat the threat.

Technology is ever-evolving faster than any other revolution we have witnessed throughout history. In the wake of the new trend in technology development, the landscape of anti-terrorism and criminal investigation is also changing rapidly. Quimbre and Silfversten (n.d) sum up the newest development in technologies that can be further developed and leveraged by criminals worldwide.

- **Artificial Intelligence/Machine Learning**

  AI and machine learning (ML) could increase attacks' automation, speed, frequency, efficiency, and the potential for tailored attacks targeting specific groups. Caldwell et al. (2020) argue that this robust technology, even at its current stage, can still significantly impact already established crimes, such as fraudulence, extortion, and distrust. AI-powered Deepfake technologies produce impeccable fake images and videos that can only be distinguished by a dedicated computer lab expert. A fake scandalous image can provide the

perfect bait for a blackmail attempt, or a fake recording or video can produce a convincing reason for the victim to bite in a phishing case. Just as criminals use AI to commit crimes, law enforcement and agencies also leverage this technology to predict, prevent, and potentially solve crime. The welcoming news is that researchers worldwide have been extensively studying the criminal justice application of AI and Machine Learning for a while, even before the public release of ChatGPT by OpenAi. As an example, Dakalbab et al. (2022) was able to leverage ML with statistical data and previous academic works to predict criminal behavior and crime hotspot with a high level of precision.

- **Autonomous Devices and Systems**

  As Caldwell et al. (2020) recognized, the reality of driverless vehicles is still unavailable. However, newer car models have already implemented autonomous parking and traffic recognition. This new technology could be used to carry out disguised criminal acts, develop new operation methods for criminals, or conduct large-scale and automated attacks. They may also increase the complexity of forensic investigations and make it harder to identify the source of crimes caused by autonomous devices.

- **Blockchain and Distributed Ledger Technologies (DLTs)**

  As transactions become digitalized and processed through DLTs, these could be manipulated for malicious purposes, such as preventing transactions from being processed. DLTs could also store disruptive or inappropriate content that could become difficult to remove. The essence of blockchain and DLT make this technology very hard to crack when used for transaction verification and encryption. Firstly, the decentralized nature of DLT, means that illegal transactions can be done digitally without passing through any credited financial institution. Secondly, the SHA256

hashing algorithm is designed as one-way encryption in which you have the key or must try one combination at a time. As the old saying goes: if we can go against it, then be with it. Digital forensic practitioners can use this technology to support the chain of custody process that is currently in existence, as suggested by Tsai (2021).

- **Computing and Data Storage Technologies**

  The development and increasing use of computing and data storage technologies could be exploited by criminals to gain access to and disseminate non-consensual recordings and illicit data.

- **Telecommunication Infrastructure**

  Technological advances could be used to enhance the anonymity, speed, and capacity of criminal activities or to steal personal and sensitive data. Telecommunication infrastructure could also be targeted to cause large-scale disruption.

- **Internet of Things (IoT)**

  Growing volumes of data collected by IoT devices could become vulnerable to theft, corruption, destruction, extortion, or sale. IoT devices are also likely to increase the scope of attacks for cyber-dependent crimes and introduce new vulnerabilities in complex IT systems and environments.

- **Privacy-Enhancing Technologies (PETs)**

  Malicious actors could exploit PETs to pursue illicit activities anonymously and secretly, making it increasingly difficult to detect, monitor and investigate criminal activity. Malicious actors could also target PETs to access confidential or private information.

References

12 Gauge: SKYNET™ Mi-5. (n.d.). https://www.lesslethal.com/products/12-gauge/als12skymi-5-detail

Caldwell, M. E., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1). https://doi.org/10.1186/s40163-020-00123-8

Boddington, R. (2016). *Practical Digital Forensics*. Packt Publishing. http://ezproxy.umgc.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1242578&site=eds-live&scope=site&ebv=EB&ppid=pp_FM-2

Bouchaud, F., Vantroys, T., & Grimaud, G. (2021). Forensic analysis of IoT ecosystem. *HAL Open Science*. https://hal.science/hal-03369836

Crawford, J., & Frater, J. (2018, July 26). 10 crimes were committed using a drone. *Listverse*. Retrieved May 6, 2023, from https://listverse.com/2018/07/26/10-crimes-committed-using-a-drone/

Dakalbab, F. M., Talib, M. A., Waraga, O. A., Nassif, A. B., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. *Social Sciences & Humanities Open*, *6*(1), 100342. https://doi.org/10.1016/j.ssaho.2022.100342

DroneGun tactical counterdrone (C-UAS) protection. (n.d.). AI-enabled Multi-Mission Solutions. Retrieved May 6, 2023, from https://www.droneshield.com/products/dronegun-tactical/

Johannesson, P., & Perjons, E. (2014). An introduction to design science. In *Springer eBooks*. https://doi.org/10.1007/978-3-319-10632-8

https://www.rand.org/randeurope/research/projects/technological-developments-and-the-future-of-cybercrime.html

Maratsi, M. I., Popov, O., Alexopoulos, C., & Charalabidis, Y. (2022). *Ethical and legal aspects of digital forensics algorithms: The case of digital evidence acquisition*. https://doi.org/10.1145/3560107.3560114

Multisensor cameras | Axis Communications. (n.d.). https://www.axis.com/products/multisensor-cameras

Passingham, M. (2017, July 19). *Netgear Arlo Pro*. Trusted Reviews. Retrieved May 6, 2023, from https://www.trustedreviews.com/reviews/netgear-arlo-pro

Quimbre, F., & Silfversten, E. (n.d.). *Technological developments and the future of cybercrime*. RAND Corporation. Retrieved May 7, 2023, from What is drone forensics? - Salvation DATA. (2023, February 10). *Salvation DATA*. Retrieved May 6, 2023, from https://www.salvationdata.com/knowledge/what-is-drone-forensics/

Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation*, *28*, S22–S29. https://doi.org/10.1016/j.diin.2019.01.012

Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2015.1201

Tarantola, A. (2017, October 11). *The rise of drone crime and how cops can stop it*. Engadget. Retrieved May 6, 2023, from https://www.engadget.com/2017-10-11-drone-crime-how-cops-stop-it.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmRlLw&guce_referrer_sig=AQAAADTdoflS2XLaiSw2Vvy-Kv3Mnk76Otv91V_Fosn2sCEAL8fbV9ugq0M1kv8vq8yIscIZpXJse8WP5D-hGoITRFj7Y5aTFCUjftrGgHfjjk_FvJknbJlhRFEqbO-rV9efQzzFEfLcFk5dAptpHmdFN2hmYxsczWPPtwZHPBQbOqjJ

Tuohy, J. P. (2022, July 14). Wink's smart home service has been down for weeks, is this the end? *The Verge*. Retrieved May 6, 2023, from https://www.theverge.com/2022/7/14/23217086/wink-smart-home-hub-outage

Tsai, F. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, *192*, 2779–2788. https://doi.org/10.1016/j.procs.2021.09.048

What is drone forensics? - salvation DATA. (2023, February 10). Salvation DATA. Retrieved May 7, 2023, from https://www.salvationdata.com/knowledge/what-is-drone-forensics/