Dashcam Forensics: A Preliminary Analysis of 7 Dashcam Devices

Harjinder Singh Lallie

University of Warwick, WMG, Gibbet Hill Road, CV4 7AL, UK

Abstract

Dashboard cameras ("dashcams") are becoming an important in-car accessory used to record audio and visual footage of car journeys. The audio/video footage produced by dashcams have become important items of evidence.

This paper explores the problems related to the management and processing of dashcam evidence, and in particular, highlights challenges to the admissibility of evidence submitted online. The key contribution of this paper is to outline the results of an experiment which aimed to reveal the prevalence and provenance of artefacts created by the use of dashcams on the SD storage system of seven dashcam systems.

The research describes the provenance of evidential artefacts relating to: the dashcam recording mode, GPS data, vehicular speed data, licence plate data, and temporal data which was found in at least six locations - namely: NMEA files, configuration/diagnostic files, EXIF metadata, directory structures, filename structures and imagery watermarks.

Keywords: dashcam, digital forensic, video forensics

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.

Provisions - such as the *self-evident* app which enables witnesses to upload videos and statements directly to law enforcement agencies, have existed for a while [69]. The first dedicated UK dashcam evidence submission portal was established by Nextbase in 2018 [43]. This portal became a central point for managing the submission of dashcam evidence on behalf of UK police forces. It should be noted, that not all UK police forces are accepting evidence in this manner. Table 1 provides an overview of how - if at all, UK police forces are accepting dashcam evidence. The Nextbase portal manages the dashcam evidence submission process by either accepting the submission and forwarding to the relevant police authority, or redirecting users to the police authority website for the evidence submission. At the time of writing, 5 police forces accept evidence submitted through the Nextbase portal, another 14 accept evidence submitted directly to them, 17 *intend* to begin accepting evidence and 7 are not accepting the online submission of dashcam evidence.

The visual evidence produced by dashcams is persuasive and compelling [55] - possibly because dashcam evidence is not subject to the same features of perspective bias that systems such as body camera systems are [66].

Table 2 presents an overview of legal cases involving dashcam evidence. The table shows that dashcam evidence has been used to reveal compromising audio conversations as in the case of Patrick Collins [70] and Shane Mullen and Gez Bennett [8], and also as evidence captured by third parties such as in the case of Ian Welsby [19], Chloe May [23], and Marcin Dariusz Purlis [15]. These cases indicate that although not all UK police authorities are currently accepting dashcam evidence submitted online

[*] A dataset comprising of a number of dashcam recordings is available to accompany this paper. To get access to this dataset, please visit http://lallie.co.uk/csdi/ and look at the information under the publication entry for this paper

Email address: HL@warwick.ac.uk (Harjinder Singh Lallie)

(as shown in Table 1), it is likely that this mode of submission might become more common, and that law enforcement agencies around the world will become more proactive in seeking dashcam evidence for incidents [6].

Maybe as a consequence, dashcam usage is increasing rapidly in the UK. In 2015, 9% of drivers were using dashcams [7], this rose to 15% in 2016 [62], 17% in 2017 [3], and 27% in 2018 [4]. Nottingham Police recorded 211,598 dashcam records over a three year period leading up to 2017 [45].

This paper explores two aspects of dashcam evidence: the problems related to the management and processing of dashcam evidence (Section 3), and an analysis of artefacts generated by dashcams (Section 4). the discussion in Section 4 presents the results of an experiment which aimed to reveal the prevalence and provenance of artefacts created by the use of dashcams on the SD storage system of seven dashcam systems.

2. Previous research

Dashcam forensics draws together a number of forensic domains including traditional file system forensics (the subject of the present paper) and video/imagery/audio related forensics. The predominance of research into video/imagery/audio related forensics is evidenced by a number of literature reviews which focus on: watermarking as a means of authenticating recordings [2]; source camera identification, forgery detection, and steganalysis [51]; and published literature in the domain of video forgery/tamper detection, video re-capture, phylogeny detection, video anti-forensics and counter anti-forensics [57].

Similarly, there is a lot of research investigating the problem of image forgery [17, 9, 49]. Although image forgery is a concern in dashcam forensics, given that most of the evidence tends to be video based, the present review does not focus on this area.

The rest 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 and geospatial data are important evidential artefacts. However, these can be disabled by the user, and may not appear in dashcam recorded footage. Where vehicular speed and GPS data is available in a watermark, there are questions relating to the extent to which metadata presented as a video watermark can be relied upon [29].

A number of complimentary, methods of estimating vehicular speed have been proposed. For example, Kamat and Kinsman [30] used uniformly spaced road markers painted on roads to estimate

Table 1: UK police forces and the acceptance of dashcam evidence

Method of accepting Evidence	**Police constabulary**
Nextbase site	Warwickshire, West Mercia, West Midlands, Wiltshire
Police site	Avon and Somerset, Cheshire, Dyfed-Powys, Essex, Gwent, Hampshire, Metropolitan Police Service, Norfolk, North Wales, South Wales, Suffolk, Surrey, Sussex, Thames Valley
Intention to activate	Bedfordshire, Cambridgeshire, City of London, Cleveland, Derbyshire, Devon and Cornwall, Durham, Greater Manchester, Hertfordshire, Humberside, Lincolnshire, Merseyside, Northamptonshire, Northumbria, Nottinghamshire, South Yorkshire, Staffordshire
Not accepting online submission	Cumbria, Dorset, Gloucestershire, Kent, Lancashire, North Yorkshire, West Yorkshire

Table 2: Example dashcam cases

Case, court and date	Summary
Scott vs Harris, 2010, United States Supreme Court [18]	Deputy Scott accused of using excessive force to stop claimants car after a car chase. Dashcam footage upheld Deputy Scott's case
Regina vs Luke Whitchard, 2015 [65]	Third party dashcam captures Whitchard dangerously overtaking cars on a bend.
Regina Vs Stocks, 2015, Mold and Caernarfon Crown Court [63]	Dashcam footage captures James Stocks recklessly overtaking other drivers - closely missing a van driver which is forced off the road
Regina v Collins 2017/05113/A2 113 EWCA, 2018 Old Bailey [70]	Patrick Collin's dashcam captures Collins knocking over and killing Selwyn Clarke and a conversation admitting the accident moments later
German supreme court, 2018 [53]	Plaintiff argues video footage of him crossing a red light breaches privacy laws. Supreme court rules against the plaintiff.
Regina vs Marc Hyland, 2018, Northallerton Magistrates [44]	Marc Hayland overtakes a series of vehicles waiting to turn
Regina vs Ryan Haffenden, 2017, Brighton Magistrates Court [24]	Haffenden overtakes vehicles on a single carriageway - narrowly missing a pedestrian and avoiding collision with oncoming traffic.
Regina vs Andrew Williams EWCA Crim 1886 WL 03777362 (Court of Appeal Criminal Division), 2018, Nottingham Magistrates Court [42]	Andrew Williams was drunk and driving in speeds in excess of 120mph Vehicle veered onto the hard shoulder and almost crashed into a motorcyclist.
Regina v Lewes Marcin Dariusz Purlis, EWCA Crim 1134, 2017, (Criminal Division) [15]	Purlis convicted of robbery. Dashcam footage captured by a third party was instrumental as was the evidence by a facial mapping expert
Gajdamowicz v First Glasgow Ltd, 2017, All Scotland Sheriff Court [52]	Cyclist - Gajdamowicz knocked over by a bus attempting to overtake. Bus camera shows Gajdamowicz wearing headphones and not indicating prior to moving into the path of the bus. Case ruled in favour of First Glasgow.
Shane Mullen and Gez Bennett, 2015, Warwick Crown Court [8]	Assailants carjacked a car and were captured in the car's dashcam admitting the theft.
Regina v Welsby (Ian), 2017, Hull Crown Court [19]	Third party dashcam shows Ian Welsby clipping a motorcyclist Colin Walker as he (Ian) cut a corner as he turned into a side street.
McIntosh v Harman [2018] EWHC 726 (QB), 2018, Queen's Bench Division [61]	Police dashcam records PC Susan McIntosh knocked down by Barry Harman as she (Susan) was interviewing members of the public.
Regina v Thompson (Chloe May) EWCA Crim 1291 Court of Appeal [23], 2017, Maidstone Crown Court	Chloe Thompson crashed into the back of a vehicle at 80-88mph killing a grandmother. Dashcam footage captured on a car travelling in the same direction.
Harvey Schofield, 2018, Chester Magistrates' Court, [12]	Harvey Schofield undertook a tipper truck and pulled out into the path of a vehicle causing him to slam his brakes.

The term *third party* is used in the table to refer to a person or persons not directly involved in the incident.

vehicular speed, and Kim et al. [31] proposed the *vehicle speed estimate method (VSEM)* as a means of estimating vehicle speed.

2.2. Extracting elements

Videos and images contain important textual data within the watermark and/or in the recorded scene. Previous research has attempted to extract text from images using a *Fully Convolutional Network* (FCN) model [71] or a *Convolutional Neural Network* (CNN) model [25], to extract watermarks [1] and licence plate numbers [37] from video images.

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 [38].

2.3. Assessing authenticity

A useful body of research has attempted to establish the authenticity of video footage. Koenig and Lacey [33] outline a number of 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. [28] propose a system which protects recordings from tampering by third parties 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. [32] detects image tampering by analysing noise characteristics - referred to as a *noise level function (NLF).*

Source camera identification methods attempt to identify the camera used to make a photograph or video. One of the earlier contributions into source camera identification was presented by Kurosawa et al. [35] who proposed a method to identify camcorders from the noise patterns created by a charge coupled device (CCD) fingerprint. Lukáš et al. [39] use *Sensor Pattern Noises* (SPNs) as device fingerprints which can be used to identify digital devices. The problem with SPNs is that they can be contaminated by scene based noise, Li [36] propose a mechanism for addressing this and enhancing the device detection rate.

A lot of the research into camera identification focuses on high quality images. The contribution by van Houten et al. [67] attempts to identify the source camera from low-quality videos.

Mehrish et al. [40] propose a framework for identifying the vehicle within which dashcam footage was recorded. Their system uses motion patterns in the vehicle which create a unique blurring effect on videos.

Algorithms used to identify the source camera of a photographic/video imagery can also be used to detect the authenticity of photographic/video imagery. This was demonstrated by Mondaini et al. [41] who used the SPN to detect forged videos. Chen et al. [11] proposed a framework for identifying both the source of an image and the likelihood of the image having been tampered by analysing the *photo-response nonuniformity noise* (PRNU).

Hsu et al. [22] attempt to reveal forged sections of video imagery from noise residue using noise correlation. The method proposed by Hsu et al. requires still backgrounds and requires low video compression.

2.4. Addressing privacy

The use of dashcams pose privacy risks because they are - as Wagner et al. puts it *"surveillance systems that are operated by private individuals in public places"* [68]. Wagner et al. propose a solution which identifies and disguises individuals faces and licence plates from a dashcam.

Such privacy concerns could inhibit the submission of dashcam evidence. The study by Park et al. [48] 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 [48, 59]. 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."* [16], there are concerns that GDPR and other regulating laws are not properly regulating the use of dashcams [68].

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 a number of related themes as highlighted herein, there is no known research into the prevalence and provenance of evidential artefacts created by the use of dashcams. As the use of dashcams increases, it will become increasingly important for law enforcement agencies and researchers to understand the location, format and sources of evidential artefacts. This paper attempts to address this imbalance.

3. Challenges Relating to the Management and Processing of Dashcam Evidence

Notwithstanding the convenience that online dashcam evidence submission provides, there are two potential challenges relating to dashcam evidence:

- deterrents to witness engagement with the submission because of concerns about inadvertent self-incrimination of traffic rule violation, or inadvertently contravening privacy regulation (the latter is discussed in Section 2.4);
- challenges to the admissibility of digital evidence submitted online.

The rest of this section considers challenges related to the admissibility of dashcam evidence.

Whilst the provision of online dashcam evidence submission could lead to an increase in successful prosecutions, this should be considered against the increased investigative resource requirements such as increased processing time and storage capacity.

A greater challenge however, relates to the admissibility of online dashcam evidence submission. Witnesses submitting dashcam evidence generally have no evidential procedure/chain of custody training. There is a period of time where the evidence is not under the control of a law enforcement authority and potentially not governed by chain of custody rules. This can create admissibility challenges. Consequently, safeguards must be built into the submission process relating to *file modification, submission timeliness, footage timespan* and *evidence sharing.*

These problem have been considered by UK police forces and the position of some police forces in relation to the timespan between an incident and the submission of the associated evidence, requirement for unedited video footage, existence of a timestamp watermark in the video footage and pre-post incident footage is outlined in Table 3 and described herein.

Modification. Tools such as NextBase Player 3 allow users to join/trim videos, create title screens, and adjust output settings. In an attempt to ensure that video is unaltered, some police forces require unedited video footage (outlined as *UEF* in Table 3) which contains a timestamp (outlined as *TS* in Table 3). There is a rich body of research which proposes methods for the detection of video forgery - for instance [22] and [60] and more recently [34] and [58].

Timeliness. Most police forces specify a maximum time period between the road traffic incident being reported to the evidence being uploaded (outlined as *DSI* in Table 3). This may be because suspects in the UK must be served with a 'notice of intended prosecution' within 14 days of the commission of the offence [64]. Although the 14 day time limit (where applied) aims to resolve this, a submission made within 14 days of a declared date is not a guarantee that the incident took place on that date. There is some scope for timestamps to be manipulated. Notwithstanding, laws relating to *perverting the course of justice* (or the equivalent in local jurisdictions) aim to prevent evidence tampering and should be sufficient to deter individuals from modifying timestamps [13].

Footage timespan. Some police forces require that the submission includes pre-incident and post incident footage (outlined as *BaAI* in Table 3). For example, Surrey Police require that 2 minutes

Table 3: Sample police constabulary requirements on the submission of online dashcam evidence

Police Forces	**DSI**	**BaAI**	**TS**	**UEF**
Wiltshire	10	✓	✓	X
Wawrickshire	NK	X	✓	X
West Mercia	NK	X	✓	X
West Midlands	NK	X	✓	X
North Yorkshire	NK	X	X	X
Avon and Somerset	7	✓	✓	X
Essex	2	X	X	✓
Cheshire	3	X	X	X
Surrey	10	✓	X	X
Sussex	10	X	X	X
Hampshire	10	✓	✓	X
Metropolitan Police	10	✓	X	X
Thames Valley	10	✓	X	X
Norfolk	NK	X	✓	X
Suffolk	NK	X	✓	X
Dyfed-Powys	14	X	X	✓
Gwent	14	X	X	✓
North-Wales	14	X	X	✓
South-Wales	14	X	X	✓

DSI: Days since incident; *BaAI:* requires before and after incident recording; *TS:* requires a time stamp; *UEF:* requires unedited footage only; *NK:* not known of pre-incident and post incident footage are included in the submission. The reason for this is to provide context to the incident in question.

Evidence sharing. Cases risk being compromised if evidence is shared with third parties and/or published online. Sharing evidence in this way could be considered contempt of court [50]. Many constabularies remind witnesses that evidence must not be shared with third parties nor published online.

The examination of methods to address these challenges is beyond the scope of the contribution. However, it is useful to briefly outlines some of the techniques and mechanisms that could be employed to

4. Experiment

This section reports on the prevalence and provenance of evidential artefacts by the use of seven dashcams. An experiment was conducted to correlate dashcam features with the evidential artefacts created by their use and to identify where the artefacts can be located. The experiment aimed to discover the prevalence of evidential artefacts relating to:

- Recordings made in emergency mode or through triggering the g-sensor in parking mode.
- GPS data.
- Vehicular speed data.
- Licence plate information.
- Temporal data.

A number of dashcam features were not analysed and could form the basis for further research. These include: the microphone facility (available on all dashcams), the use of the voice command feature (Garmin), the invocation of the time autoupdate facility (SilentWitness), red light/speed camera warnings (Garmin), forward collision warning (Garmin), lane departure warnings (Cobra, Garmin) and wifi connectivity (Nextbase 312, Nextbase 512, Garmin). All the dashcams except the Garmin, recorded videos in the *mov* format, the Garmin recorded videos in the *mp4* format.

4.1. Dashcams

Dashcams record audio and video, and are also capable of recording photographs. Dashcams are user-configurable and enable users to set - for example, the recording mode, licence plate, and set whether a watermark is recorded in the video/photographic footage.

4.1.1. Recording Mode

Dashcams make video recordings in one of four modes: *normal, emergency, parking* and *time-lapse*. The recording mode can help explain the context of an incident.

Normal recordings are made when the ignition is turned on or when a user presses the record button.

Emergency recordings are made when either the user presses the emergency recording button or when the g-sensor (gravity sensor) is activated. The g-sensor is an accelerometer which measures

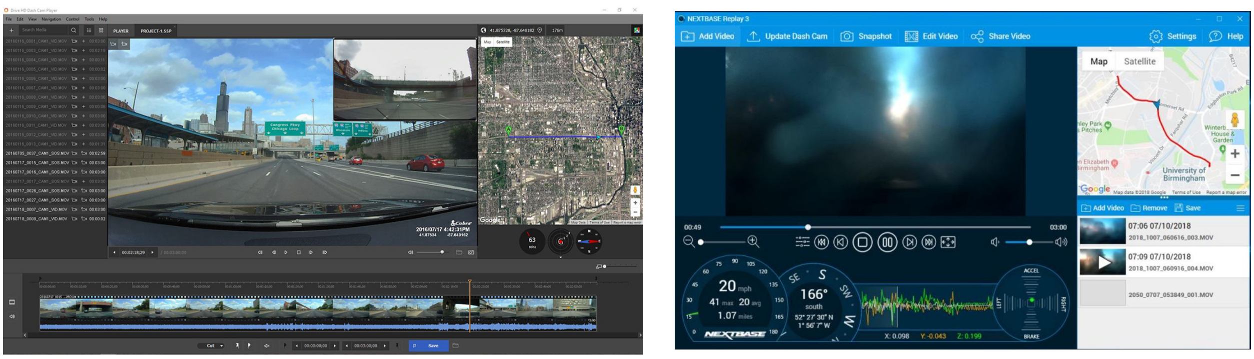


Figure 1: The Cobra video player software (left) and the Nextbase Replay 3 software (right)

excessive deceleration or acceleration in any axis - such as with an impact when the car is parked (*parking mode*).

Emergency and parking recordings are recorded with write attributes disabled and cannot be overwritten under normal usage. Often these recordings are saved into a uniquely named directory.

A *time-lapse* recording is essentially a sequence of images which reduce the amount of storage occupied by a recording. The Nextbase 512 for example, can record timelapse videos at $1/6^{\text{th}}$ of the normal speed.

4.1.2. Licence Plate Information

Some dashcams enable users to enter a registration/licence plate number for the car in which the dashcam is installed. Whilst licence plate information was displayed in the watermarks on some dashcam models (as shown in Table 4), this study could find no evidence of licence plate data being displayed elsehwere - for example in the metadata.

4.2. Materials.

Seven dashcams: Cobra HD CDR 895D, Garmin 55, Mio MiVue 538, Nextbase 512GW, Nextbase 312GW, RAC205 and SilentWitness SW006 - referred to hitherto as Cobra, Garmin, MiVue, Nextbase512, Nextbase312, RAC and SilentWitness respectively, were tested under varying conditions to reveal artefacts of forensic interest. These dashcams were selected because they represented a wide variety of dashcam features such as the *emergency recording mode, parking mode, and recording of license plate data* as outlined in Section 4.1.

4.3. Process

A series of recordings were made using each dashcam in turn. An 8GB SD card was used to make the recordings. This contained sufficient storage space and no recordings were overwritten. A dataset comprising of 7 dashcam recordings recorded on 16GB SD cards is available to accompany this paper. Further details on how to obtain this are provided in the front matter to this paper.

Each recording lasted around three hours. Features such as GPS, licence plate, the G-sensor etc., were enabled if available on the dashcam. Where the feature was available, a number of recordings were specifically made in each of the recording modes described in Section 4.1.1.

Dashcams allow users to set the length of each recording. For example, the Mivue allows users to select 1, 3 or 5 minute recordings. Some dashcams issue a warning when the SD card is full, others - for instance the Garmin, automatically overwrite the oldest recording. The recording length for each dashcam was left at the default setting.

Each SD card was removed from the dashcam and a digital forensic image (`.E01` format) was created. This was then analysed to reveal the location and format of evidence created. Folder locations and filenames were observed using EnCase and Autopsy.

4.4. Analysis Methods

Three types of tool: *dedicated forensic tools, external metadata viewers,* and/or *native video players* were used to analyse the digital forensic images.

4.4.1. Dedicated forensic tools

Although dedicated forensic tools such as Encase, FTK and Autopsy, were used to analyse the digital forensic image, 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.

4.4.2. Native Video Player

Native video players are available for most dashcams (Figure 1). Native video players synthesise the video footage, a map, and vehicular speed data into a single user interface. These tools are generally not accepted in courts and often do not have a provision for extracting the metadata. However, native video players can be a useful aid to verifying the findings of dedicated forensic tools. Native video players were available for all the dashcams except Silent Witness.

4.4.3. Specialist Metadata Extraction Tools

Exiftools [20] is a specialist tool which enable analysts to extract metadata. *Exiftools* is dedicated to the extraction of EXIF data. The command: `exiftool -ee FILENAME` (where `-ee` means *extract embedded*), displays GPS data, vehicular speed and associated timestamps for file `FILENAME`, and the command: `exiftool -T -FileName -CreateDate - Modifydate -FileSize *.MOV *JPG` extracts dates from all files with the extension `.mov` and `.jpg`. An example of the output from *exiftools* is provided as follows:

```
Sample Duration    :  0.25s
GPS Latitude       :  52 deg 28' 9.40'' N
GPS Longitude      :  1 deg 55' 24.25''
GPS Speed          :  26
GPS Speed ref      :  mph
Sample Time        :  0.25s
Sample Duration    :  0.25s
```

5. Results

Table 4 outlines the results of the experiment. The table abbreviates each source as follows: ***N****MEA files (a)*, ***c****onfiguration/diagnostic files (c)*, ***E****XIF metadata (e)*, ***d****irectory structures (d)*, ***f****ilenames (f)*, and ***w****atermarks (w)*.

The table correlates each feature with the associated evidential artefact. This section describes the provenance and prevalence of evidential artefacts in further detail.

5.1. NMEA (a)

NMEA (National Marine Electronics Association) files contain both temporal and GPS data. These files have a. `.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`.

Examples of fields that contain temporal data include: `$GPBWC, $GPZDA, $PMGNTRK` and `$PRWIINIT` [14].

These fields are referred to as *sentences*. A brief explanation of some of these fields is presented herein, for a more detailed explanation, the reader is referred to [5] and [56]

Table 4: Matrix of dashcams, features and prevalence of artefacts

Make	Emergency recording			Parking mode				GPS				Speed			License plate	Time					
Cobra	$\otimes$	f	p	$\otimes$	f	$\otimes$	$\otimes$	§	§	§	§	e	n	w	$\otimes$	$\otimes$	$\otimes$	$\otimes$	f	$\otimes$	w
Nextbase 312GW	d	$\otimes$	p	d	$\otimes$	$\otimes$	p	$\otimes$	e	n	w	e	n	w	w	$\otimes$	$\otimes$	e	f	n	w
Nextbase 512GW	d	$\otimes$	p	d	$\otimes$	$\otimes$	p	$\otimes$	e	n	w	e	n	w	w	$\otimes$	$\otimes$	e	f	n	w
SilentWitness[1]	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	e	$\otimes$	$\otimes$	e	$\otimes$	w	w	$\otimes$	$\otimes$	$\otimes$	f	$\otimes$	w
MiVue	d	f	p	d	f	n	$\otimes$	a	e	n	w	e	n	w	$\otimes$	a	$\otimes$	e	f	$\otimes$	w
Garmin	$\otimes$	$\otimes$	$\otimes$	d	$\otimes$	$\otimes$	p	$\otimes$	e	n	w	e	n	w	$\otimes$	$\otimes$	c	e	$\otimes$	n	w
RAC[1]	$\otimes$	f	p	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	w

Key: [1]does not have a native video player *a*=NMEA file, *c*=configuration file, *d*=directory structure, *e*=EXIF data in video, *f*=filename, *n*=native video player, *p*=write protection, *w*=watermark
§ Optional extra, not included in the system analysed in this research
$\otimes$ not available

The `$GPRMC` field provides GPS transit data as well as response times from the satellite. The following example:

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

can be translated as follows:

- `070851.00` is the time of fix (07:08:51 UTC);
- `A` = valid (where `V` would mean an invalid fix);
- `5227.77102,N` means Latitude 52 deg. 27.77 min North (or 52d27'77"N);
- `00156.72583,W` Longitude 1 deg. 56.72583 min West (or 1d56'72"W);
- `0.032` The speed over ground calculated in knots;
- `078.7` course made good which is the direction the vehicle is travelling from true North;
- `041018` - the date of the fix;
- `010.3,E` the magnetic variation - in this case 10.3 deg East;
- `6C` - a mandatory checksum.

The `$GPGGA` sentence provides GPS fix data and includes data relating to the time and position. The following example:

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

can be translated as follows:

- `071010.00` : UTC time of the fix (07:10:10 UTC)
- `5227.76885,N` : 52d 27.76885' North (or 52d27'76"N);
- `00156.61993,W` : 1d 56.61993'West (or 1d56'61"W)
- `1` : Data is from a GPD fix;
- `08` : there are 8 GPS satellites in use;
- `1.20` : this is the relative accuracy of the horizontal position; `151.9, M` : This is the distance above mean sea level; `48.0 M` : This is the height of the geoid above WGS84 ellipsoid
- `x.x` : not present in the above example, but the age of the differential GPS data measured in seconds;
- `42` : checksum

Tools such as the NMEA convertor [46] can be used to convert NMEA to KML which can then be uploaded to and viewed in Google Earth.

5.2. Configuration Files (c)

Configuration files reveal system configuration and diagnostic data. Examples of this are provided in the Garmin and MiVue dashcams.

Two key diagnostic files in the Garmin dashcam are the `drive_hours_logger.db` and the `elog.JSON`. The `drive_hours_logger.db` is an SQL file which contains logs of journey times. Each journey time has a corresponding `create_timestamp` field which presents the time that the entry was created - indicating the start of the journey. This time is presented in `YYY-MM-DD HH_MM_SS` format. The `elog.JSON` file stores error data. Two particular fields in the XML file are of importance, these are the `uptime_ms` field which outlines the time that the unit has been operational in milliseconds, and the `error_cause` (with *Low Battery Shutoff* indicating that the unit closed down because of a failed battery) which has a corresponding `Time` field indicating the time that the unit closed down. This field has the format `YYYY-MM-DD HH:MM:SS`.

Similarly, the MiVue saves one configuration file: `DEVICE.XML` which stores a range of configuration data such as: the firmware version (`FWVersion`), the product name (`ProductName`), the operating system (`OSVersion`), the memory size (`MemorySize`) and the storage size (`StorageSize`).

5.3. Directory Structure (d)

The directory naming structure can reveal the recording mode. Table 5 outlines the directory structure of the seven dashcams under investigation.

The table shows that the Garmin dashcam saves files with directory names such as `100PARKM` and `104TLPSE` to indicate recordings made in *parking* mode and *timelapse* mode respectively. Similarly, the Nextbase dashcams split normal videos and videos recorded in *emergency* or *parking* mode into the `NBDVR/VIDEO/VIDEO` and `NBDVR/VIDEO/PROTECTED` respectively.

Dashcams such as the Cobra, SilentWitness and RAC make no distinctions within the directory structure.

5.4. Filename Structure (f)

Filename structures can reveal: temporal data; file sequences; and the recording mode. Of these, the temporal data and recording mode are of importance to the present study. The data provided in Table 4 shows that 5 of the 7 filename structures (Cobra, Nextbase 512GW, Nextbase 312G, SilentWitness and MiVue), reveal temporal information. Table 5 shows the filename structure for each dashcam under investigation.

The Table show for example, that 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.

3 of the 7 filename structures (Cobra, MiVue and RAC) reveal the recording mode within the filename. So in the same filename format, `TTT` is any of `JPG` (photo), `MOV` (movie) or `SOS` which indicates that the recording was made using the emergency function or with the GSensor facility activated. Similarly, the MiVue has a video filename format: `TTTTYYMMDD-HHmmSS.MOV`, where `TTTT` can be `EMER` for emergency recordings, `FILE` for normal recordings, and `PARK` for recordings made in parking mode.

Table 5: Directory/filename structures

Make	Filename/directory structure
Cobra	**Filename:** `YYYYMMDD_NNNN_CAMN_TTT.EXT` `TTT`: is any of `JPG` (photo), `MOV` (movie); `SOS`: a recording made using the emergency function or with the GSensor facility activated; `NNNN`: sequence number; `CAMN`: camera, where `CAM1` and `CAM2` are the forward and reverse facing cameras respectively e.g., `20160101_0006_CAM1_VID.MOV`, `20160101_0010_CAM1_IMG.JPG` and `20181106_0004_CAM1_SOS.MOV` **Directory:** `DCIM/100/DSC` : all files
Garmin	**Filename:** `GRMSNNNN.EXT` where `EXT` could be `MP4` or `JPG` e.g., `GRMN0021.MP4` **Directory:** `DCIM/100EVENT` : GSensor activated recordings; `DCIM/101PHOTO` : photos; `DCIM/102SAVED` : *normal mode*; `DCIM/103PARKM` : *parking mode*; `DCIM/104TLPSE` : *timelapse mode*; `DCIM/105UNSVD` : unsaved video footage
Nextbase312	**Filename:** `YYYY_MMDD_HHmmSS_NNN.EXT` e.g., `2018_1007_051316_001.jpg` **Directory:** `DCIM/PHOTO` : photos; `DCIM/VIDEO` : videos; `DCIM/PROTECTED` : *parking mode*
Nextbase512	**Filename:** `YYYY_MM_DD_HHmmSS_NNN.EXT` e.g., `2018_100_7_051316_001.jpg` **Directory:** `NBDVR/PHOTO` : photos; `NBDVR/VIDEO` : videos; `NBDVR/VIDEO/PROTECTED` : *parking mode* and *emergency mode*
SilentWitness	**Filename:** `MMDDHHmm_NNNN.EXT` **Directory:** `DCIM/100Media` : *normal mode*⋆
MiVue	**Filename:** Photos: `IMGYYMMDD-HHmmSS.JPG` Video: `FILEYYMMDD-HHmmSS.MOV`, where `FILE` can be `EMER` for emergency recordings, `FILE` for normal recordings, and `PARK` for recordings made in parking mode. **Directory:** `Emergency` : *emergency mode*; `Normal` : *normal mode*; `Parking` : *parking mode*; `Photo` : photos
RAC	**Filename:** `XXXXNNNN.EXT`, where `XXXX` is a four-letter prefix which can have the values: `MOV_` for recordings, `IMAG` for pictures and `SOS_` for emergency-saved files. **Directory:** `100_NOML` : contains all the recorded files‡.

Key: `YYYY`: year; `MM`: month; `DD`: date; `HH` hour (24 hour); `mm` minutes; `SS` seconds. In all examples, `NNNN` is the sequence number.
†Files named according to the DCIM standard [27]. `\elog.json` - Error log, stores data such as power shutdown due to poor battery; `Garmin/Garmin.XML` - System configuration data; `/Garmin/Diag/GarminOS.log` - a record of when the Garmin was turned on; `/.System/SQLite/drive_hours_logger` - SQL database ‡`/DCIM/DATA` Contains a file called `GSensor_Info.txt`
⋆`/Player` - stores the native video player for the dashcam
All the dashcam devices store local time and not UTC time - this is notwithstanding the data stored in the NMEA files (described in Section 5.1)

Filenames can be correlated with the system file timestamps and watermark (w) timestamps to help determine whether filenames have been tampered with.

5.5. Application Metadata (e)

Artefacts such as timestamps and GPS data can be found in the application metadata within video files using tools such as *exiftools* (geospatial and temporal data from within video files) as shown in Section 4.4.3.

6. Discussion

Having outlined the sources of evidential artefact, it is useful to summarise where the features outlined in Section 4 can be located in a dashcam SD card. The data is provided comprehensively in Table 4 and can be summarised briefly here.

6.1. GPS data

GPS data is found in at least four places:

- as a *watermark* (w) within the video if the feature has been enabled (highlighted in Figure 2).
- In the EXIF metadata (e) within video files. This can be recovered using specialist tools such as *exiftools* and *log2timeline* - as shown in Section 4.4.3.
- In NMEA data - as shown in Section 5.1.
- In a native video player (n) (Figure 1) - as shown in Section 4.4.2.

6.2. Vehicular speed data

Vehicular speed data can be viewed using a native video player (n) as a *watermark (w)* within the video if the feature has been enabled (Figure 2), and as EXIF metadata (e) within the metadata as described in Section 4.4.3.

6.3. Licence plate information

Licence plate information is only available as a *watermark (w)* within the video if the feature has been enabled (this is shown in Figure 2 right).

6.4. Temporal data

The analysis of time is important not only to identify the time of the incident under investigation, but because the time could be deliberately manipulated by a suspect to argue an alibi. All the dashcams under investigation - and presumably on the market, record temporal data. Table 4 shows that temporal data can be found in at least five locations:

- Within The *NMEA* file (a) which pulls time data from GPS systems - as shown in Section 5.1.
- Within *configuration* files (c) - as shown in Section 5.2.
- As *EXIF metadata (e)* - within MOV/MP4/JPG files - as shown in Section 5.5.
- Within the *filename* structure (f) - as shown in Section 5.4.

Figure 2: [Left] A dashcam watermark from a Garmin dashcam [Right] A dashcam watermark from a Nextbase312 dashcam demonstrating licence plate data

- As a *watermark (w)* within the video if the feature has been enabled - as shown in Figure 2.

In addition to these locations, temporal data is also available in the following locations:

- Within the *video imagery* itself where daytime/nightime recording can be clearly seen. Systems such as *Suncalc* [21] can be used to help determine the time (Figure 3).
- As *system metadata* in file timestamps. This has been explained in detail by [10] and [47] and many other authors and will not be repeated here.

7. Conclusions

Insofar as the author is aware, this is the first significant contribution to analysing the sources of evidential artefacts in a dashcam system. The research outlined herein creates a number of opportunities for further research in an area that is becoming increasingly important.

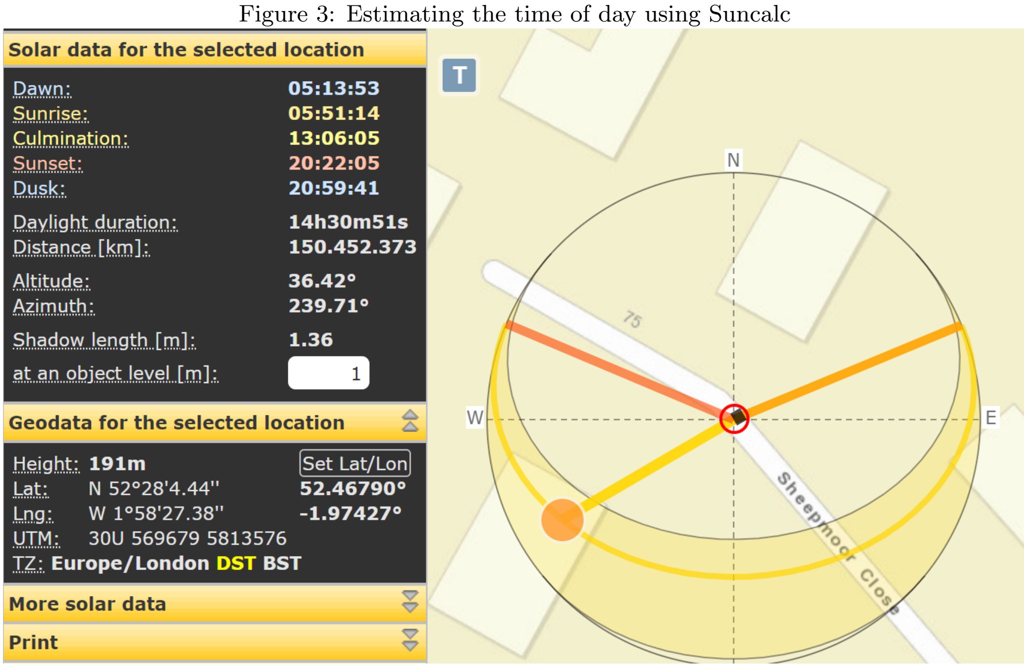
This research has highlighted the problems related to the management and processing of dashcam evidence and has applied a particular emphasis on analysing the evidential artefact sources in a dashcam. The research showed that the artefacts are available in seven locations - namely the NMEA file, configuration files, directory naming structures, EXIF metadata, filename structures, file system attributes, and watermarks. The research also showed that evidential artefacts can be synthesised using proprietary tools such as native video players.

Section 4.3 outlined that there were a number of dashcam features which were not investigated in this study. These features include the the microphone facility, the use of the voice command feature (Garmin), the invocation of the time autoupdate facility (SilentWitness), red light/speed camera warnings (Garmin), forward collision warning (Garmin), lane departure warnings (Cobra, Garmin) and Wi-Fi connectivity (Nextbase 312, Nextbase 512, Garmin). These areas are all worthy of further investigation, and in particular, it would be useful to determine if the use of the Wi-Fi facility on a dashcam leaves evidentiary artefacts in other locations.

This research explored the evidentiary artefacts created by the dashcam on an SD card. The research has not investigated the existence of evidentiary artefacts left directly on the dashcam – or methods of extracting these artefacts.

This research has shown that a number of tools were required to extract and analyse the evidential artefacts. Better methods are required for extracting and synthesising the metadata from dashcams. This work could include the extraction of watermark data and other data within the imagery itself

Figure 3: Estimating the time of day using Suncalc



to identify location and objects. A number of contributions have previously considered this [26, 54]. However, a cursory investigation of the literature appears to show that there is a dearth of material specifically evaluating the efficacy of extracting metadata from watermark data using OCR techniques.

Section 6.4 outlined the locations of the temporal data that can be found within dashcam devices. Collectively, the paper has shown that there is a wide range of both geospatial and temporal data on a dashcam. The discussion herein has not proceeded to provide additional information on the relationships between the range of geospatial and temporal data. This is an area for future research - which might particularly focus on both synthesising this data and analysing it.

References

[1] Al-maweri, N. A. A. S., Sabri, A. Q. M., and Mansoor, A. M. (2016). Automatic rotation recovery algorithm for accurate digital image and video watermarks extraction. *International Journal ogf Advanced Computer Science and Applications*, 7(11):65–72.

[2] Asikuzzaman, M. and Pickering, M. R. (2018). An overview of digital video watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(9):2131–2153.

[3] Aviva (2017). The Connected Car. A Study of Motorists' Views on Cars and Technology. Technical report, Aviva.

[4] Aviva (2018). Dash for dash cams. Date accessed: 1-11-18.

[5] Baddeley, G. (2001). GPS - NMEA sentence information. Date accessed: 30-9-19.

[6] Baker, J. (2018). Appeal for Dash Cam Footage. Date accessed: 20-09-2018.

[7] Barkham, P. (2015). The Road to Britain's Dashcam Boom. Date accessed: 1-11-2018.

[8] BBC (2015). Coventry Carjackers Jailed After Voices Recorded on Dashcam. Date accessed: 1-11-2018.

[9] Birajdar, G. K. and Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital investigation*, 10(3):226–245.

[10] Buchholz, F. and Spafford, E. (2004). On the role of file system metadata in digital forensics. *Digital Investigation*, 1(4):298–309.

[11] Chen, M., Fridrich, J., Goljan, M., and Lukás, J. (2008). Determining image origin and integrity using sensor noise. *IEEE Transactions on information forensics and security*, 3(1):74–90.

[12] Cheshire Police (2018). Man Convicted of Dangerous Driving Thanks to Dashcam Footage. Date accessed: 1-11-2018.

[13] CPS (2019). Public Justice Offences incorporating the Charging Standard. Date accessed: 1-10-2019.

[14] DePriest, D. (2019). Nmea data. Technical report.

[15] England and Wales Court of Appeal, Criminal Division (2018). [2017] EWCA Crim 1134. Date accessed: 1-11-2018.

[16] European Parliament (2014). Parliamentary questions. Date accessed: 1-11-2018.

[17] Farid, H. (2009). Image forgery detection. *IEEE Signal processing magazine*, 26(2):16–25.

[18] FindLaw (2014). United States Supreme Court, SCOTT v. HARRIS, (2007). Date accessed: 1-11-2018.

[19] Hartley-Parkinson, R. (2017). Pensioner jailed for killing biker after ignoring DVLA note to renew his licence.

[20] Harvey, P. (2019). Exiftool.

[21] Hoffmann, T. (2019). Suncalc.

[22] Hsu, C.-C., Hung, T.-Y., Lin, C.-W., and Hsu, C.-T. (2008). Video forgery detection using correlation of noise residue. In *2008 IEEE 10th workshop on multimedia signal processing*, pages 170–174. IEEE.

[23] Hunt, Keith (2017). Chloe Thompson Jailed for Causing Death of Anne Tongs in M25 Crash Near Swanley. Date accessed: 1-11-2018.

[24] ITV News (2017). Dangerous Driver Convicted Thanks to Dashcam Footage. Date accessed: 1-11-2018.

[25] Jaderberg, M., Simonyan, K., Vedaldi, A., and Zisserman, A. (2016). Reading text in the wild with convolutional neural networks. *International Journal of Computer Vision*, 116(1):1–20.

[26] Jalil, Z. and Mirza, A. M. (2010). An invisible text watermarking algorithm using image watermark. In *Innovations in Computing Sciences and Software Engineering*, pages 147–152. Springer.

[27] Japan Electronic Industry Development Association (1998). Design Rule for Camera File System. Technical report. 1-11-18.

[28] Kadu, S., Cheggoju, N., and Satpute, V. R. (2018). Noise-resilient Compressed Domain Video Watermarking System for In-car Camera Security. *Multimedia Systems*, 24(5):583–595.

[29] Kafer, T. (2018). Forensic report = accident uber-volvo 18.03.2018. Technical report, Car-Forensics.

[30] Kamat, D. D. and 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)*, pages 1–5. IEEE.

[31] Kim, J.-H., Oh, W.-T., Choi, J.-H., and Park, J.-C. (2018). Reliability Verification of Vehicle Speed Estimate Method in Forensic Videos. *Forensic Science International*, 287:195–206.

[32] Kobayashi, M., Okabe, T., and Sato, Y. (2010). Detecting forgery from static-scene video based on inconsistency in noise level functions. *IEEE Transactions on Information Forensics and Security*, 5(4):883–892.

[33] Koenig, B. E. and Lacey, D. S. (2015). Forensic authentication of digital audio and video files. *Handbook of Digital Forensics of Multimedia Data and Devices*, pages 133–181.

[34] Kono, K., Yoshida, T., Ohshiro, S., and Babaguchi, N. (2018). Passive video forgery detection considering spatio-temporal consistency. In *International Conference on Soft Computing and Pattern Recognition*, pages 381–391. Springer.

[35] Kurosawa, K., Kuroki, K., and Saitoh, N. (1999). Ccd fingerprint method-identification of a video camera from videotaped images. In *Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348)*, volume 3, pages 537–540. IEEE.

[36] Li, C.-T. (2010). Source camera identification using enhanced sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 5(2):280–287.

[37] Li, H. and Shen, C. (2016). Reading car license plates using deep convolutional neural networks and lstms. *arXiv preprint arXiv:1601.05610.*

[38] Limantoro, S. E., Kristian, Y., and 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(2).

[39] Lukáš, J., Fridrich, J., and Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2):205–214.

[40] Mehrish, A., Subramanyam, A., and Kankanhalli, M. (2017). Multimedia signatures for vehicle forensics. In *IEEE International Conference on Multimedia and Expo (ICME)*, pages 685–690, Hong Kong, China. IEEE.

[41] Mondaini, N., Caldelli, R., Piva, A., Barni, M., and Cappellini, V. (2007). Detection of malevolent changes in digital video for forensic applications. In *Security, steganography, and watermarking of multimedia contents IX*, volume 6505, page 65050T. International Society for Optics and Photonics.

[42] Naylor, M. (2018). Lexus crash driver who was over the limit clocked doing 121mph - by his own dashcam. Date accessed: 1-11-18.

[43] Nextbase (2018). Caught an Incident on Your Dashcam or Another Device? Date accessed: 1-11-18.

[44] North Yorkshire Police (2018). Suspended prison sentence for dangerous driver reported to Operation Spartan.

[45] Nottinghamshire Police (2017). Request under the freedom of information act 2000 (foia).

[46] NVS Technologies (2012). Converter NMEA to KML. Date accessed: 20-09-2018.

[47] Olsson, J. and Boldt, M. (2009). Computer forensic timeline visualization tool. *digital investigation*, 6:S78–S87.

[48] Park, S., Kim, J., Mizouni, R., and Lee, U. (2016). Motives and Concerns of Dashcam Video Sharing. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4758–4769, San Jose, California, USA. ACM.

[49] Ranjan, S., Garhwal, P., Bhan, A., Arora, M., and Mehra, A. (2018). Framework for image forgery detection and classification using machine learning. In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, pages 1–9. IEEE.

[50] Roberts, J. and Hodgetts, C. (2015). Courting Contempt?: Untangling the Web of Jurors' Internet Use Under Section 8 of the Contempt of Court Act 1981. *Communications Law*, 20(3):86.

[51] Rocha, A., Scheirer, W., Boult, T., and Goldenstein, S. (2011). Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics. *ACM Computing Surveys (CSUR)*, 43(4):26.

[52] Scottish Courts and Tribunals (2017). Roksana Gajdamowicz Against (First) First Glasgow Limited and (Second) Keith Moffat. Date accessed: 1-11-18.

[53] Sheahan, Maria (2018). Dashcam Footage Gets Top German Court Approval for Car Crash Cases. Date accessed: 1-11-18.

[54] Shen, M. and Lei, H. (2015). Improving ocr performance with background image elimination. In *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, pages 1566–1570. IEEE.

[55] Sherwin, R. K., Feigenson, N., and Spiesel, C. (2006). Law in the Digital Age: How Visual Communication Technologies are Transforming the Practice, Theory, and Teaching of Law. *Boston University Journal of Science and Technology Law*, 12:227.

[56] Si, H. and Aung, Z. M. (2011). Position data acquisition from nmea protocol of global positioning system. *International Journal of Computer and Electrical Engineering*, 3(3):353.

[57] Singh, R. D. and Aggarwal, N. (2018). Video Content Authentication Techniques: a Comprehensive Survey. *Multimedia Systems*, 24(2):211–240.

[58] Sitara, K. and Mehtre, B. (2019). Differentiating synthetic and optical zooming for passive video forgery detection: An anti-forensic perspective. *Digital Investigation*, 30:1–11.

[59] Štitilis, D. and Laurinaitis, M. (2016). Legal Regulation of the Use of Dashboard Cameras: Aspects of Privacy Protection. *Computer Law & Security Review*, 32(2):316–326.

[60] Subramanyam, A. V. and Emmanuel, S. (2012). Video forgery detection using hog features and compression properties. In *2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP)*, pages 89–94. IEEE.

[61] TG Chambers (2018). McIntosh v. Harman [2018] EWHC Civ – 06.04.2018. Date accessed: 1-11-2018.

[62] The AA (2017). Dash Cams and Your Car Insurance. Date accessed: 1-11-2018.

[63] The Daily Telegraph (2015). Dash cam footage of dangerous overtaking lands driver in jail in UK first. Date accessed: 1-11-2018.

[64] The National Archives (1988). Road Traffic Offenders Act 1988. Date accessed: 1-11-2018.

[65] The South Wales Argus (2015). Motorist banned from driving after 'moment of madness' overtaking car on bend caught on camera. Date accessed: 1-11-2018.

[66] Turner, B. L., Caruso, E. M., Dilich, M. A., and Roese, N. J. (2019). Body camera footage leads to lower judgments of intent than dash camera footage. *Proceedings of the National Academy of Sciences*, 116(4):1201–1206.

[67] van Houten, W., Geradts, Z., Franke, K., and Veenman, C. (2010). Verification of video source camera competition (camcom 2010). In *Recognizing Patterns in Signals, Speech, Images and Videos*, pages 22–28. Springer.

[68] Wagner, P., Birnstill, P., Krempel, E., Bretthauer, S., and Beyerer, J. (2017). Privacy Dashcam–Towards Lawful Use of Dashcams Through Enforcement of External Anonymization. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 183–201. Springer.

[69] Witness Confident (2018). Witness Confident. Date accessed: 1-11-2018.

[70] Your Local Guardian (2017). Croydon Man Jailed After Fatal Crash With Pedestrian . Date accessed: 1-11-2018.

[71] Zhang, Z., Zhang, C., Shen, W., Yao, C., Liu, W., and Bai, X. (2016). Multi-oriented text detection with fully convolutional networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4159–4167.

Acknowledgment

The authors would like to thank David Hegedus and Deryck Greer (MSc., graduates, University of Warwick) for their inputs into Table 3.