Forensic Science International: Digital Investigation 45 (2023) 301558

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 USA - Proceedings of the Twenty Third Annual DFRWS Conference

Dashcam forensic investigation guidelines

Harjinder Singh Lallie

WMG, University of Warwick, Coventry, CV4 7AL, UK

ARTICLE INFO

Article history:

Keywords:
Digital forensics
Dashcam
Investigation guidelines

ABSTRACT

Dashboard cameras ("dashcams") have become an important in-car accessory used to record audio and visual footage of car journeys. Dashcams appear more often in digital investigations and will become more prevalent with the growth of autonomous vehicles. The audio/video footage produced by dashcams contain important items of evidence, including the routes followed by the motor vehicle, video footage of the road ahead, the road behind and the cabin, as well as audio footage of conversations within the car.

However, there exist no tools or guidelines on how these devices should be investigated, this could lead to cases of miscarriage of justice. This paper provides an overview of the key features of forensic interest within a dashcam device, followed by guidance on how to respond at a crime scene which involves a dashcam device and in particular how to preserve the evidence found therein.

This is followed by with guidelines on how to acquire the evidence in a dashcam device, the problems and challenges involved in the examination and analysis of dashcams, before finishing with a discussion around the reporting and presentation of dashcam evidence.

1. Introduction

A dashboard camera ("dashcam") is an in-vehicle mountable camera which records video and audio footage of vehicle journeys. Dashcams create numerous artefacts of evidential value such as GPS data, temporal data, vehicular speed data, audio, video and photographic images. Generally, there are three types of dashcam, these are (i) 'inbuilt' dashcams which are factory fitted to the vehicle (ii) after-market user-installed dashcams (iii) and app based dashcams (Tummala et al., 2019).

Lallie (2020) demonstrated that increasing numbers of police forces, particularly in the UK, are accepting dashcam evidence. This is expected to continue worldwide. The paper also outlined the range of recoverable dashcam evidence.

Notwithstanding the contribution by Lallie (2020), there appear to be no guidelines on how to investigate the evidence contained within dashcam devices, i,e, the sequence of steps to follow. In the absence of such guidelines, there is a risk that investigations could become compromised, and evidence tainted. This paper contributes to this research gap by proposing a set of dashcam investigation guidelines. This is the first set of guidelines known to the author, and should act as an important reference point for investigators presented with dashcam devices.

There exist innumerable investigation models, and we want to avoid creating another model. The guidelines proposed herein are based around an existing accepted forensic investigation model, namely that proposed by Ayers et al. (2014) which proposes mobile device investigation guidance. The present contribution does not repeat some of the generic guidance provided by Ayers et al., for example, the need to maintain chain of custody, sealing evidence, transporting to a forensic laboratory etc., and assumes that the reader can become familiarised on these concepts through other sources.

This paper organises the investigation into the same steps as Ayers et al., namely: *preservation, acquisition, examination and analysis*, and *reporting*. The discussion begins in Section 2 with an overview of the background followed by Section 3 which provides an overview of the key features of forensic interest within a dashcam device. This is followed in Section 4 with guidance on how to respond at a crime scene which involves a dashcam device and in particular how to *preserve* the evidence found therein. This is followed in Section 5 with advice on how to *acquire* the evidence in a dashcam device. The problems and challenges involved in the *examination and analysis* of dashcams is presented in Section 6. The final section (Section 7) ends with a discussion around the *reporting and presentation* of dashcam evidence.

E-mail address: HL@warwick.ac.uk.

https://doi.org/10.1016/j.fsidi.2023.301558

2. Background

Dashcam forensics draws together several forensic domains including traditional file system forensics and video/imagery/audio forensics. The predominance of research into video/imagery/audio forensics is evidenced by a number of literature reviews which focus on: watermarking as a means of authenticating recordings (Asikuzzaman and Pickering, 2018); source camera identification, forgery detection, and steganalysis (Rocha et al., 2011); and published literature in the domain of video forgery/tamper detection, video re-capture, phylogeny detection, video anti-forensics and counter anti-forensics (Singh and Aggarwal, 2018).

Similarly, several contributions investigate the problem of image forgery (Wu et al., 2022; Kaur et al., 2023; Tyagi and Yadav, 2022). Although image forgery is a concern in dashcam forensics, given that most of the evidence is video based, the present review does not focus on this area.

The remainder of this review outlines previous research into assessing vehicle speed; extracting elements such as text from recordings; assessing the authenticity of the source camera, source vehicle and the video itself; and addressing privacy concerns.

2.1. Vehicle speed

Vehicular speed, an important evidential artefact, appears in several locations within the dashcam as described in Lallie, (2020). These locations include: EXIF data, the NMEA file and the watermark. The NMEA (National Marine Electronics Association) file is a form of geospatial data representation which existed prior to GPS systems. Watermarks in the present context are metadata watermarks which can include speed, date, and geospatial data. However, where vehicular speed is available (Kafer, 2018), has questioned the extent to which this can be relied upon. It is noteworthy that the presence of vehicular speed in the watermark can be disabled by the user.

Several complimentary methods of estimating vehicular speed have been proposed. For example (Kamat and Kinsman, 2017), used uniformly spaced road markers painted on roads to estimate vehicular speed, and (Kim et al., 2018) proposed the *vehicle speed estimate method (VSEM)* as a means of estimating vehicle speed. A review of vehicle speed detection methods is provided in Zhou et al., (2022).

2.2. Text/object extraction

Previous research has attempted to extract text from watermarks using a *Fully Convolutional Network* (FCN) model (Zhang et al., 2016) or a *Convolutional Neural Network* (CNN) model (Jaderberg et al., 2016). (Al-maweri et al., 2016) extracted data from the watermark and (Li and Shen, 2016) extracted licence plate numbers from the recorded scene. Research in this domain is not restricted to the extraction of textual data and there are also important contributions which have attempted to extract objects such as motorcyclists from videos (Limantoro et al., 2018).

2.3. Assessing authenticity

A useful body of research has attempted to establish the authenticity of video footage (Koenig and Lacey, 2015). outline several approaches designed to confirm the authenticity of video and audio files and this section briefly outlines approaches such as tamper protection, source camera identification, source vehicle identification, and video anti-forensics detection.

Kadu et al., (2018) propose a system which protects recordings from third party tampering by storing them on a server and making them accessible only to an authenticated user and an administrator (in case of a claim). The proposal by Kobayashi et al., (2010) detects image tampering by analysing noise characteristics, referred to as a *noise level function (NLF)*.

The contributions of Kurosawa et al., (1999); Lukáš et al., (2006) and Li, (2010) propose novel methods for identifying the camera used to take a photograph (Kurosawa et al., 1999). utilised noise patterns from the charge coupled device (CCD) to help identify the camera (Lukáš et al., 2006), used *Sensor Pattern Noises* (SPNs), and (Li, 2010) applied a similar mechanism, but addressed the problem of scene based noise. A review of source identification methods is provided by Yang et al., (2020).

2.4. Addressing privacy

The use of dashcams pose privacy risks because they are, as (Wagner et al., 2017) puts it, surveillance systems which capture personal video footage in public places. Wagner et al. propose a solution which identifies and disguises individuals faces and licence plates from a dashcam (Zhu et al., 2020). proposed a method for evaluating privacy protection using a CNN convolutional neural network combined with an RNN convolutional network.

Such privacy concerns could inhibit the submission of dashcam evidence. The study by Park et al., (2016) of 481 participants in Korea found that although privacy concerns were an inhibitor to users sharing dashcam footage, they were often able to rationalise footage sharing on the grounds of reciprocal altruism/social justice and even monetary reward.

Privacy laws relating to videos recorded without explicit permission of the subject(s) vary from country to country (Park et al., 2016; Štitilis and Laurinaitis, 2016). In the EU, although the official position states that the processing of dashcam evidence *"must comply with the principles and rules of the GDPR"* and that *"the processing of personal data by dashcams [must be] lawful."* (European Parliament, 2014), there are concerns that GDPR and other regulating laws are not properly regulating the use of dashcams (Wagner et al., 2017).

In the UK at least, where a vehicle is not being used for personal use, such as in taxis, the driver must inform all the passengers of the use of the dashcam and ability to record private conversations. Where a vehicle is being used by multiple drivers, all drivers should know that a dashcam is being used.

Although there is a good deal of research into several related themes as highlighted herein, there is little or no research into the prevalence and provenance of evidential artefacts created by the use of dashcams.

Lallie, (2020) was one of the first research papers around the subject of dashcam forensic examination. The authors analysed 7 dashcams and outlined the prevalence of evidence in dashcam devices. This was followed by a useful contribution by Lee et al., (2021) who classified metadata relating to 14 dashcam models from 11 manufacturers. Although both papers have made important contributions to the domain of dashcam forensics, there is no known contribution which outlines the steps an investigator should follow when presented with a dashcam device. This paper attempts to address this imbalance.

3. Dashcam characteristics

We investigated the following dashcams in the preparation of this paper: Cobra HD CDR 895D, Garmin 55, Mio MiVue 538, Nextbase 512 GW, Nextbase 312 GW, RAC205 and SilentWitness SW006. The examination of these devices was a continuation of the work performed in our previous study (Lallie, 2020). A series of recordings were made on each dashcam during normal vehicle routes.

Each option in the dashcam was turned on and then off to determine the response to the option within the recording produced. The lens was blurred so as not to capture identities - including vehicle registration plates and faces. This did not impact the experiment, as the focus of this is to examine video watermark content, EXIF data, and folder contents. The file structure, video content, and EXIF metadata was then examined using Encase, FTK, and EXIFTools to understand the artefacts created as a consequence of the recordings. The original recordings are available at request from the author.

The result of these experiments led to the formulation of the guidelines presented herein, and which are presented in Fig. 1.

Dashcams record audio and video, and are also capable of recording photographs. Dashcams are user-configurable and enable users to configure settings such as the time, recording mode, licence plate, and the presence of a watermark within the recorded footage. Most dashcams present comparable features such as an LCD screen, an operating system, battery, external power capabilities, a microprocessor, GPS, Bluetooth, Wi-Fi, and read only and random access memory (ROM/RAM). Video footage is normally stored on a removable micro SD card. Dashcams utilise closed operating systems which have no published documentation.

3.1. Recording features

Most dashcams record both video and photographic images. The supported video recording resolution varies, and in the present study, range from 480p to 1440p. The resolution is likely to increase as time progresses with newer dashcams offering better resolutions. Lower resolutions create smaller files. So, a recording made at 1920 × 1080 @ 30fps on a 32 GB Micro SD will render 300 min of recorded material typically divided into 100 × 3 min recordings.

Dashcams operate a loop-recording feature where the oldest non-write protected recording is overwritten when the device runs out of storage space.

Some dashcams support front and rear camera recording, for example the *TOGUARD dual dashcam*, and the *Nextbase DUO HD*. Some dashcams for example the *Nextbase* 322 GW, 422 GW and 522 GW support cabin recording which is a recording of the passengers.

3.2. Recording modes

Dashcams make video recordings in one of three recording modes: *ignition initiated, manually initiated* and *G-sensor initiated*. The recording mode can help explain the context of an incident.

- **Ignition initiated.** Assuming the dashcam is configured to create ignition initiated recordings, and that it is connected to the vehicle ignition system, the dashcam will begin a recording when the ignition is turned on. These recordings are not write protected and will be overwritten when the storage device runs out of space.
- **Manually initiated recordings.** Users manually initiate recordings in one of two ways.
  - *Normal manual.* A user presses the record button on the dashcam. The recording is not write-protected and will be overwritten when the storage device runs out of space.
  - *Emergency record.* If the dashcam supports this feature, then pressing the *emergency record* button will initiate a recording which is saved with write attributes disabled and cannot be overwritten under normal usage.
- **G-Sensor activated recordings.** These recordings are automatically initiated when the g-sensor (gravity sensor) is activated. G-sensor activated recordings are saved with write attributes disabled and cannot be overwritten under normal usage.

A *time-lapse* recording is essentially a sequence of time-lapsed images captured at given increments, so for example, the Nextbase 512, can record time-lapse videos at 1/6th of the normal speed. This has the added effect of reducing the amount of storage space used.

3.3. Battery and power

Dashcams are typically powered by a lithium ion (Li-ion) battery which offers around 30 min of recording time. The limited battery lifetime requires that investigations are conducted with an external power supply connected throughout to ensure that the dashcam does not lose power during the investigation. External power is provided by a USB cable connected to a cigarette lighter. Wall-powered USB cables can also be used for most dashcams. Some dashcams, for example the *Philips* ADR81BLX1 AD*R 810*, have no battery and are wholly reliant on external power source.

3.4. Memory

Recorded video/audio is stored on an external SD card formatted to a standard file system, typically FAT32 or exFAT. Dashcams have an upper limit on the size of the SD card. For example, the *RAC dashcam* accepts a maximum 32 GB, whereas the *NextBase* 512 GW accepts a maximum of 128 GB. The investigative implication of a standard file system is that standard forensic tools such as *Encase*, *FTK* and *x-ways* can be used to extract data and features such as the storage system operates in a manner that should be familiar to investigators. Because the file system is a standard FAT/FAT32/NTFS file system, deleted files, file naming systems and date/time stamping will be familiar to digital investigators.

3.5. Communication systems

Dashcams support a range of communication technology which includes GPS, Bluetooth, WiFi, and GSM. The investigative implications of this are that investigators must disable all radio networks prior to investigation. This is discussed further in Section 4.2.

3.6. Encryption

None of the dashcams investigated in this study, or of which the author is aware incorporated any provision for encryption. Neither the dashcam system itself, nor the recording made thereof was encrypted.

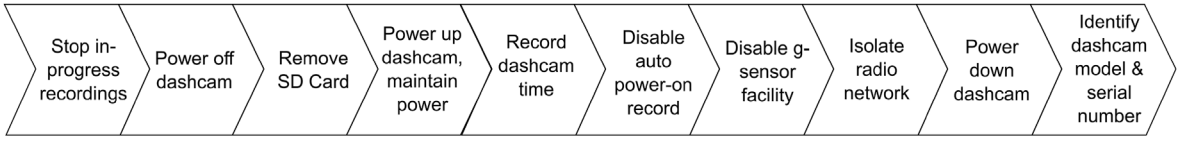

Fig. 1. First response.

3.7. Operating systems

Inbuilt and user-installed dashcams utilise proprietary dashcam operating systems, whereas application-based dashcams utilise host operating systems, typically IOS and Android.

4. First response and preservation

Digital evidence must be protected against alteration and be presented exactly as found. This section explains the measures that must be taken to preserve the integrity of evidence. An overview of the guidelines is presented in Fig. 1. Before an investigation is conducted, it is important for the investigator to understand the characteristics of the specific device in question. This should then enable the investigator to apply specific guidelines need to be tailored to the device under investigation.

4.1. Handling a dashcam at the crime scene

As with all other investigators, the first responder must take precautions to ensure that evidence is not destroyed or tampered with. A dashcam may be found in either a powered-up or powered-down state. All communications, data storage systems, and any other element capable of rendering changes to the dashcam must be disabled as soon as possible. The actions to be taken by a first responder, described in Fig. 1, should be as follows:

- **Stop active recordings.** If the dashcam is recording, the recording should be stopped.
- **Power off.** If the dashcam device is in a powered up state, it should be powered down and the power cable removed. This stage reduces likelihood of corruption or damage to the SD card or the data stored therein.
- **Remove the SD card.** The power having been removed, it is safe to remove SD card. Removing the SD card protects the SD card from inadvertent modification.
- **Power up the dashcam.** With the SD card removed and no immediate risk of damage to the data contained therein, the investigator can now investigate the configuration settings on the dashcam. Connect the dashcam to a power supply and then power it up.
- **Record time.** The dashcam time should be recorded and compared with a reference time such as the Coordinated Universal Time (UTC).
- **Disable auto-power on.** If an auto-power up facility exists, disable it. This will prevent the dashcam attempting to make a recording whenever it is turned on.
- **Disable g-sensor.** This will prevent the dashcam attempting to make a recording whenever it experiences a movement.
- **Isolate the dashcam from the radio network.** This is described in Section 4.2.
- **Record identifying features.** Note the dashcam make/model/serial number from the exterior of the dashcam for the purpose of establishing chain of custody. It is not necessary to note the firmware and operating system details at this stage as this can be done at the point of acquisition.

4.2. Isolating the dashcam from the radio network

Dashcams can incorporate several radio devices, these can include: Wi-Fi, Bluetooth, GPS, and GSM. Dashcams such as the *Jimi New JC100 3G 1080P, Driving Recorder Concox JC100, Mini 3G Cloud Dash Cam D9, VSS HD 3G Vehicle Incident Cam*, accommodate SIM cards which enable GSM connectivity. This connectivity enables live video streaming, receiving data and/or internet connectivity.

First responders must isolate the dashcam from the radio network as incoming data may modify the state of data on the dashcam device and/or outgoing data may alert a third party to the location of the dashcam device (Ayers et al., 2014). It is useful to reflect on how this is achieved on a mobile phone:

1. Turn on the *airplane mode* facility;
2. Isolate each radio component, e.g. turning off the Bluetooth facility;
3. Consider After First Unlock/Before First Unlock (AFU/BFU advice);
4. Place the device in a shielded container.

Methods 2, 3 and 4 can be used with dashcams. However, although dashcams are mobile devices, no dashcams known to the authors have an *airplane mode* facility.

Although there is sometimes pressure to keep a mobile phone device powered up because of the risk of activating a PIN lock, none of the dashcam devices known to the authors have an authentication mechanism such as a PIN or password.

4.3. Securing and evaluating the scene

Traditional forensic techniques such as fingerprint/DNA analysis may need to be applied to link a device with the user/owner. Dashcam devices may be discovered in compromised states such as immersion in water/other liquids, and/or on accident scenes where there is significant damage to the device. In these cases, the agency should revert to their own specific procedures, if they exist, for dealing with such circumstances. It should be noted that although the dashcam device might be damaged, data stored on the storage card might still be recoverable.

It may be necessary to identify *tangential equipment*, which in this case includes but is not limited to items such as GPS modules, screen suction devices, cables, storage cards and power cables.

4.4. Documenting the scene

The crime scene must be documented in particular to include a record – preferably photographs – of the dashcam, its connection to the windscreen, its connection to the power supply and the GPS module if it is a separate module.

4.5. Triage

Triage forensics is a method of completing a rapid on site forensic investigation for the purpose of assessing the severity of an incident and prioritising devices for investigation (Mislan et al., 2010). outline the rationale for conducting triage forensics, some of the reasons proposed include:

1. Assessing the offender's potential danger to society;
2. Rapidly obtaining actionable intelligence;
3. Identifying the most useful sources of evidence pertaining to an investigation;
4. Identify victims that may be at high risk;
5. Identify potential immediate charges;
6. Determine whether a device requires deeper investigation such as in the case of encrypted devices, which might become decrypted should the device be turned off.

We can add to this that by performing a triage at the crime scene, the first responder aids in addressing the forensic backlog by reducing to a minimum the number of devices that should undergo

a full investigation. Having said that, dashcam memory sizes are very low, often up to 128 GB and triaging does little to address the forensic backlog problem.

The problems presented by encryption (rationale 6) do not apply to dashcams. None of the dashcams investigated in this study, nor those that we were aware of at the time of writing supported encryption.

The decision to perform a triage investigation is a matter for the first responder based on the observations outlined above. It should be noted that at the time of writing, no known tools exist to enable the 'safe' triaging of dashcam devices at the crime scene.

5. Acquisition

The *Mobile Device Tool Classification System* shown in Fig. 2 illustrates methods for conducting an acquisition (Brothers, 2008). This system has been used by researchers to describe the relationship between tools and the associated technical, invasive, time consuming and expensive nature of investigating them (Ayers et al., 2014). This system can be used to outline methods of performing an acquisition of the data on a dashcam.

5.1. Manual extraction

Manual extraction involves the direct manipulation of the dashcam using the touchscreen, buttons, dials and other interface elements to identify configuration settings through the LCD panel. This is shown in Fig. 3. Although manual extraction is time consuming and introduces the risk of inadvertently modifying, deleting or creating data, with most dashcam devices that we are aware of, this is the only way of extracting certain configuration settings such as warning sounds, and exposure settings.

Before any form of extraction is attempted, the SD card should be removed. The manual extraction process should be recorded with an external video camera. Amongst the elements that should be recorded/photographed through manual extraction are the make/model of the device, firmware ID, the software/operating system version. In some cases, this information is embedded in EXIF data and can be triangulated therein.

5.2. Logical extraction

Logical extraction involves creating an exact bit for bit copy (digital forensic image) of the data stored on the target using external tools. There are two methods of performing a logical extraction on a dashcam: SD data extraction and extraction directly from the dashcam. In both cases, standard forensic imaging tools such as FTK Imager can be used.

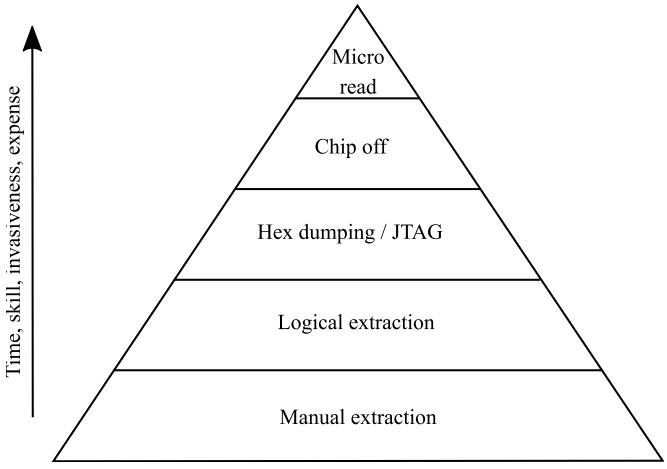

Fig. 2. Dashcam tool classification system, based on (Brothers, 2008).

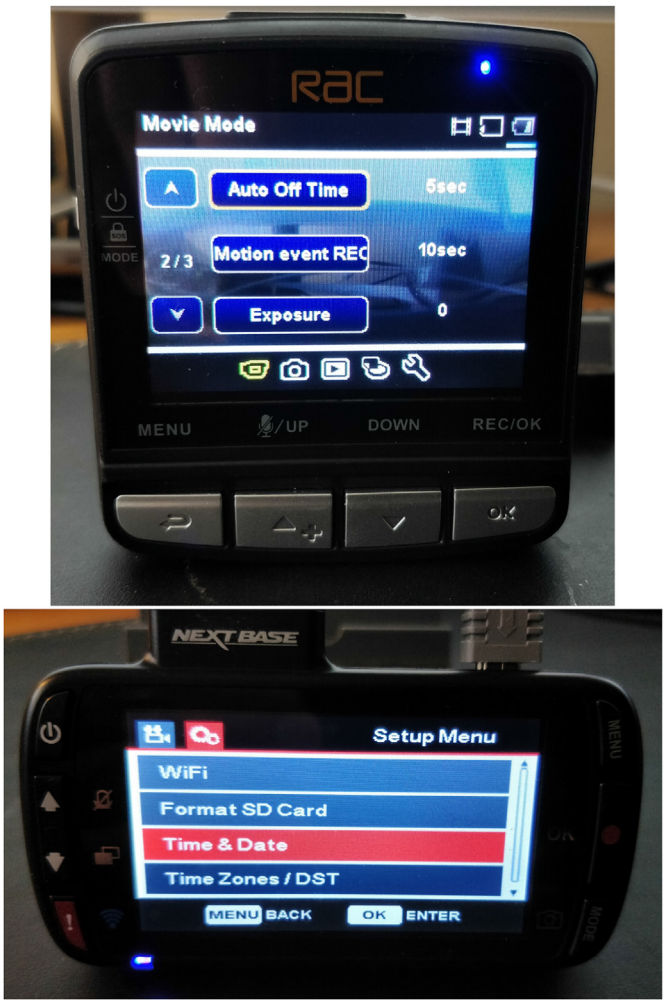

Fig. 3. Manual evidence extraction. RAC (top), Nextbase 312 (bottom).

5.2.1. SD data extraction

The logical extraction of data from a dashcam SD card follows procedures generally accepted in the digital forensics domain: remove the micro SD card, validate the make/model/serial number of the SD card against that recorded at seizure, photograph the SD card, write block the SD card reader prior to the imaging tool being used to create the digital forensic image, make a forensic image, validate the image (hash checking) and then store the SD card securely.

5.2.2. Direct extraction

Several dashcam devices support *mass storage* mode (USB *MSC* or *UMS*). This means that, assuming the SD card is inserted in the dashcam, the dashcam can be mounted and the digital forensic image created directly from the dashcam without the need to remove the SD card. The dashcam device is connected directly to a forensic workstation through a USB cable. The dashcam is mounted and then appears as an external device within the digital forensic imaging tool. This mechanism should be deployed as a last resort with care as any number of scenarios such as a faulty cable, or the g-

sensor enabled on the dashcam, will result in the dashcam initiating a recording automatically when turned on instead of enabling the forensic workstation to mount the dashcam.

5.3. Hex dumping, chip-off and micro-reading

To date although there is a variety of research into performing JTAG based extraction (Breeuwsma, 2006; Kim and Ryu, 2008), hex-dumping through the use of *flasher boxes* to acquire data from memory systems (Al-Zarouni, 2007; Jonkers, 2010), and chip-off (Fukami et al., 2017), we are not aware of any research into applying these methods to dashcam devices.

6. Examination and analysis

This section describes the *tools* available to investigate a dashcam, and the evidence locations. The discussion proceeds to outline how some of the evidence can be extracted manually – that being the only mechanism to extract some configuration settings. The substantive element of this Section is a workflow explaining how geospatial evidence can be obtained from dashcam footage into CSV, KML, and GPX formats, and how this evidence can be mapped using two mapping systems: Google Maps, and GPXSee.

6.1. Tools

Three types of tool, previously described in Lallie, (2020), are available to aid in the examination and analysis phase: *dedicated forensic tools, native video players* and *specialist metadata extraction tools.*

- **Dedicated forensic tools.** At the time of writing, traditional dedicated forensic tools such as Encase, FTK, XRY and Autopsy were not able to analyse the full range of items of evidentiary interest. These tools are limited in their ability to extract specific metadata, such as GPS data, from MP4 and MOV files. Generally, they rely on specially crafted scripts and functions.
- **Native Video Player.** Many dashcam manufacturers provide tools which enable users to view the video created by the dashcam. These tools also provide extra functionality such as the ability to view a travel route and the associated vehicular speed. These tools are not designed to aid forensic investigations and any useful data they present will need to be independently verified using other tools.
- **Specialist Metadata Extraction Tools.** Tools such as Exiftool (Harvey, 2021) enable analysts to extract metadata from video files. These tools provide results as textual outputs which must either be parsed into CSV/other useful formas using a second tool or converted directly into a KML or other mapping file, which in turn can be viewed using a mapping tool (described in Section 6.2.3). After that, the output must be converted into a meaningful format. Tools such as the NMEA convertor (NVS Technologies, 2012) can be used to convert NMEA data to KML which can then be uploaded to and viewed in Google Earth.

6.2. Dashcam evidence locations

Table 1 reveals the presence of some of these items of evidentiary interest in the dashcams investigated in the present study. The table reveals that temporal data can be found in:

- The file system: file names, directory structures, and file attributes.
- Configuration files
- NMEA files
- EXIF data
- Audio/Video recordings
- Within the dashcam configuration settings through manual extraction

Amongst the additional items of interest to an investigator, we can include the following:

1. *Recording initiation.* This was previously described in Section 3.1 and includes: *ignition activated, manually activated (normal manual* and *emergency record initiated)* and *g-sensor activated* recordings.
2. Whether the time was set manually, or set to auto-update.
3. Whether warnings such as: red light/speed camera warnings, the forward collision warning or lane departure were provided to the user.
4. General dashcam configuration settings as described in Section 6.3.

Of these, (1) can be revealed through a logical extraction by analysing filenames, directory structures and file attributes, and (2, 3 & 4) can only be revealed through manual extraction.

The file system structure can be analysed through a logical extraction as described in Section 5. The file structure can reveal: the recording mode, temporal data and file sequences.

6.2.1. Recording mode

The recording mode is revealed by analysing the filename, directory structure and/or file attributes. A review of filename and directory name structures was presented in Lallie (2020). Some example filename and directory structures are provided in Table 2 and described in Table 2.

In the Cobra filename structure outlined in Table 2, the TTT: is any of JPG (photo), MOV (movie) or SOS which indicates a recording made using the emergency function or with the g-sensor facility activated.

In the MiVue filename structure outlined in Table 2, TTTT can be EMER for emergency recordings, FILE for normal recordings, and PARK for recordings made in parking mode.

In the RAC filename structure outlined in Tables 2 and XXXX is a four-letter prefix which can have the values: MOV_ for recordings, IMAG for pictures and SOS_ for emergency-saved files.

Some dashcams organise the directory structure to reflect the recording mode. For example, the Nextbase dashcams split normal videos and videos recorded in *emergency* or *parking* mode into the NBDVR/VIDEO/PROTECTED. Similarly, the Garmin dashcam saves files with directory names such as 100PARKM and 104TLPSE to indicate recordings made in *parking* mode and *timelapse* mode respectively.

Where recordings are made in *emergency, g-sensor activated* or *parking* mode, the file attributes are typically modified to *read only* so that these files cannot be over-written.

6.2.2. Temporal data

Lallie (2020) showed that dashcams record time in at least 6 possible places: the NMEA file, where available, configuration files, as EXIF data in videos, the filename, through the native video player, and as a watermark in the video. The time on a dashcam can be set manually by the user, or can be set to auto-update according to GPS timing. In either case, where a dashcam records EXIF data and has GPS capability, it includes the GPS time within that data. Although the user configured dashcam time can be inaccurate, even forged, it is difficult for a user to forge the GPS time as presented within the EXIF data.

Table 1
Directory structure.

Item of interest	File system	Config files	NMEA files	EXIF data	Audio/video recordings	Dashcam settings
Recording mode						
Ignition activated	✓	X	X	X	X	✓
Record button manual press	✓	X	X	X	X	✓
Emergency button press	✓	X	X	X	X	✓
G-sensor activated	✓	X	X	X	X	✓
Speed	X	X	X	✓	✓	X
Geospatial data	✓	X	X	✓	✓	X
Temporal data	✓	✓	✓	✓	✓	X
Configuration settings	X	X	X	X	X	✓
Licence plate	X	X	X	X	✓	✓

Table 2
Sample filename/directory name structures.

Dashcam	File/directory name structure	Example
Cobra HD CDR 895D	YYYYMMDD_NNNN_CAMN_TTT.EXT	20181106_0004_CAM1_SOS.MOV
MiVue 538	TTTTYYMMDD-HHmmSS.MOV	EMER181106-080456.MOV
RAC 205	XXXXNNNN.EXT	SOS_0012.MOV

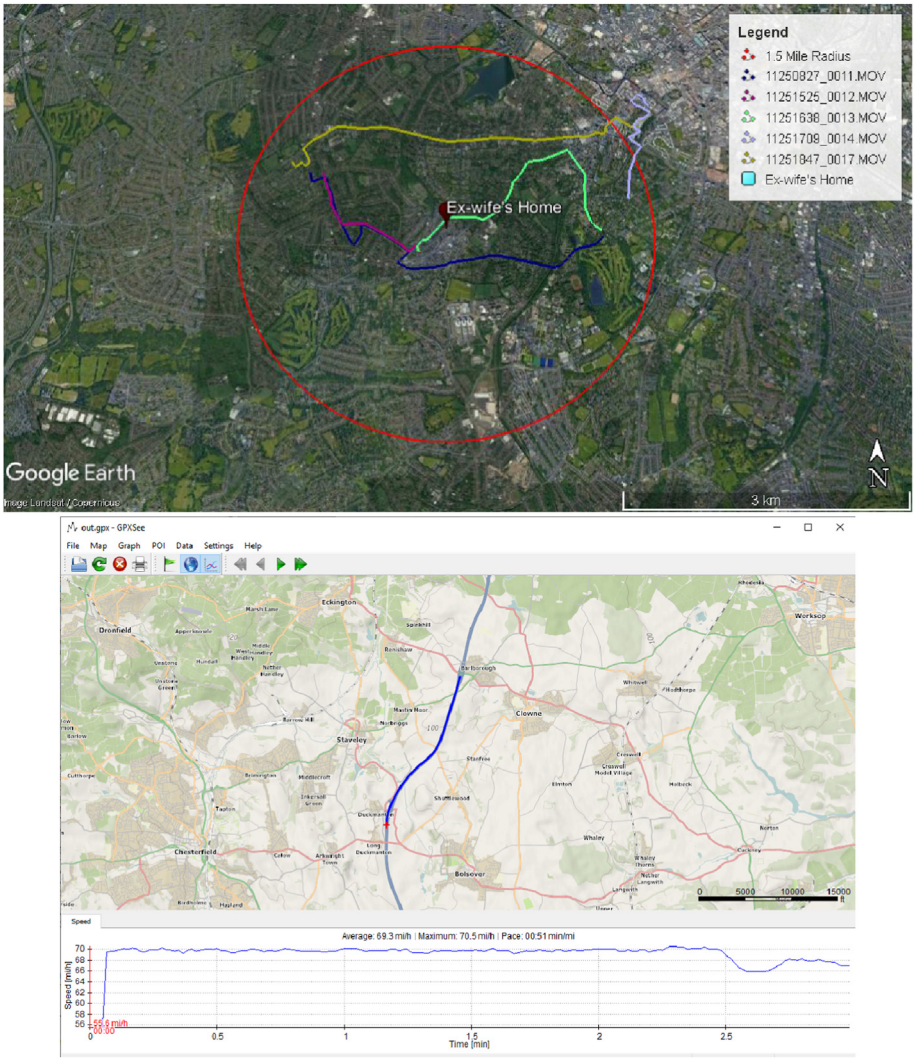

Fig. 4. Samples of routes mapped using Google maps (left) and GPXSee (right). Note: reference to 'ex-wife' is fictitious.

Fig. 5. A sample dashcam watermark from a Silentwitness dashcam. This watermark has been cropped from the original and was presented on the bottom right of the image.The arrow has been added by the author.

During the analysis, the investigator needs to be aware of all these timestamps and record the time noting inconsistencies in the time, for instance between that given in the file name, MAC times, watermarks and the EXIF data.

Temporal data is sometimes revealed in the filenames of videos created by the dashcam. The date and time that the recording of a particular file was started is incorporated within the file. Some example formats follow.

The Cobra has a filename format: YYYYMMDD_NNNN_-CAMN_TTT.EXT where: YYYY is the year, MM is the month and DD is the date, (e.g., 20160101_0006_CAM1_VID.MOV). Nextbase 312 has a filename format: YYYY_MMDD_HHmmSS_NNN.EXT e.g., 2018_1007_051316_001.jpg, the Nextbase512 has a filename format: YYYY_MM_DD_HHmmSS_NNN.EXT (e.g., 2018_100_7_051316_001.jpg); SilentWitness has a filename format: MMDDHHmm_NNNN.EXT (e.g., 10260824_0123.MOV); MiVue: IMGYYMMDD-HHmmSS.JPG or FILEYYMMDD-HHmmSS.MOV (e.g., IMG191026-082437.MOV).

NMEA (National Marine Electronics Association) files contain geospatial, temporal, and speed data. These files have an.nmea extension and are paired with a.mov file. In some dashcams - such as the MiVue, they have the same filename, for example, xxxxx.mov and xxxxx.nmea.

NMEA files contain geospatial, temporal and speed data within the following fields, referred to as *sentences*: $GPBWC, $GPZDA, $PMGNTRK and $PRWIINIT (DePriest, 2019). A brief explanation of some of these fields is presented herein, for a more detailed explanation, the reader is referred to (Baddeley, 2001) and (Si and Aung, 2011). The rest of this section uses the following two examples, previously provided in Lallie, (2020):

Sample 1:

$GPRMC,070851.00,A,5227.77102,N,00156.72583,W,0.032,078.7,041018,010.3,E*6C.

Sample 2:

$GPGGA,071010.00,5227.76885,N,00156.61993,W,1,08,1.20,151.9,M,48.0,M,*42.

6.2.3. Geospatial data

NMEA files contain GPS data held within the following fields: $GPBWC, $GPZDA, $PMGNTRK and $PRWIINIT (DePriest, 2019).

Sample 1 contains the latitude 5227.77102,N (52 deg. 27.77 min North or 52d27′77″N) and the longitude 00156. 72583,W (1 deg. 56.72583 min West or 1d 56′72″W), and the *direction* where: 078.7 indicates the direction the vehicle is travelling from true North and 010.3,E indicates the magnetic variation, in this case 10.3 deg East.

Sample 2 contains the longitude (5227.76885,N: 52d 27.76885′ North or 52d27′76″N) and latitude (00156.61993,W: 1d 56.61993′West or 1d56′61″W).

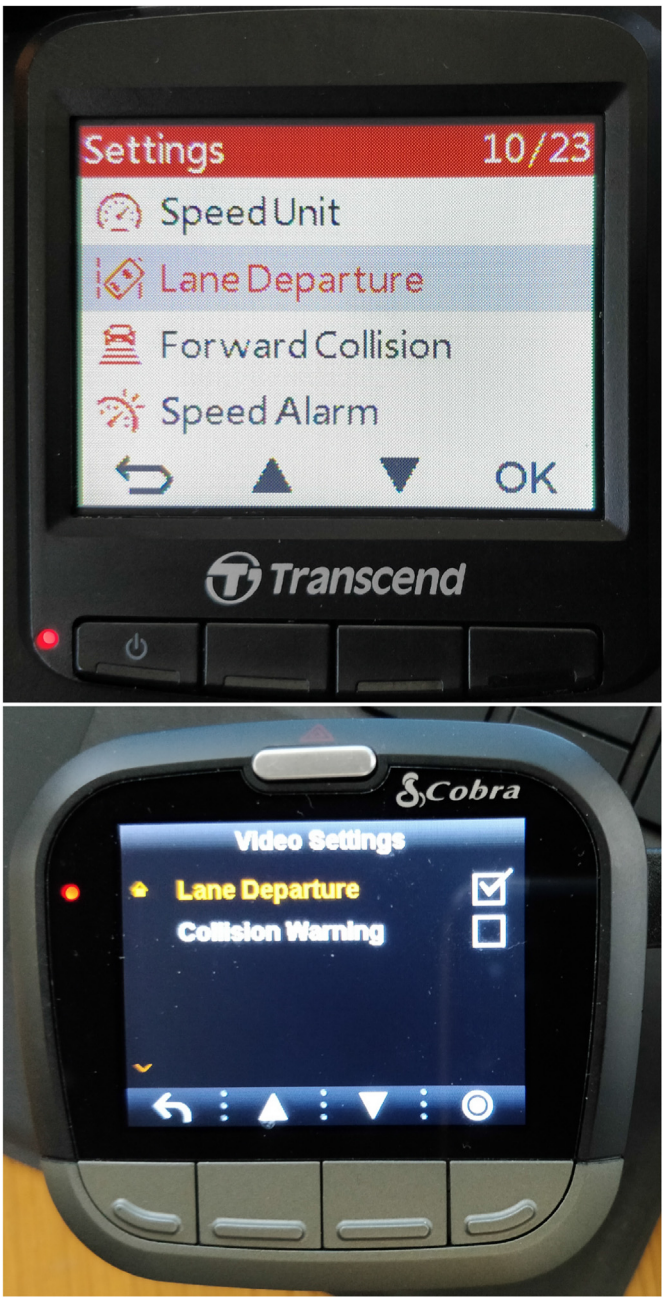

Fig. 6. The need to take dashcam photos for evidence collection: user warning configuration, Transcend (top) Cobra (bottom).

6.2.4. Temporal data

Sample 1 contains 2 temporal references: 070851.00 is the time fix, in this case 07:08:51 UTC. 041018 is the date of the fix, in this case 4th October 2018. Sample 2 also contains temporal data. The field: 071010.00 refers to the time which in this case is: 07:10:10 UTC.

6.2.5. Speed data

Sample 1 contains speed data as follows. *0.032* indicates the speed over ground calculated in knots.

NMEA data can be converted into formats such as KML by using online convertors such as (Schmidt, 2008) and [45].

Table 3
Sample EXIF commands.

Command	Explanation
(1) exiftool -ee FILENAME	-ee means *extract embedded*). This command displays GPS data, vehicular speed and associated timestamps for file FILENAME. Sample output data from this command is presented in Fig. 7.
(2) exiftool -T -FileName -CreateDate -Modifydate -FileSize *.MOV *JPG	- extracts filenames, create dates, modify dates and file sizes of all files with the.mov and.jpg extension.
(3) exiftool -ee -GPSLongitude -GPSLatitude *.MOV	Extracts all GPS longitude/latitude data (in separate sequences) from all files which have the extension.MOV
(4) exiftool -ee -p kml.fmt FILENAME ¿ out.kml	Extract GPS coordinates from file FILENAME and exports them to kml format[a]
(5) exiftool -ee -p gpx.fmt FILENAME ¿ out.gpx	Extract GPS coordinates from file FILENAME and exports them to gpx format[a]
(6) exiftool -csv out.csv -GPS* FILENAME	Extracts all GPS coordinates from file FILENAME and exports them to csv format

[a] Both commands require a sample kml.fmt and gpx.fmt file to exist in the same directory. Sample kml.fmt and gpx.fmt files are available from: https://github.com/alchemy-fr/exiftool/blob/master/fmt_files/kml.fmt and https://github.com/alchemy-fr/exiftool/blob/master/fmt_files/gpx.fmt respectively.

```
GPS Date/Time          :   2019:12:06 08:09:14.000Z
Sample Time            :   0.25 s
Sample Duration        :   0.25 s
GPS Latitude           :   52 deg 27' 32.79" N
GPS Longitude          :   1 deg 57' 7.73" W
GPS Speed              :   24
GPS Speed Ref          :   mph
```

Fig. 7. A sample EXIF output.

Configuration files contain temporal data relating to the operation of the dashcam. An example of configuration files is provided by the Garmin dashcam. The Garmin dashcam creates two important configuration files which are stored within the file system: drive_hours_logger.db, an SWL file, and elog.JSON.

The drive_hours_logger.db contains journey logs. Each entry has a corresponding create_timestamp field which has the format YYY-MM-DD HH_MM_SS and indicates the time that the entry was created, in this case indicating the start of the journey.

The elog.JSON file stores error data. This file contains two fields which reveal temporal data: uptime_ms and error_cause. uptime_ms indicates the period of time (in ms) that the dashcam was operational. The error_cause indicates the reason that the dashcam was closed down – for example Low Battery Shutoff. This field has a corresponding Time field with the format YYYY-MM-DD HH:MM:SS indicating the time that the unit closed down.

GPS data can be extracted from EXIF and NMEA data and plotted using systems such as GoogleMaps, Google Earth or GPXSee. This section describes the EXIF and NMEA data and demonstrates how this can be extracted.

There is an abundance of evidence contained within the video file in terms of the video photography and possibly audio. If watermarks are enabled, these will present a range of further evidence including: speed travelled, geospatial data, temporal data, the licence place, the make and sometimes model of the vehicle, and the data/time. Video and audio analysis is time consuming because it has to be analysed by viewing the file (Fig. 5). There are no known watermark data forensic extraction tools, so for the time being, this also has to be analysed manually.

6.3. Manual extraction

Configuration settings such as: whether the time was set manually or to auto-update; whether user warnings such as *lane departure, forward collision* and *speed* were enabled; licence plate data; and evidence of wifi connectivity can only be revealed through a manual extraction (Fig. 6). This is achieved by perusing the dashcam settings. These settings must be recorded by taking photographs. An example of this is shown in Fig. 6.

For the 8 dashcams investigated in this study, where warning features were enabled, these were presented to the user on the dashcam screen as and when appropriate, but were not recorded anywhere in the video or in any configuration files.

Some dashcams enable users to enter a vehicle registration/licence plate number. Whilst licence plate information was displayed in the watermarks on some dashcam models (as shown in Table 1 and Fig. 5), we found no evidence of this in the metadata or any other location. However, newer generations of dashcams, for example the *Nextbase* 522 GW include the licence plate in the metadata.

6.4. Geospatial evidence extraction workflow

Before proceeding the discussion further, it is useful to outline perhaps the two most important evidence formats. An investigator is likely to want to convert the EXIF data from a recording into a 'mappable' format, i.e. one that can be viewed using a tool such as Google Maps or GPXSee, or into CSV format, which enables further finite analysis of the data. The extraction of this data has to be done with the use of secondary tool because there is currently no digital forensic tool that supports the extraction and mapping of geospatial data from dashcam systems. This Section describes a manual workflow which enables the extraction of geospatial evidence into multiple formats, and then the mapping of those formats onto mapping systems.

Existing tools are unable to extract and map/visualise the relevant metadata, specifically GPS, time, and other data described in Section 3. The solution is our proposed four step process involving: data extraction, parsing, data formatting, and finally, mapping.

6.4.1. Extraction

EXIF data can be extracted using Phil Harvey's Exiftool utility (Harvey, 2021). Sample EXIF commands and their explanations are provided in Table 3. An example of the output from *exiftools* is provided in Fig. 7 of the commands described therein, commands (4) and (5) are particularly as these produce mapping files which require no further intervention and can be mapped directly. Command (6) is of particular use as this produces raw CSV output which can be analysed further by the investigator.

6.4.2. Mapping

Quite often, GPS data contained within EXIF files is not useful unless it is plotted onto a map. Once GPS data is extracted, it has to be parsed and converted to a format such as KML or GPX which can be accepted by mapping systems such as Google Maps, Google Earth or GPXSee.

Google Maps and Google Earth are able to present the GPS coordinates and enable users to add limited configuration options. GPXSee synthesises the speed travelled with the GPS coordinates to

show the route travelled coupled with the speed at each point as shown in Fig. 4.

6.5. Forging dashcam videos and metadata

It is important at this juncture to consider the extent to which the evidence recovered can be relied upon. There are two elements of evidence to consider, the video including its watermark if one exists, and the EXIF data within the video. The issue of source camera identification, authenticating recordings, image forgery, forgery detection, video anti-forensics and counter anti-forensics were discussed in Lallie, (2020). Moreover, the domain of image and watermark forgery within images is covered reasonably well in the literature and we refer readers to (Kaur et al., 2023) for a review of contributions in this domain.

At this juncture, we focus on the forgery of metadata within videos recovered from dashcams. EXIF data is remarkably difficult to forge for three reasons.

Firstly, for a perpetrator to forge any of the three key evidentiary artefacts: geospatial, temporal, and speed, the perpetrator would have to manipulate each and every corresponding record in each frame of a video segment. For a 3 min video at 30FPS that could be 5400 timestamp entries and a corresponding number of geospatial and speed entries. The perpetrator might need to apply this to a complete relevant segment, i.e. the segment in question, as there may need to be a sense of continuity in the forged output, this might be extended to an hour's worth of relevant video - which becomes 108,000 frames that need adjusting.

Secondly, fundamentally the process of inserting fake data is not difficult in itself, however, the inserted data must be realistic. All three components (geospatial, temporal, and speed) need to be consistent with each other. The time can be easily generated, however, the speed needs to be consistent with the time and co-ordinates. i.e. setting the speed to low, but the coordinates to far apart in each frame will indicate forgery. The most difficult element of this is to generate realistic alternative coordinates. Using Fig. 4 as an example, the perpetrator might be motivated to suggest an alternative location to the one found in the figure, if so, every single coordinate of the new location/route must be generated and altered to be consistent with the speed. Without appropriate tools to aid this process, this is not a trivial task.

Thirdly, the forged metadata needs to be consistent with the video. The examiner will need to consider whether coordinates indicating location 'a', at a speed of 'b' at a time of 'c' are consistent with what is seen in the video.

7. Reporting

This section outlines the additional reporting that must be made in a dashcam investigation report. The discussion assumes that the reader is aware of generic forensics reporting and the report structure.

Forensic investigation reports typically include (but are not limited to) the following sections: the investigator and agency details, the case number description and dates etc., the investigation method and investigation findings. These sections should include:

7.1. Method

- Details of the dashcam, including make, model, serial number.
- Details of other items seized.
- An overview of actions taken to secure the dashcam/SD card from accidental, deliberate erasure and/or manipulation.
- Description of items submitted for examination, including serial number, make, and model.
- Materials and equipment used to conduct the investigation, particularly a precis of specialist 'non-standard' tools and the approach taken to verify their results.
- A description of how the examination was conducted including searches and commands issued.

7.2. Findings

- Complete video footage of the dashcam contents.
- Photos of the dashcam.
- photos of the configuration settings.
- Evidence of routes followed accompanied with geospatial and temporal data presented in both raw (CSV, excel, KML, GPX) and map image formats.
- Evidence of photos taken with the dashcam.
- Evidence of recording modes.
- Speeds covered by the driver.

8. Discussion and conclusions

This paper has outlined the range of evidence available on a dashcam. Having outlined this, we have proceeded to describe this using the investigative framework proposed by Ayers et al., namely: *preservation*, *acquisition*, *examination and analysis*, and *reporting*. For each of these steps we described how a dashcam should be treated, for instance, how dashcam evidence should be preserved, how acquisition should be performed etc.

8.1. Further research

Most of the steps described in this paper involve manual steps of extraction, conversion, and presentation using multiple tools. This area calls for a digital forensic tool which can automate this process and produce evidence which can be accepted by courts.

There is no known method of extracting all dashcam configuration data other than manually interacting with the dashcam and taking photos of configuration settings. This requires further research. Although JTAG based extraction may help, this method is intrusive.

References

Al-maweri, N.A.A.S., Sabri, A.Q.M., Mansoor, A.M., 2016. Automatic rotation recovery algorithm for accurate digital image and video watermarks extraction. Int. J. Adv. Comput. Sci. Appl. 7, 65–72.
Al-Zarouni, M., 2007. Introduction to Mobile Phone Flasher Devices and Considerations for Their Use in Mobile Phone Forensics.
Asikuzzaman, M., Pickering, M.R., 2018. An overview of digital video watermarking. IEEE Trans. Circ. Syst. Video Technol. 28, 2131–2153.
Ayers, R., Brothers, S., Wayne, J., 2014. Guidelines on cell phone forensics (NIST Special Publication 800-101), techreport. URL: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final.
Baddeley, G., 2001. GPS - NMEA sentence information. URL: http://aprs.gids.nl/nmea/. date accessed: 30-9-19.
Breeuwsma, M., 2006. Forensic imaging of embedded systems using jtag (boundary-scan). Digit. Invest. 3, 32–42.
Brothers, S., 2008. How Cell Phone "Forensic" Tools Actually Work—Cell Phone Tool Leveling System. Mobile Forensic World, Chicago, IL.
DePriest, D., 2019. NMEA Data, Technical Report. URL: https://www.gpsinformation.org/dale/nmea.htm.
European Parliament, 2014. Parliamentary questions. URL: http://www.europarl.europa.eu/doceo/document/P-8-2018-000591-ASW_EN.html. date accessed: 1-11-2018.
Fukami, A., Ghose, S., Luo, Y., Cai, Y., Mutlu, O., 2017. Improving the reliability of chip-off forensic analysis of nand flash memory devices. Digit. Invest. 20, S1–S11.
Harvey, P., 2021. Exiftool. URL: https://www.sno.phy.queensu.ca/~phil/exiftool/.
Jaderberg, M., Simonyan, K., Vedaldi, A., Zisserman, A., 2016. Reading text in the

wild with convolutional neural networks. Int. J. Comput. Vis. 116, 1–20.
Jonkers, K., 2010. The forensic use of mobile phone flasher boxes. Digit. Invest. 6, 168–178.
Kadu, S., Cheggoju, N., Satpute, V.R., 2018. Noise-resilient compressed domain video watermarking system for in-car camera security. Multimed. Syst. 24, 583–595.
Kafer, T., 2018. Forensic report = accident uber-volvo 18.03.2018, technical report, car-forensics. URL: https://www.kaeferlive.de/downloads/DigiFor_Inside_04-2018_engl.pdf.
Kamat, D.D., Kinsman, T.B., 2017. Using road markers as fiducials for automatic speed estimation in road videos. In: 2017 IEEE Western New York Image and Signal Processing Workshop (WNYISPW). IEEE, pp. 1–5.
Kaur, G., Singh, N., Kumar, M., 2023. Image forgery techniques: a review. Artif. Intell. Rev. 56, 1577–1625.
Kim, K.-W., Ryu, J.-C., 2008. Forensic data acquisition on cell phone using jtag interface. In: Proceedings of the IEEK Conference. The Institute of Electronics and Information Engineers, pp. 333–334.
Kim, J.-H., Oh, W.-T., Choi, J.-H., Park, J.-C., 2018. Reliability verification of vehicle speed estimate method in forensic videos. Forensic Sci. Int. 287, 195–206.
Kobayashi, M., Okabe, T., Sato, Y., 2010. Detecting forgery from static-scene video based on inconsistency in noise level functions. IEEE Trans. Inf. Forensics Secur. 5, 883–892.
Koenig, B.E., Lacey, D.S., 2015. Forensic Authentication of Digital Audio and Video Files, Handbook of Digital Forensics of Multimedia Data and Devices, pp. 133–181.
Kurosawa, K., Kuroki, K., Saitoh, N., 1999. Ccd fingerprint method-identification of a video camera from videotaped images. In: Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348), vol. 3. IEEE, pp. 537–540.
Lallie, H.S., 2020. Dashcam forensics: a preliminary analysis of 7 dashcam devices. Forensic Sci. Int.: Digit. Invest. 33, 200910.
Lee, K., Choi, J.-H., Park, J., Lee, S., 2021. Your car is recording: metadata-driven dashcam analysis system. Forensic Sci. Int.: Digit. Invest. 38, 301131.
Li, C.-T., 2010. Source camera identification using enhanced sensor pattern noise. IEEE Trans. Inf. Forensics Secur. 5, 280–287.
Li, H., Shen, C., 2016. Reading Car License Plates Using Deep Convolutional Neural Networks and Lstms arXiv preprint arXiv:1601.05610.
Limantoro, S.E., Kristian, Y., Purwanto, D.D., 2018. Pemanfaatan deep learning pada video dash cam untuk deteksi pengendara sepeda motor. Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI) 7.
Lukáš, J., Fridrich, J., Goljan, M., 2006. Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Secur. 1, 205–214.
Mislan, R.P., Casey, E., Kessler, G.C., 2010. The growing need for on-scene triage of mobile devices. Digit. Invest. 6, 112–124.
NVS Technologies, 2012. Converter NMEA to KML. URL: http://nvs-gnss.com/support/soft/item/19-converter-nmea-2-kml.html. date accessed: 20-09-2018.
S. Park, J. Kim, R. Mizouni, U. Lee, Motives and concerns of dashcam video sharing, in: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM, San Jose, California, USA, 2016, pp. 4758–4769. URL: http://chi2016.acm.org/wp/. doi:https://dl.acm. org/citation.cfm?doid=2858036.2858581.
Rocha, A., Scheirer, W., Boult, T., Goldenstein, S., 2011. Vision of the unseen: current trends and challenges in digital image and video forensics. ACM Comput. Surv. 43, 26.
Schmidt, H., 2008. Nmea to Kml Converter. URL: https://www.h-schmidt.net/NMEA/.
Si, H., Aung, Z.M., 2011. Position data acquisition from nmea protocol of global positioning system. Int. J. Comput. Electr. Eng. 3, 353.
Singh, R.D., Aggarwal, N., 2018. Video content authentication techniques: a comprehensive survey. Multimed. Syst. 24, 211–240.
Štitilis, D., Laurinaitis, M., 2016. Legal regulation of the use of dashboard cameras: aspects of privacy protection. Comput. Law Secur. Rep. 32, 316–326.
Tummala, G.K., Das, T., Sinha, P., Ramnath, R., 2019. Smartdashcam: automatic live calibration for dashcams. In: Proceedings of the 18th International Conference on Information Processing in Sensor Networks, pp. 157–168.
Tyagi, S., Yadav, D., 2022. A detailed analysis of image and video forgery detection techniques. Vis. Comput. 1–21.
Wagner, P., Birnstill, P., Krempel, E., Bretthauer, S., Beyerer, J., 2017. Privacy dashcam–towards lawful use of dashcams through enforcement of external anonymization. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, pp. 183–201.
Wu, H., Zhou, J., Tian, J., Liu, J., 2022. Robust image forgery detection over online social network shared images. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 13440–13449.
Yang, P., Baracchi, D., Ni, R., Zhao, Y., Argenti, F., Piva, A., 2020. A survey of deep learning-based source image forensics. J. Imag. 6, 9.
Zhang, Z., Zhang, C., Shen, W., Yao, C., Liu, W., Bai, X., 2016. Multi-oriented text detection with fully convolutional networks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 4159–4167.
Zhou, Z., Yang, Z., Zhang, Y., Huang, Y., Chen, H., Yu, Z., 2022. A comprehensive study of speed prediction in transportation system: from vehicle to traffic. iScience, 103909.
Zhu, B., Fang, H., Sui, Y., Li, L., 2020. Deepfakes for medical video de-identification: privacy protection and diagnostic information preservation. In: Proceedings of the AAAI/ACM Conference on AI. Ethics, and Society, pp. 414–420.