Dashcam Forensic investigation Guidelines

Dr. Harjinder Singh Lallie
Discipline Group Leader (Cyber Security)
University of Warwick
HL@warwick.ac.uk

Sundry

- Lallie, H.S., 2020. Dashcam forensics: a preliminary analysis of 7 dashcam devices. *Forensic Science International: Digital Investigation*, *33*, p.200910.
- Lallie, H.S., 2023. Dashcam forensic investigation guidelines. *Forensic Science International: Digital Investigation*, vol45, Supplement 2023, 301558, ISSN 2666-2817

- Dashcam datasets available for research

- 19th Teaching digital forensics, November, Warwick

Nick Simper
Roger Glover
CANIS MAJOR
LEPUS
COLUMBA
PUPPIS
Bobby Woodman-Clarke
Neil Diamond
Graham Bonnet
R1.15
R1.03 &

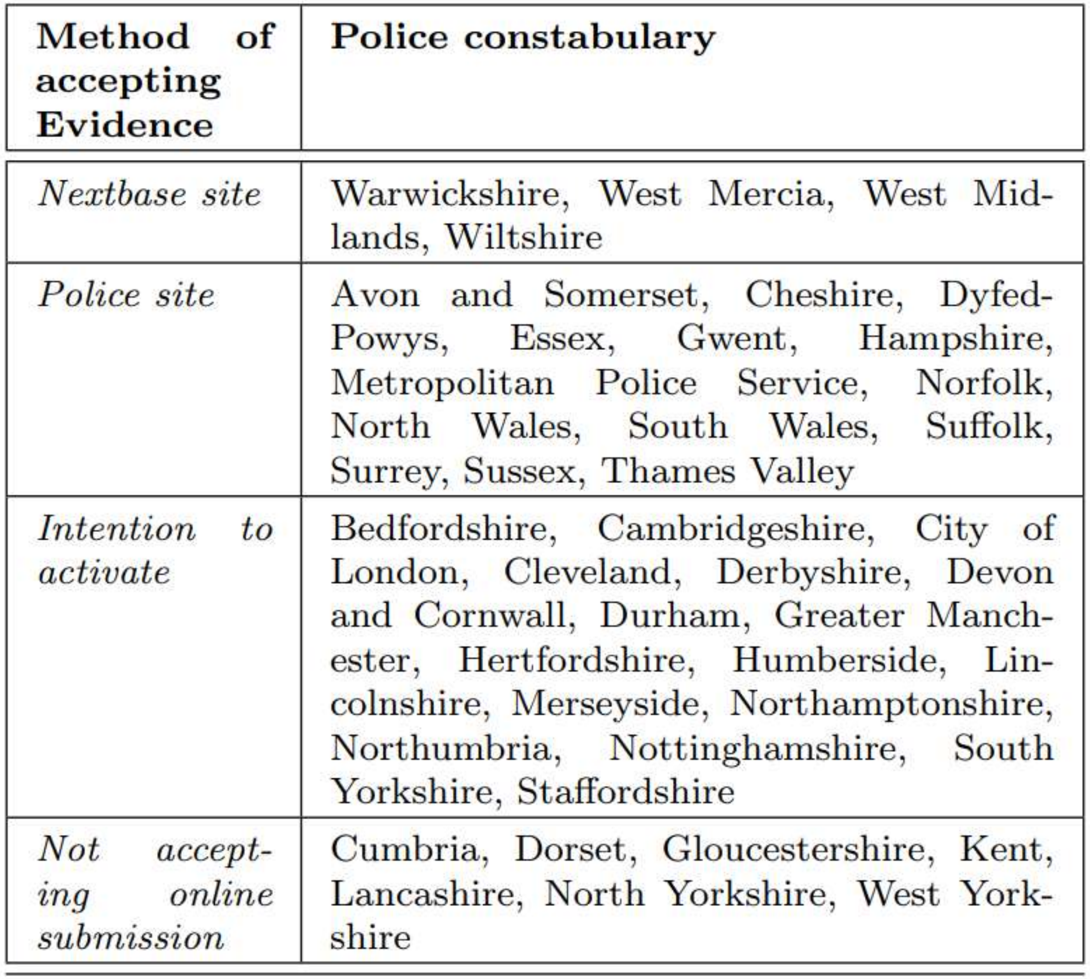
Background

Previous contributions

- **Vehicle speed** (Kafer 2018, Kamat and Kinsman 2017, Kim et al 2018, Zhou et al 2022)
- **Text object/extraction** (Zhang et al., 2016, Jaderberg et al., 2016, Al-maweri et al., 2016, Li and Shen, 2016, Limantoro et al., 2018).
- **Assessing authenticity** (Koenig and Lacey, 2015, Kadu et al., 2018, Kobayashi et al., 2010, Kurosawa et al., 1999, Lukas et al., 2006, Li 2010, Kurosawa et al., 1999, Yang et al., 2020).
- **Addressing privacy** (Wagner et al., 2017, Zhu et al., 2020, Park et al., 2016, Stitilis and Laurinaitis, 2016)
- **Analysing dashcam evidence** (Lallie 2020, Lee et al 2021)

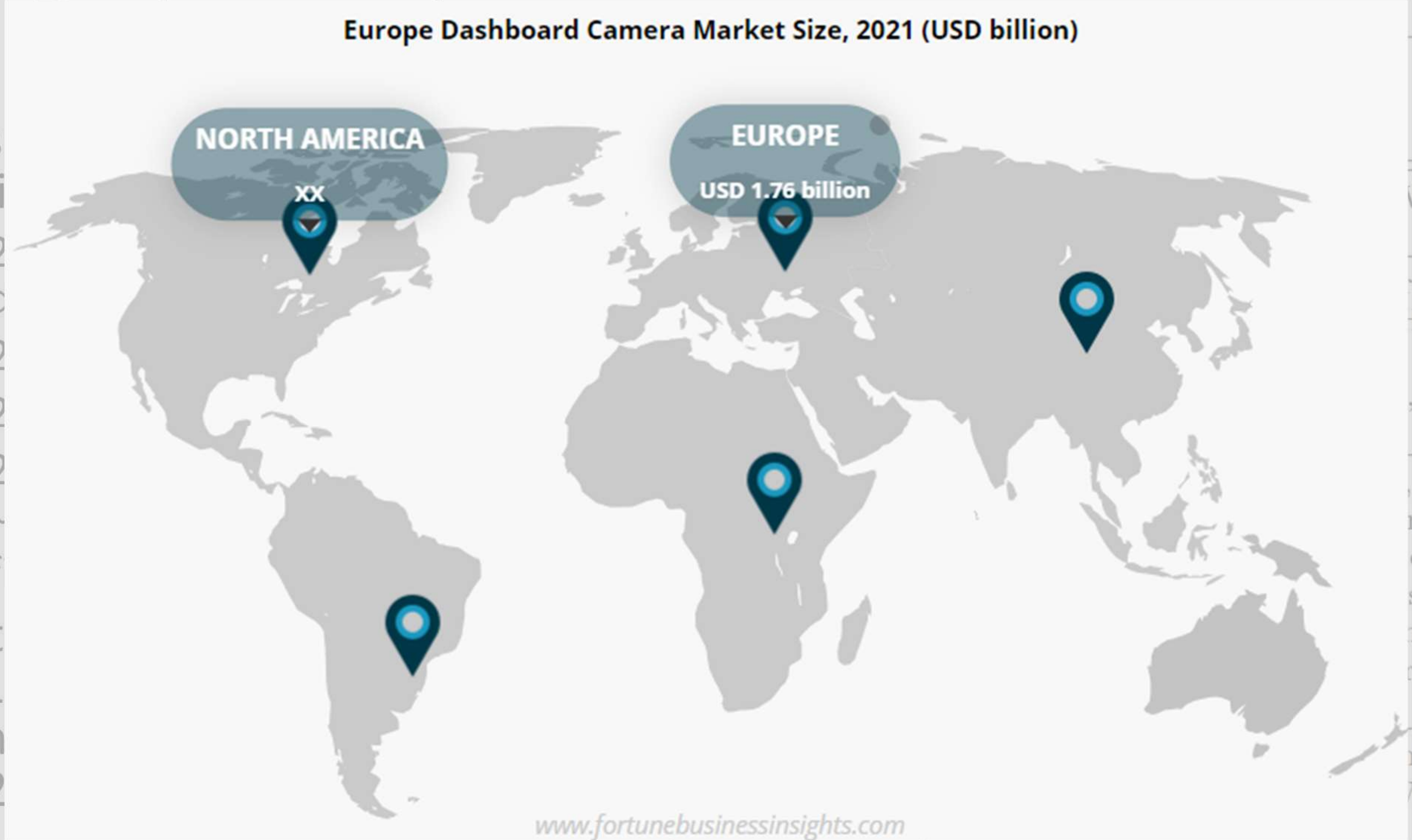
Background

- Dashcam usage increasing rapidly in the UK.
  - 2015, 9% of drivers were using dashcams
  - 2016: 15%
  - 2017: 17%
  - 2018: 27%
  - ~2026, may become a standard fixture
- Nottingham Police recorded 211,598 dashcam records over a three year period leading up to 2017.



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

- Das
  rapi
  - 2
    c
  - 2
  - 2
  - 2
  - ~
    f
- Not
  211
  a th
  to 2



Europe Dashboard Camera Market Size, 2021 (USD billion)

West Mid-

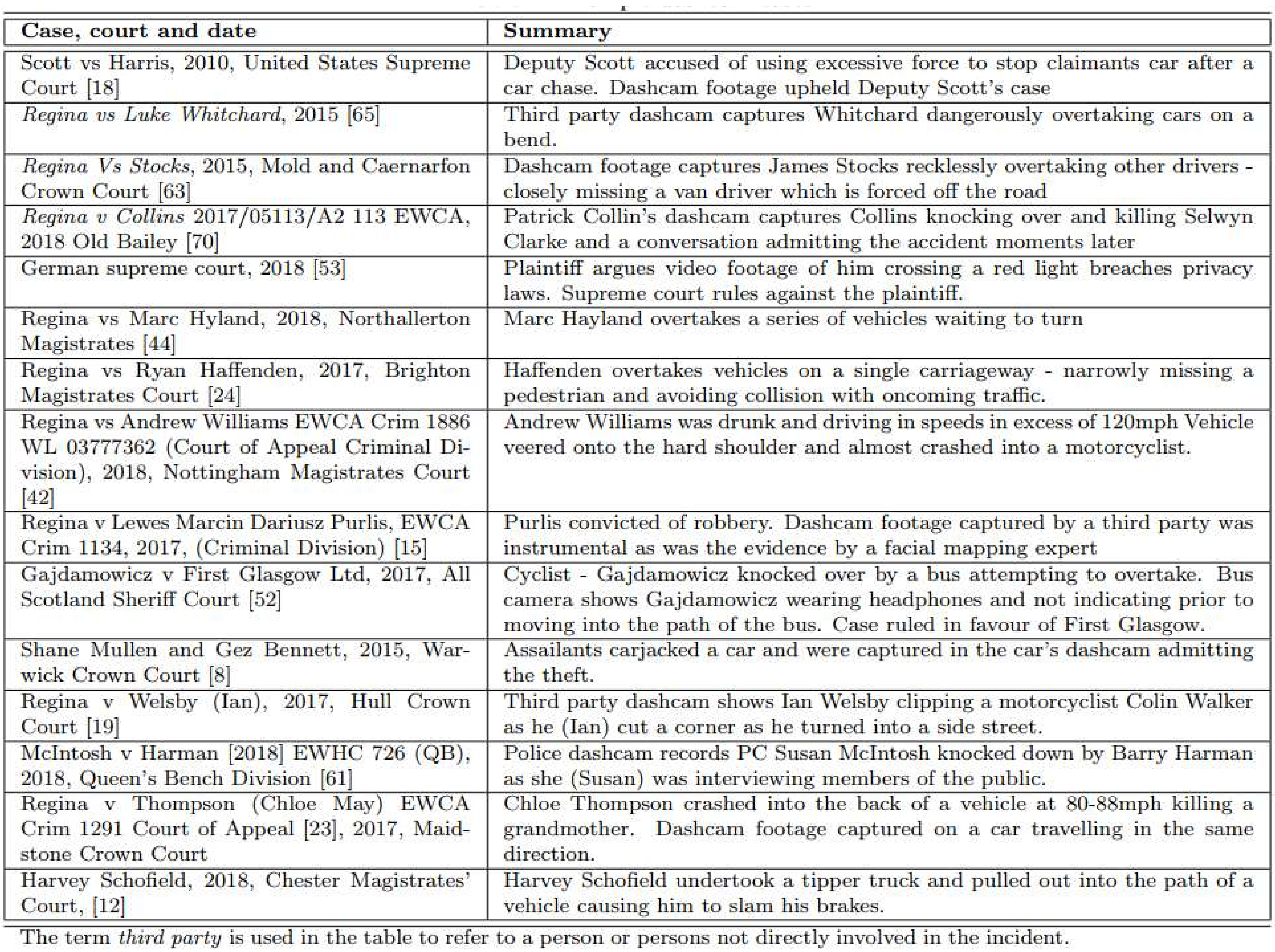
re, Dyfed-
Hampshire,
Norfolk,
, Suffolk,

, City of
re, Devon
er Manch-
side, Lin-
nptonshire,
re, South

hire, Kent,
West York-

https://www.fortunebusinessinsights.com/dashboard-camera-market-103046

Dashcam evidence is appearing in an increasing number of court cases



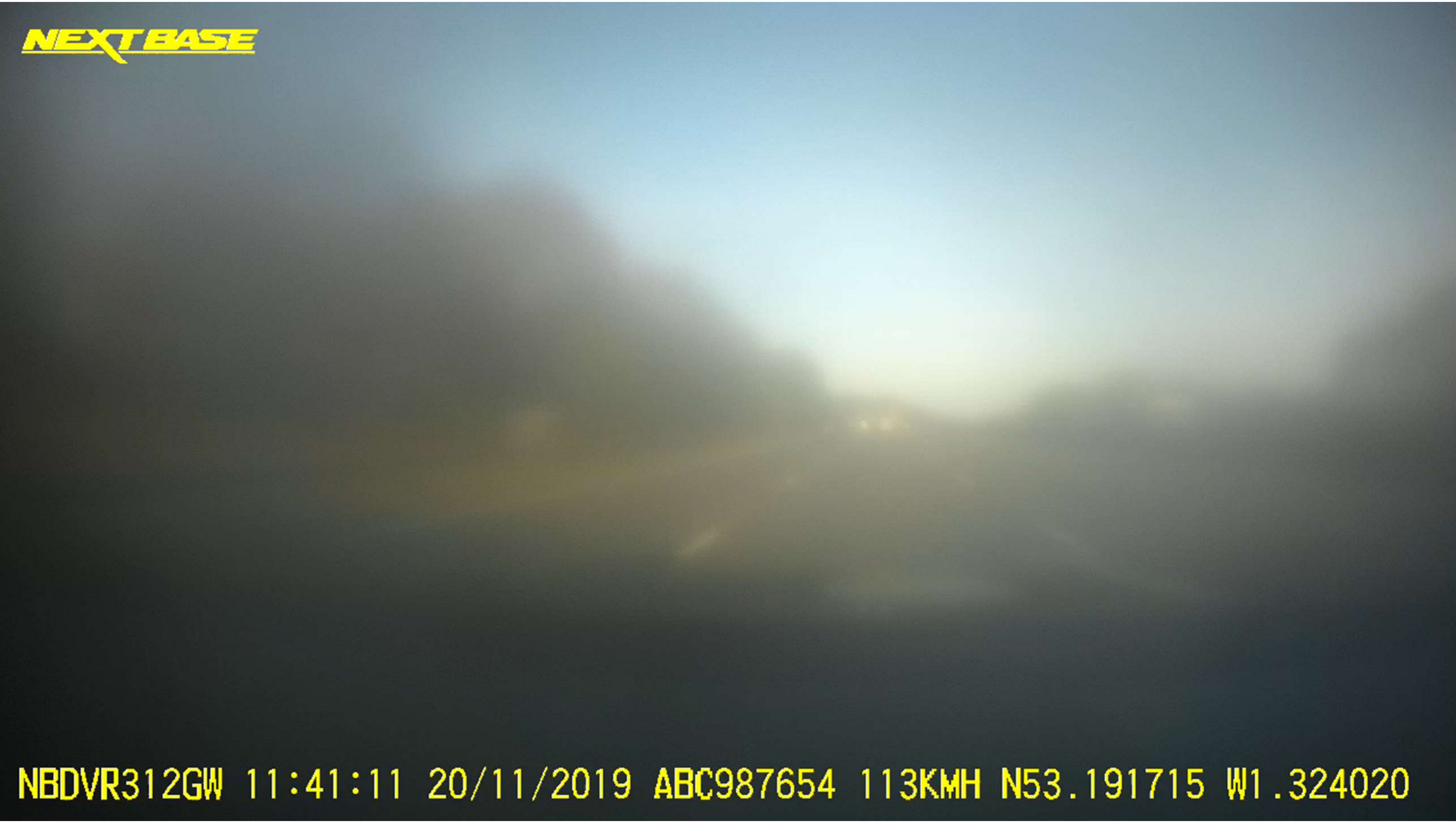
Case, court and date	Summary
Scott vs Harris, 2010, United States Supreme Court [18]	Deputy Scott accused of using excessive force to stop claimants car after a car chase. Dashcam footage upheld Deputy Scott's case
Regina vs Luke Whitchard, 2015 [65]	Third party dashcam captures Whitchard dangerously 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.

There are no tools or guidelines on how to investigate, rendering the risk of miscarriage

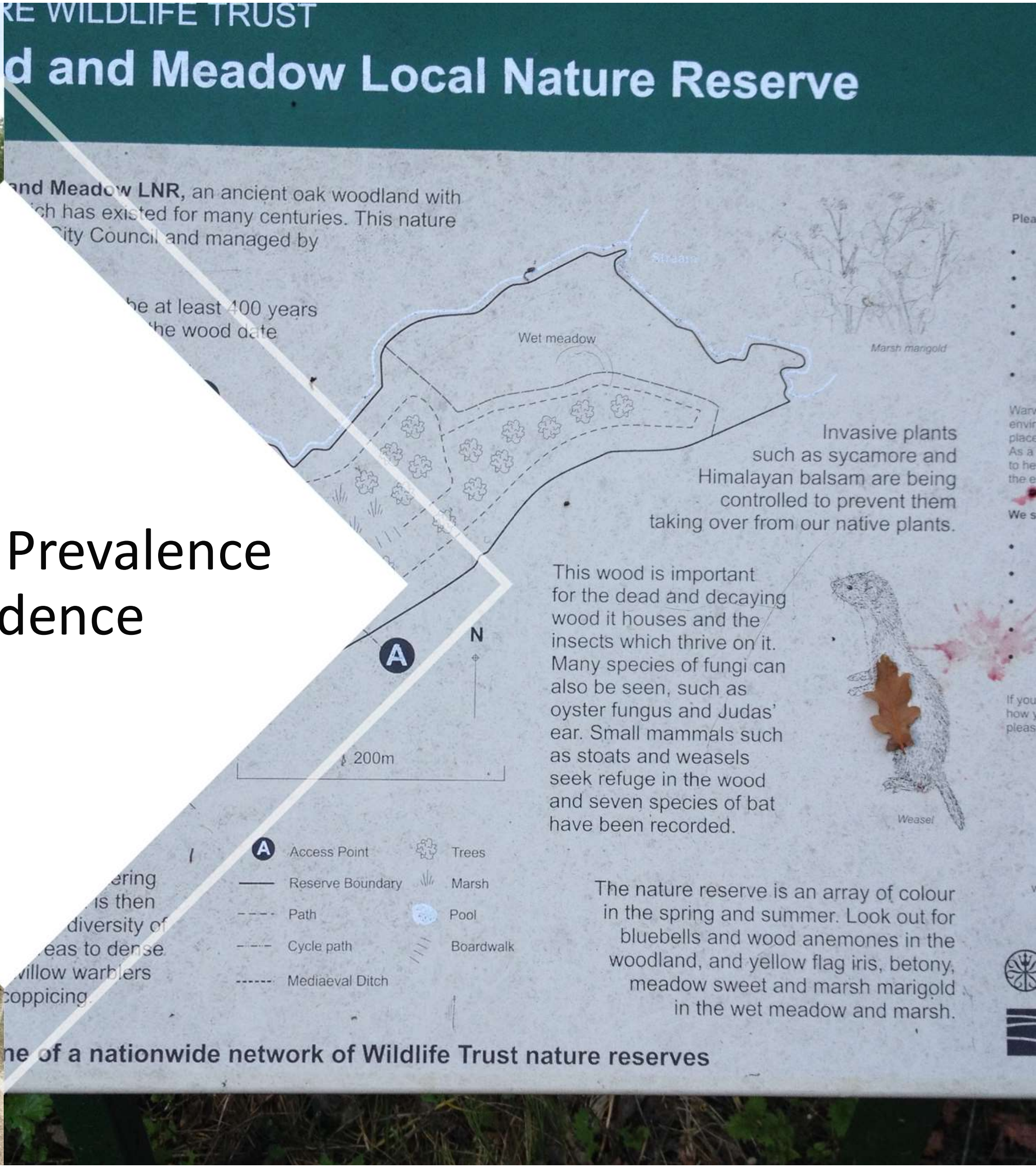
Data Gathering

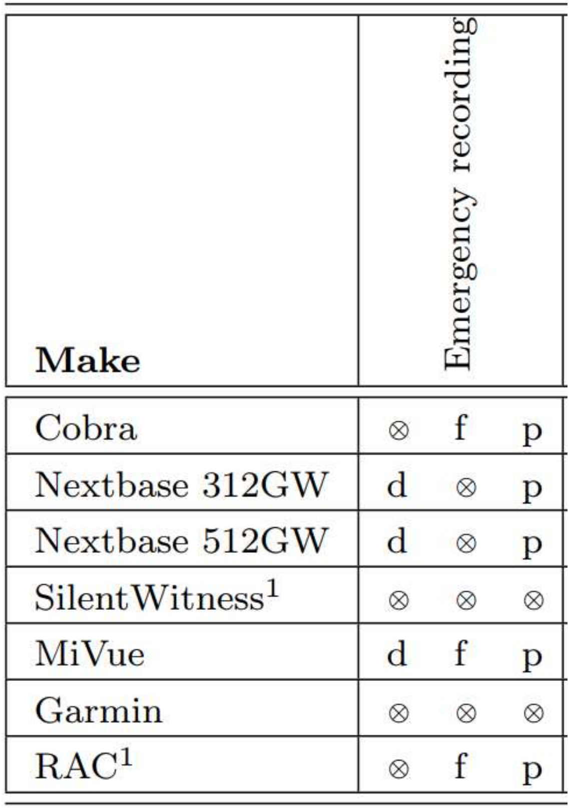
NEXTBASE
NEXTBASE
Transcend
Trip computer
Classic
8:29 am
8:08 am
21 min
3 mls
23.5 mpg
[redacted]
[redacted]



NBDVR312GW 11:41:11 20/11/2019 ABC987654 113KMH N53.191715 W1.324020

Range and Prevalence of Evidence


RE WILDLIFE TRUST
d and Meadow Local Nature Reserve
and Meadow LNR, an ancient oak woodland with
ich has existed for many centuries. This nature
City Council and managed by
be at least 400 years
the wood date
Stream
Wet meadow
Marsh marigold
Invasive plants such as sycamore and Himalayan balsam are being controlled to prevent them taking over from our native plants.
This wood is important for the dead and decaying wood it houses and the insects which thrive on it. Many species of fungi can also be seen, such as oyster fungus and Judas' ear. Small mammals such as stoats and weasels seek refuge in the wood and seven species of bat have been recorded.
Weasel
N
A
200m
A Access Point
Reserve Boundary
Path
Cycle path
Mediaeval Ditch
Trees
Marsh
Pool
Boardwalk
ering
is then
diversity of
eas to dense
willow warblers
coppicing
The nature reserve is an array of colour in the spring and summer. Look out for bluebells and wood anemones in the woodland, and yellow flag iris, betony, meadow sweet and marsh marigold in the wet meadow and marsh.
ne of a nationwide network of Wildlife Trust nature reserves
Plea
We s
If you
how y
pleas



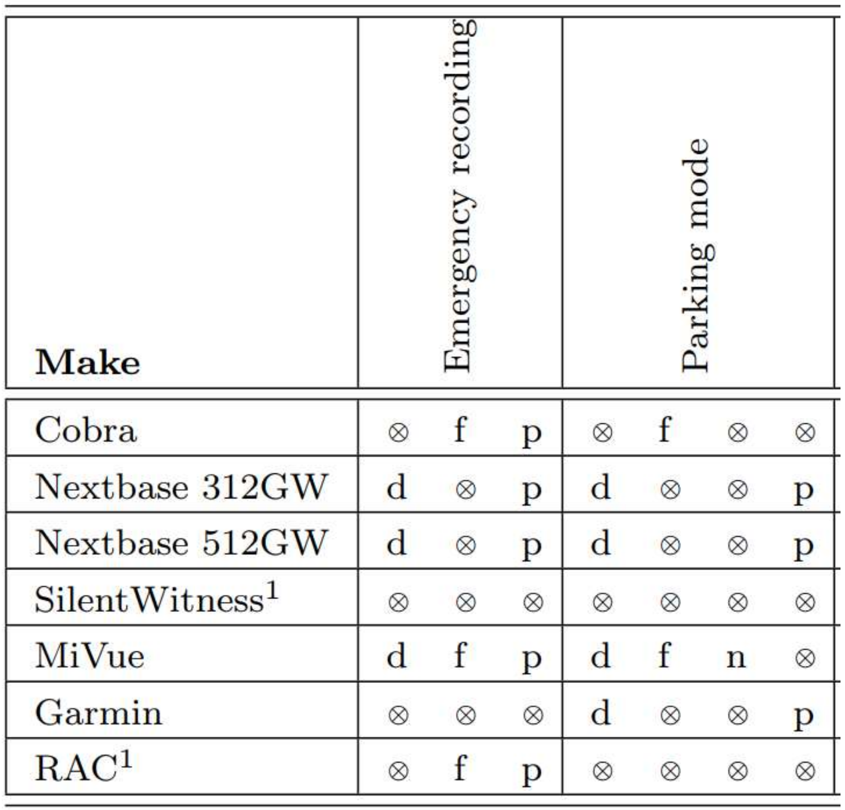
Make	Emergency recording		
Cobra	⊗	f	p
Nextbase 312GW	d	⊗	p
Nextbase 512GW	d	⊗	p
SilentWitness[1]	⊗	⊗	⊗
MiVue	d	f	p
Garmin	⊗	⊗	⊗
RAC[1]	⊗	f	p

User initiates an emergency recording in the event of an incident. Evidence found in directory names, file names, and in file attributes (files are write protected)

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

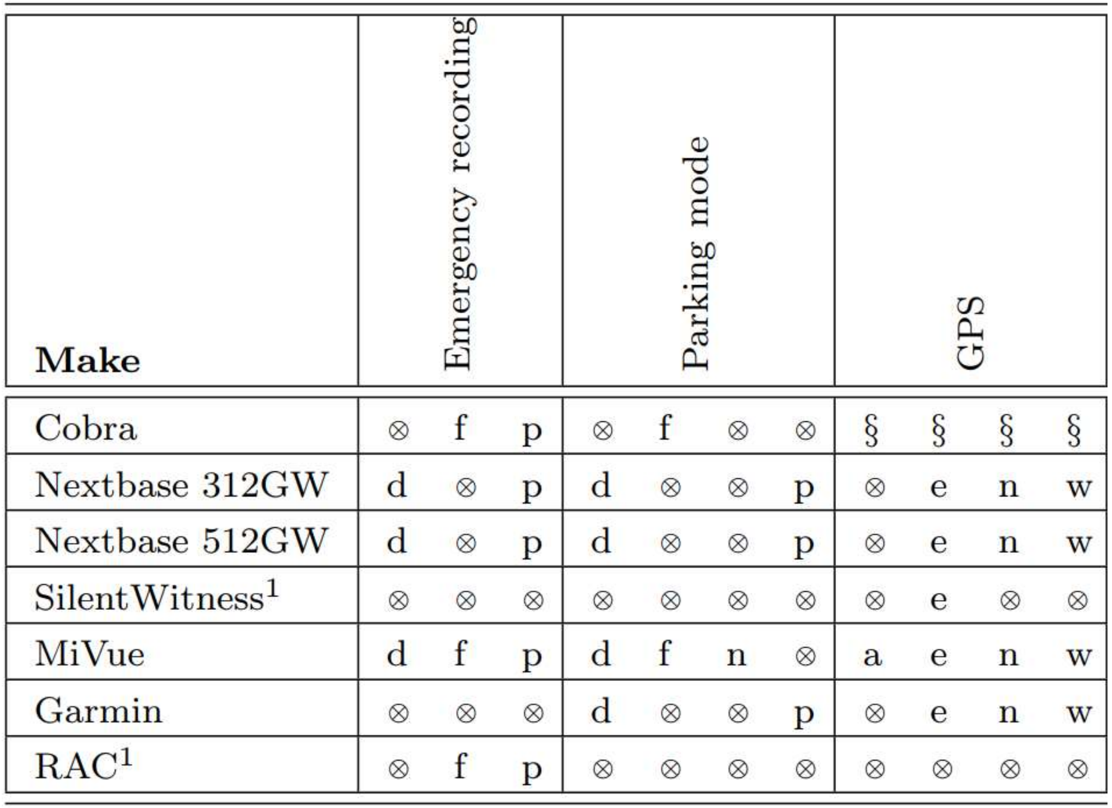
⊗ not available



Make	Emergency recording			Parking mode			
Cobra	⊗	f	p	⊗	f	⊗	⊗
Nextbase 312GW	d	⊗	p	d	⊗	⊗	p
Nextbase 512GW	d	⊗	p	d	⊗	⊗	p
SilentWitness[1]	⊗	⊗	⊗	⊗	⊗	⊗	⊗
MiVue	d	f	p	d	f	n	⊗
Garmin	⊗	⊗	⊗	d	⊗	⊗	p
RAC[1]	⊗	f	p	⊗	⊗	⊗	⊗

A sudden impact on the car, whether parked or not, initiates an emergency recording. Evidence found in directory names, file names, and in file attributes (files are write protected)

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
⊗ not available



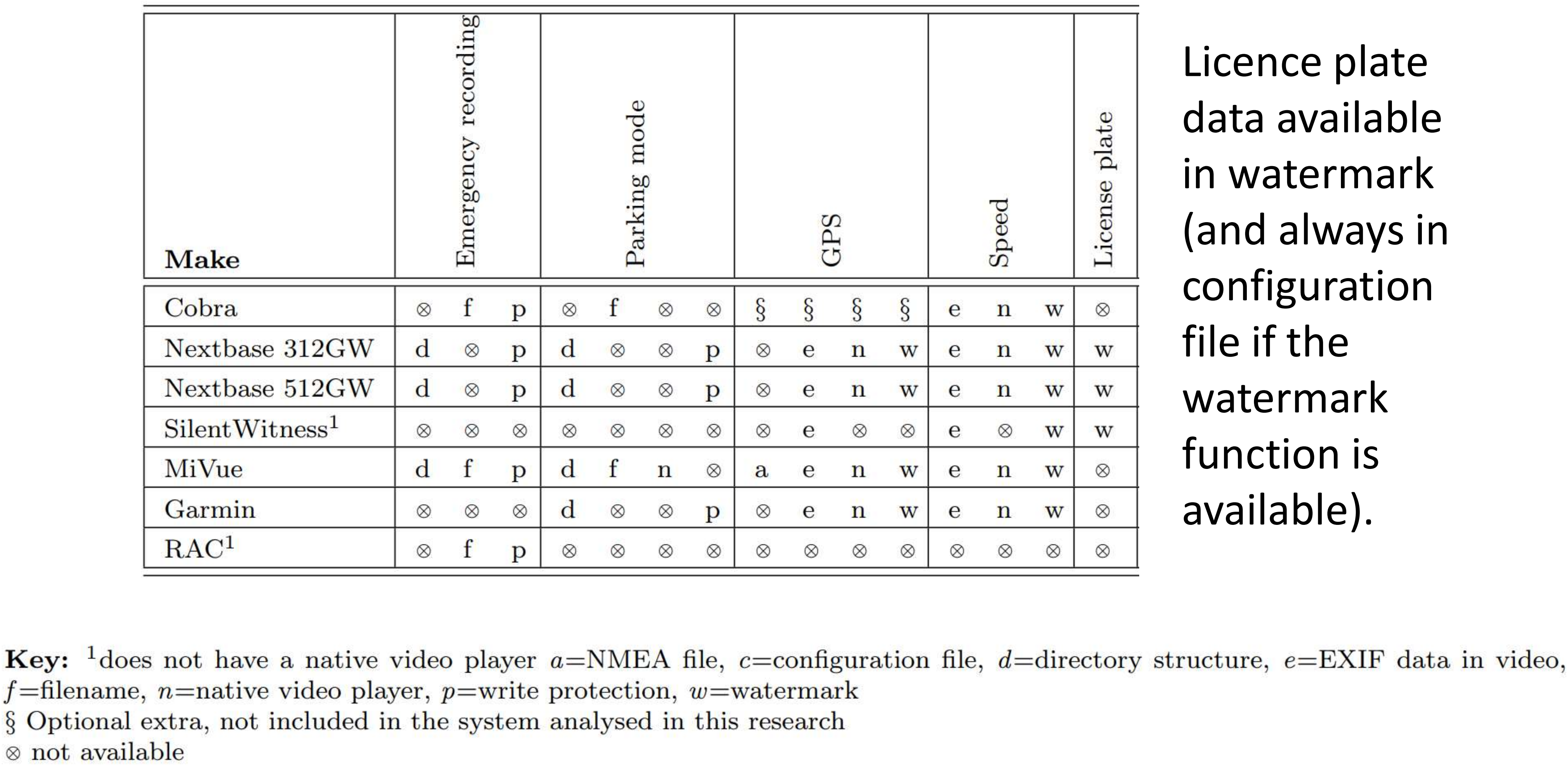
Make	Emergency recording			Parking mode				GPS			
Cobra	⊗	f	p	⊗	f	⊗	⊗	§	§	§	§
Nextbase 312GW	d	⊗	p	d	⊗	⊗	p	⊗	e	n	w
Nextbase 512GW	d	⊗	p	d	⊗	⊗	p	⊗	e	n	w
SilentWitness[1]	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	e	⊗	⊗
MiVue	d	f	p	d	f	n	⊗	a	e	n	w
Garmin	⊗	⊗	⊗	d	⊗	⊗	p	⊗	e	n	w
RAC[1]	⊗	f	p	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗

GPS coordinate are stored in NMEA files, EXIF data, a watermark and in some cases, only accessible through a native video player,

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

⊗ not available



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

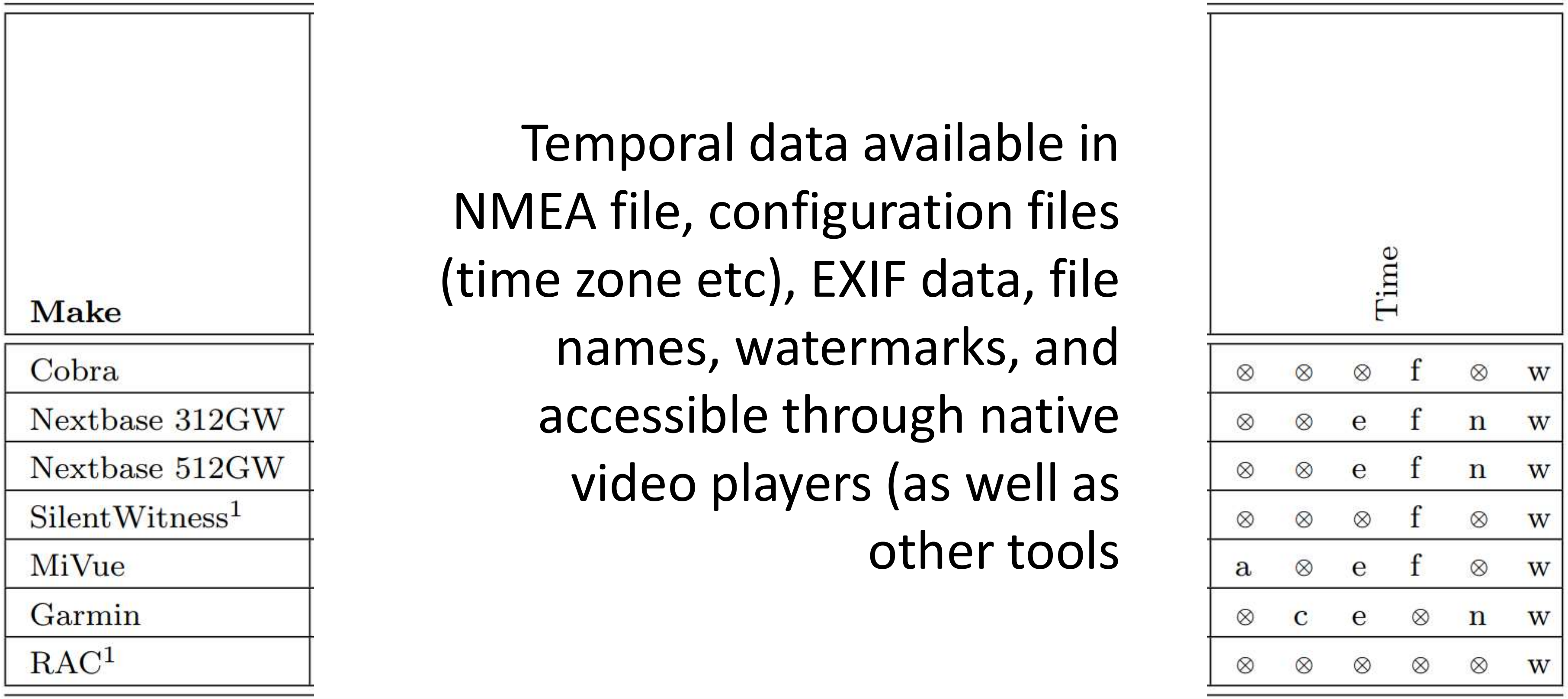
Key: [1]does not have a native video player *a*=NMEA file, *c*=configuration file, *d*=directory structure, *e*=EXIF data in video, *f*=filename, *n*=native video player, *p*=write protection, *w*=watermark

§ Optional extra, not included in the system analysed in this research

⊗ not available

Licence plate data available in watermark (and always in configuration file if the watermark function is available).

Temporal data available in NMEA file, configuration files (time zone etc), EXIF data, file names, watermarks, and accessible through native video players (as well as other tools

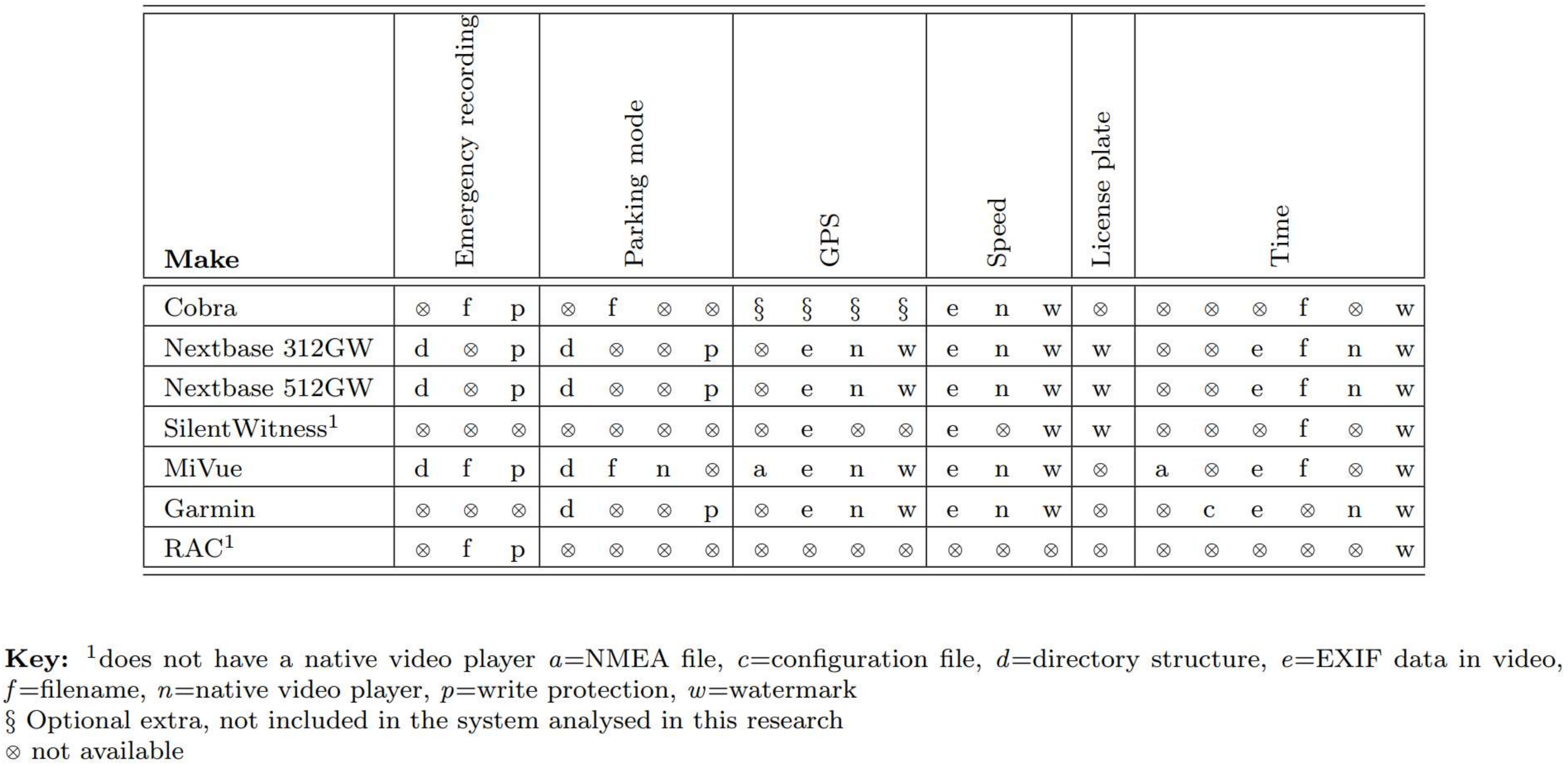


Make	Time					
Cobra	⊗	⊗	⊗	f	⊗	w
Nextbase 312GW	⊗	⊗	e	f	n	w
Nextbase 512GW	⊗	⊗	e	f	n	w
SilentWitness[1]	⊗	⊗	⊗	f	⊗	w
MiVue	a	⊗	e	f	⊗	w
Garmin	⊗	c	e	⊗	n	w
RAC[1]	⊗	⊗	⊗	⊗	⊗	w

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

⊗ not available

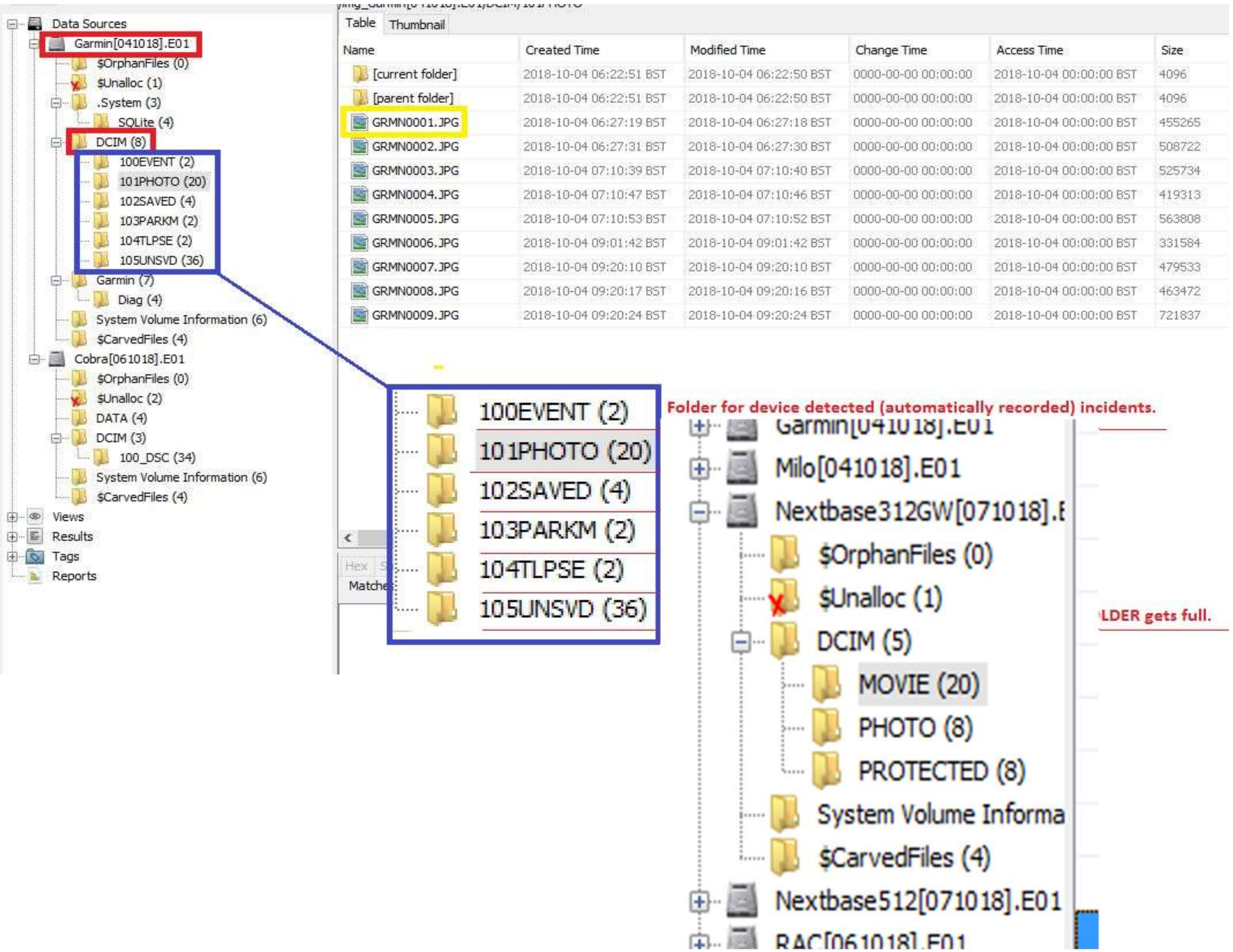


Make	Emergency recording			Parking mode				GPS				Speed			License plate	Time					
Cobra	⊗	f	p	⊗	f	⊗	⊗	§	§	§	§	e	n	w	⊗	⊗	⊗	⊗	f	⊗	w
Nextbase 312GW	d	⊗	p	d	⊗	⊗	p	⊗	e	n	w	e	n	w	w	⊗	⊗	e	f	n	w
Nextbase 512GW	d	⊗	p	d	⊗	⊗	p	⊗	e	n	w	e	n	w	w	⊗	⊗	e	f	n	w
SilentWitness[1]	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	e	⊗	⊗	e	⊗	w	w	⊗	⊗	⊗	f	⊗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

⊗ not available



Name	Created Time	Modified Time	Change Time	Access Time	Size
[current folder]	2018-10-04 06:22:51 BST	2018-10-04 06:22:50 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	4096
[parent folder]	2018-10-04 06:22:51 BST	2018-10-04 06:22:50 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	4096
GRMN0001.JPG	2018-10-04 06:27:19 BST	2018-10-04 06:27:18 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	455265
GRMN0002.JPG	2018-10-04 06:27:31 BST	2018-10-04 06:27:30 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	508722
GRMN0003.JPG	2018-10-04 07:10:39 BST	2018-10-04 07:10:40 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	525734
GRMN0004.JPG	2018-10-04 07:10:47 BST	2018-10-04 07:10:46 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	419313
GRMN0005.JPG	2018-10-04 07:10:53 BST	2018-10-04 07:10:52 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	563808
GRMN0006.JPG	2018-10-04 09:01:42 BST	2018-10-04 09:01:42 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	331584
GRMN0007.JPG	2018-10-04 09:20:10 BST	2018-10-04 09:20:10 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	479533
GRMN0008.JPG	2018-10-04 09:20:17 BST	2018-10-04 09:20:16 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	463472
GRMN0009.JPG	2018-10-04 09:20:24 BST	2018-10-04 09:20:24 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	721837

Folder for device detected (automatically recorded) incidents.

LDER gets full.

Investigation Model

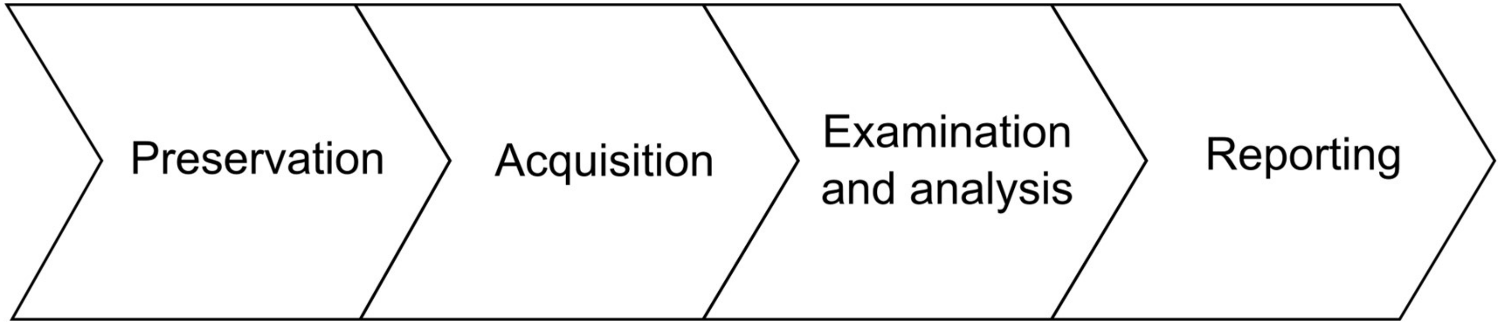
Digital forensic guidance model (Abdalla, 2007)
Smart grid digital forensics investigation framework (Abdullah, 2020)
Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, 2011)
Blockchain based Forensic Model in IoT (Agbedanu, 2023)
Enhanced Digital Forensic Investigative Model with CoC (Ajetunmobi, 2016)
Database Forensic Process Investigation Process Model (DBFIPM) (AlDhaqm, 2015)
Unified Forensic Investigation Model for UAV (AlDhaqm, 2021)
Flowthing model (AlFedaghi, 2012)
Drone Forensic Metamodel (DRFM) (Alhussan, 2022)
Drone Forensic Metamodel (DRFM) (Alhussan2022towards, 2022)
Metamodel for mobile forensics investigation (Ali, 2017)
Cloud-IoT Forensic Process Model (CFPM) (AlMolhis, 2022)
Comprehensive Collection and Analysis Forensic Model (CCAFM) (Alotaibi, 2022)
Forensic Investigation Model for Online Social Networks (Arshad, 2020)
Mobile forensic investigation process model (Asghari, 2021)
NIST Guidelines on Mobile Device Forensics (Ayers, 2007)
Enhanced digital investigation process model (EIDIP) (Baryamureeba, 2004)
Hierarchical Objectives-Based Framework for the Digital Investigations Process (Beebe, 2005)
Modified electronic discovery reference model (Billard, 2009)
Extended model for e-discovery operations (Billard2, 2009)
Crime scene analytical procedure model (Bulbul, 2013)
Integrated Digital Investigation Model (IDIP) (Carrier, 2003)
Digital Crime Scene Investigation Process (Carrier, 2005)
Investigative Process Model (Casey, 2005)
Inveatigative Proceas Model (Casey, 2010)
Generic Process model of network forensics (Chabbra, 2015)
Extended Model of Cybercrime Investigation (EMCI) (Ciardhuain, 2004)
Chain of Digital Evidence Based Model of Digital Forensic Investigation Process (Cosic, 2011)
Peritus framework (Cunha, 2020)
A Smart Technologies Digital Forensic Investigation Model (Cussack, 2014)
Platform Independent Forensics Process Model for forensics Process Model (PIFPM) (Dancer, 2013)
D4I Digital forensics framework for reviewing and investigating cyber-attacks (Dimitriadis, 2020)
Digital Forensic Investigation and Verification Model for Industrial Espionage (DEIV-IE) (Dokko, 2018)
SCADA Forensic Incident Response Model (Eden, 2015)
Ediscovery reference model (EDRMNET, 2009)
Abstract network forensic process model (Erbacher, 2006)
Smart Digital Forensic Readiness Model for Shadow IoT Devices (Fagbola, 2022)
digital Forensic Investigative Model For Business Organisations AKA Organisational Investigative Model (Forrester, 2007)
Common model (Freiling, 2007)
Smartphone Forensic Investigation Process Model (Goel, 2012)
UAV Digital Forensics Investigation Framework (Gulatacs, 2018)
Internet of Things Forensics Model (Hambouz, 2021)
An Improved Digital Evidence Acquisition Model for the Internet of Things (Harbawi, 2017)
The Lifecycle Model (Harrison, 2004)
Cloud Forensics Process (Hemdan, 2021)
Integrated Digital Forensics Investigation Framework v3 (Hikmatyar, 2017)
Digital Field Triage model (Hitchcock, 2016)
iPhone forensic framework (Iff) (Husain, 2010)
FORZA--Digital forensics investigation framework that incorporate legal issues (Ieong, 2006)
Android cache taxonomy and forensic process (Immanuel, 2015)
Digital Forensic Investigation for Internet of Things (Islam, 2019)
Forensic investigation framework for cloud-IoT ecosystem (Islam2019Comprehensive, 2019)
Harmonised Digital Forensic Investigation Process (ISO, 2015)
The TEAR evidence process (Kao, 2019)
Framework for enhancing potential digital evidence presentation (Karie, 2013)
Network Forensic System Architecture (Kaushik, 2015)
Cloud Forensic Readiness Model (Kebande, 2014)

Enhanced cloud forensic readiness model (ECFRM) (Kebande, 2015)
Digital Forensic Investigation Framework for Internet of Things(IoT) (Kebande, 2016)
Integrated Digital Forensic Investigation Framework (IDFIF-IoT)* (Kebande, 2018)
Log aggregation forensic analysis framework (Khan, 2017)
Two-Dimensional Evidence Reliability Amplification Process Model (Khatir, 2008)
Forensic investigation model for malware of IoT device (Kim2020S, 2020)
An improved IoT forensic model (Kim, 2023)
Digital Forensics Model (Kishore, 2014)
Integrated digital forensic process model (Kohn, 2013)
Enhanced Systematic Digital Forensic Investigation Model (ESDFIM) (Kyei, 2012)
Log file digital forensic model (Lalla, 2012)
Scientific Crime Scene Investigation process (Lee, 2001)
Thumbnail forensic recovery process for Android devices (Leom, 2015)
blockchain-based DF investigation framework in the Internet of Things (IoT) (Li, 2019)
Smart-Phone digital evidence forensics standard operating procedure (DEFSOP) (Lin, 2011)
Multi-disciplinary digital forensic investigation process model (Lutui, 2016)
Digital Forensics Model based on Data Fusion (Ma, 2011)
IR process model (Mandia, 2001)
An integrated conceptual digital forensic framework for cloud computing (Martini, 2012)
Conceptual Evidence Collection and Analysis Methodology for Android Devices (Martini, 2015)
Triage workflow (Marturana, 2011)
Incident response methodology model (Mitropoulos, 2006)
Standardised Digital Forensic Investigation Model* also referred to `Advanced Investigative Process Model' (Montasari, 2019)
Mobile Forensics Investigation Process Framework (MFIPF) (Moreb, 2023)
Cellular Phone Evidence Extraction Process (Murphy, 2008)
Behavioural Digital Forensics Model (Mutawa, 2019)
Proactive Smartphone Investigation Scheme (Mylonas, 2012)
Network Forensics Framework (Nasir, 2015)
Wireless forensic readiness model (WFRM) (Ngobeni, 2010)
PRoFIT (Privacy-aware IoT-Forensic Model) (Nieto, 2017)
Next-Best-Thing Triage (NBT) model (Oriwoh, 2013)
DFRWS Investigative Process for Digital Forensic Science (Palmer, 2001)
Network forensic investigation process model (Patil, 2022)
Internet Of Things(IoT) Digital Forensic Investigation Model (Perumal, 2015)
Generic framework for network forensic analysis (Pilli, 2010)
The ``three tiered model'' (Pollit, 1995)
Digital Forensics Investigation Model for IoT (DFIM) (Qatawneh, 2019)
Digital forensic multi-staged process (Raghavan, 2013)
Mobile Forensic Investigation (MFI) Life Cycle Process for Digital Data Discovery (DDD)* (Rajendran, 2016)
Windows Mobile Device Forensic Model (Ramabhadran, 2007)
Proactive Network Forensics Evidence Analysis (PNFEA) (Rasmi, 2015)
Abstract Digital Forensics model (Reith, 2002)
Unmanned Aerial Vehicle Forensic Investigation Process (Roder, 2018)
Multi-perspective cybercrime investigation process model (Roger, 2012)
Cyber Forensic Field Triage Process Model (CFFTPM) (Rogers, 2006)
Online social network forensic model (Rua, 2019)
Integrated Digital Forensics Investigation Framework (Ruuhwan, 2017)
Blockchain-based decentralized efficient investigation framework for IoT digital forensics (Ryu, 2019)
Unified mobile devices forensics investigation model (Sadiq, 2016)
Extended Abstract Digital Forensic Model with 2PasU (Saleem, 2014)
Common Investigation Process Model For The Internet Of Things Forensics Field (Saleh, 2021)
Domain specific cyber forensic investigation process model (DSCFIPM) (Satti, 2015)
Digital Forensic Investigation Framework (DFIF) (Selamat, 2008)
Digital forensic investigation framework for the metaverse (Seo, 2023)
New digital forensics investigation procedure model (Shin, 2008)
New model for cyber crime investigation procedure (Shin, 2011)

Encapsulated Approach of Forensic (EAF) (Shrivastava, 2014)
Secured Proactive Network Forensic Framework (Sivaprasad, 2017)
Digital Forensic Methodology (Smith2, 2007)
Framework for digital forensic investigation of big data (Song, 2020)
End-to-End Digital investigation Process (Stephenson, 2003)
Conceptual Drone Forensics Framework (CDFF) (Studiawan, 2023)
Application-Specific Internet of Things (IoT) Digital Forensics Investigative Model (Tanveer, 2017)
Next Generation Digital Forensic Investigation Model (NGDFIM) (Thakar, 2021)
Systematic Network Forensic Investigation model (SNFIM) (Thomas, 2023)
Harmonised Digital Forensic Investigation Process (Valjarevic, 2012)
Comprehensive and Harmonized Digital Forensic Investigation Process Model (Valjarevic, 2015)
comprehensive harmonized digital forensic investigation process model (Valjarevic, 2016)
A Model for Hybrid Evidence Investigation (Vlachopoulos, 2012)
Control framework for digital forensics (VonSolms, 2006)
General Collection Methodology for Android Devices (Votipka, 2013)
Symbian Smartphones Forensic Process Model (Yu, 2009)
Generic Computer Forensic Investigation Model (GCFIM) (Yusoff, 2011)
digital forensic investigation for Online Social Networking (Zainudin, 2010)
Blockchain based forensic model (Zarpala, 2021)
Forensics aware IoT Model (Zawoad, 2015)
Open cloud forensics model (Zawoad2, 2015)
Application-Specific Digital Forensics Investigative Model in Internet of Things (Zia, 2017)

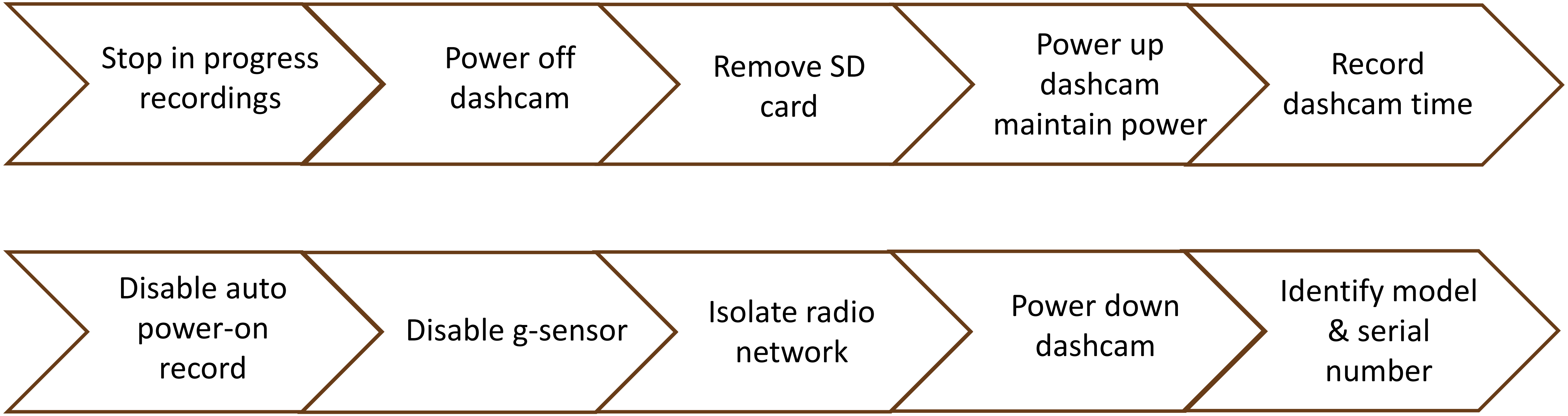
Too many models?

Overarching Digital Forensic Investigation Model



Ayers, R., Brothers, S., Wayne, J., 2014. Guidelines on cell phone forensics (NIST Special Publication 800-101)

Preservation



Stop in progress recordings

Power off dashcam

Remove SD card

Power up dashcam maintain power

Record dashcam time

Disable auto power-on record

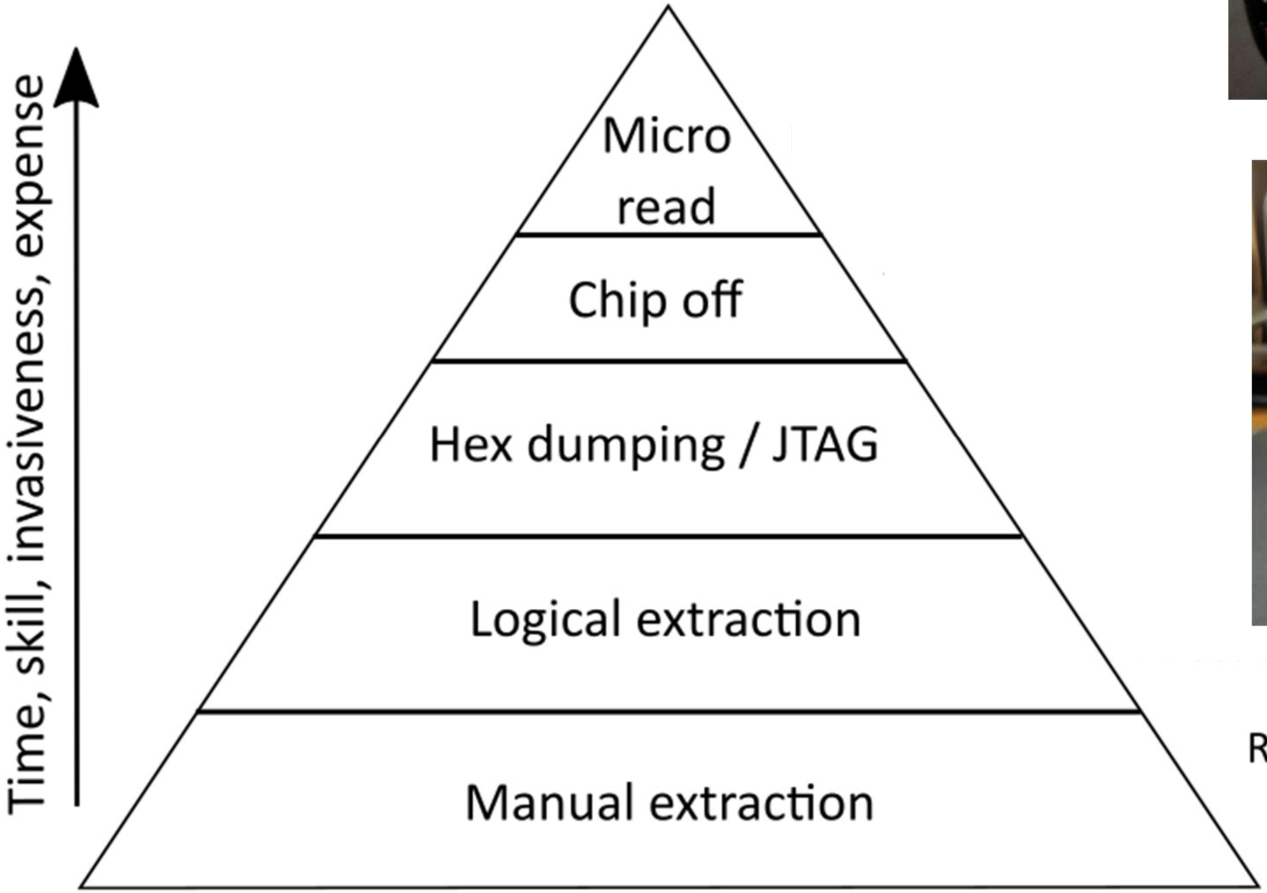
Disable g-sensor

Isolate radio network

Power down dashcam

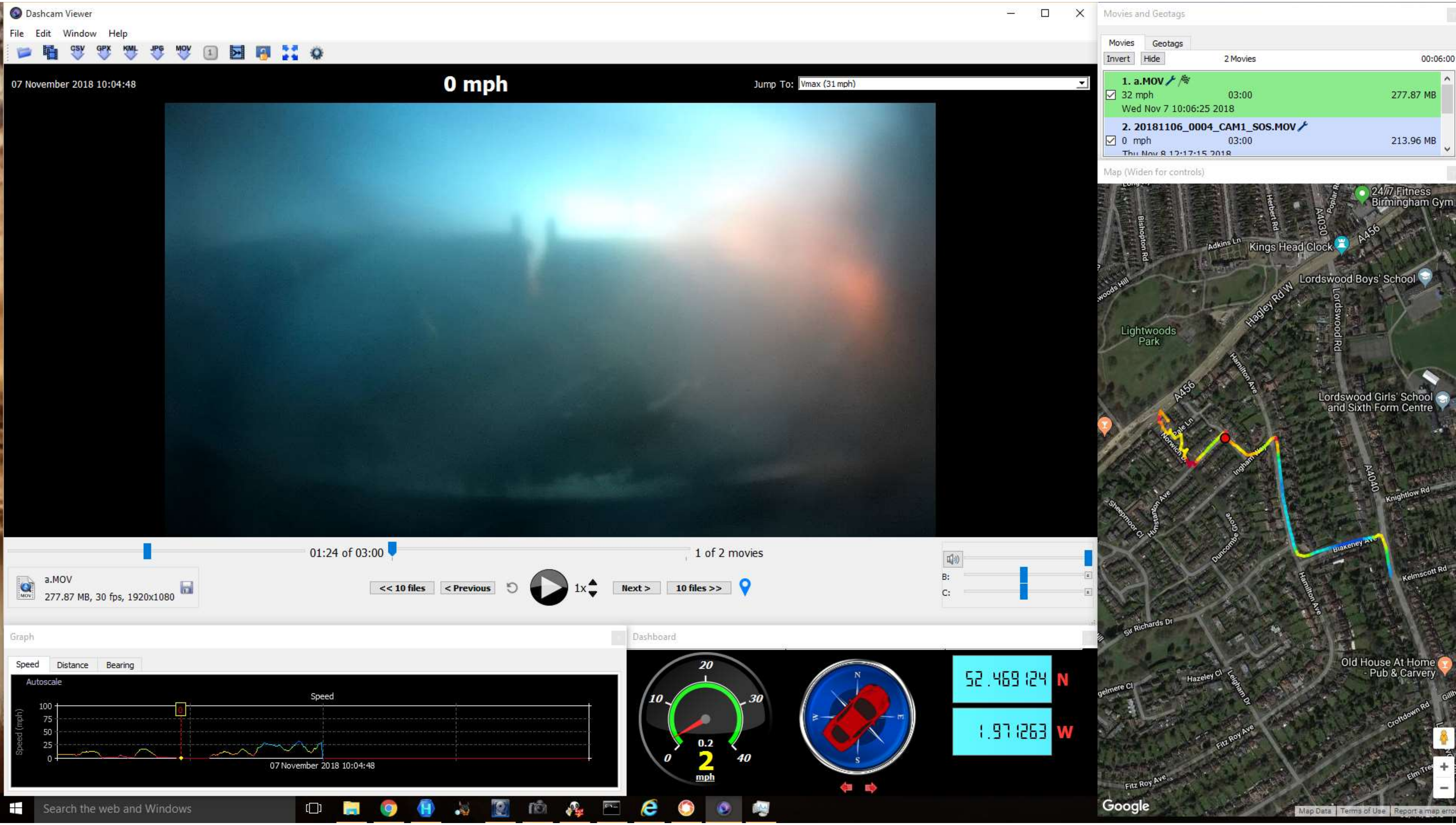
Identify model & serial number

Acquisition



Remove SD, take config photos

Examination and Analysis



07 November 2018 10:04:48

0 mph

Jump To: Vmax (31 mph)

2 Movies 00:06:00

☑ 1. a.MOV	32 mph	03:00	277.87 MB
	Wed Nov 7 10:06:25 2018		
☑ 2. 20181106_0004_CAM1_SOS.MOV	0 mph	03:00	213.96 MB
	Thu Nov 8 12:17:15 2018		

01:24 of 03:00

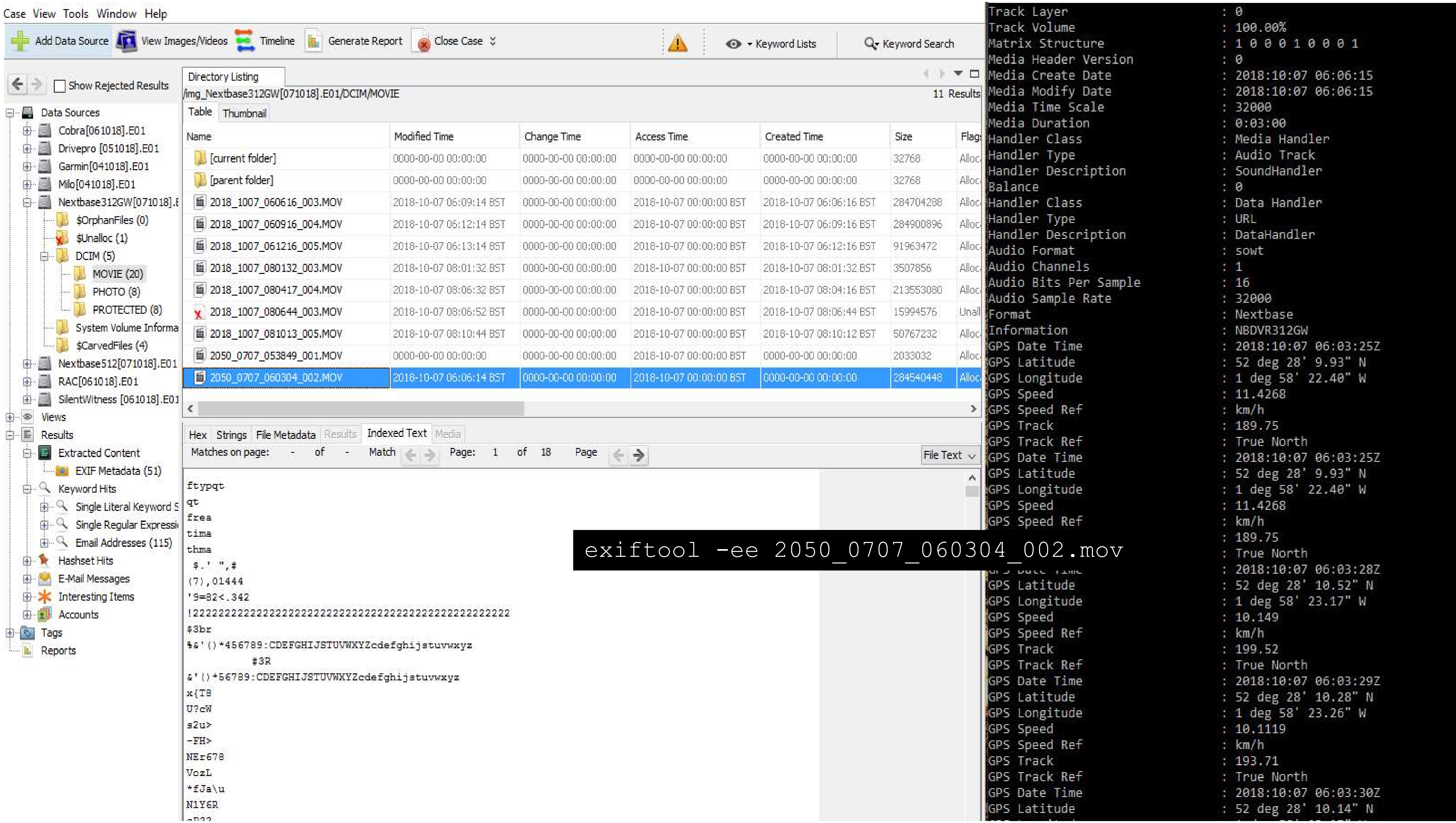
1 of 2 movies

a.MOV
277.87 MB, 30 fps, 1920x1080

07 November 2018 10:04:48

52.469124 N

1.971263 W



/img_Nextbase312GW[071018].E01/DCIM/MOVIE 11 Results

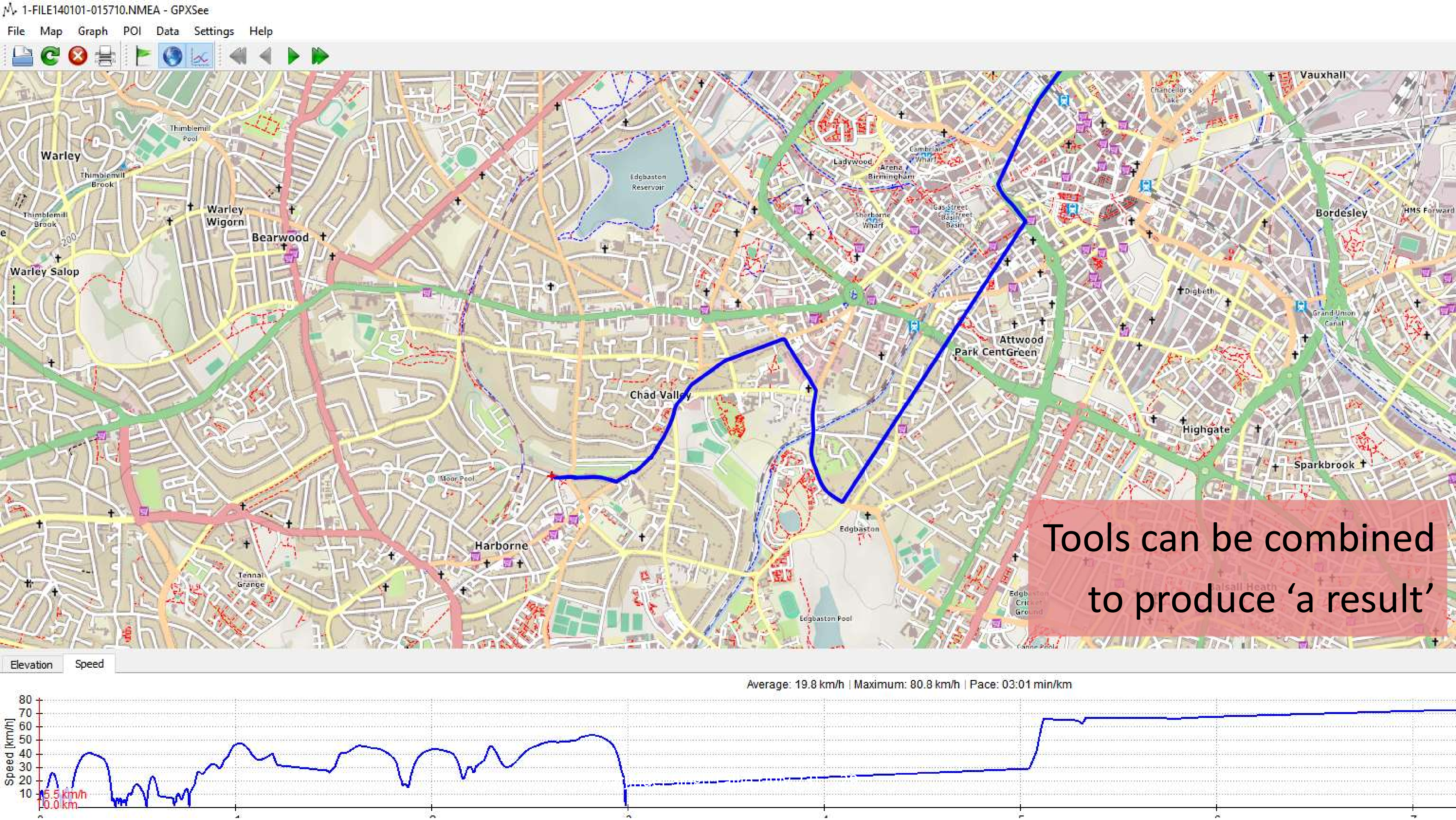
Name	Modified Time	Change Time	Access Time	Created Time	Size	Flag:
[current folder]	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32768	Alloc
[parent folder]	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32768	Alloc
2018_1007_060616_003.MOV	2018-10-07 06:09:14 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 06:06:16 BST	284704288	Alloc
2018_1007_060916_004.MOV	2018-10-07 06:12:14 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 06:09:16 BST	284900896	Alloc
2018_1007_061216_005.MOV	2018-10-07 06:13:14 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 06:12:16 BST	91963472	Alloc
2018_1007_080132_003.MOV	2018-10-07 08:01:32 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 08:01:32 BST	3507856	Alloc
2018_1007_080417_004.MOV	2018-10-07 08:06:32 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 08:04:16 BST	213553080	Alloc
2018_1007_080644_003.MOV	2018-10-07 08:06:52 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 08:06:44 BST	15994576	Unall
2018_1007_081013_005.MOV	2018-10-07 08:10:44 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	2018-10-07 08:10:12 BST	50767232	Alloc
2050_0707_053849_001.MOV	0000-00-00 00:00:00	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	0000-00-00 00:00:00	2033032	Alloc
2050_0707_060304_002.MOV	2018-10-07 06:06:14 BST	0000-00-00 00:00:00	2018-10-07 00:00:00 BST	0000-00-00 00:00:00	284540448	Alloc

Matches on page: - of - Match Page: 1 of 18 Page

```
ftypqt
qt
frea
tima
thma
 $.' ",#
(7),01444
'9=82<.342
!222222222222222222222222222222222222222222222222222
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
           #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
x{T8
U?cW
s2u>
-FH>
NEr678
VozL
*fJa\u
N1Y6R
```

```
exiftool -ee 2050_0707_060304_002.mov
```

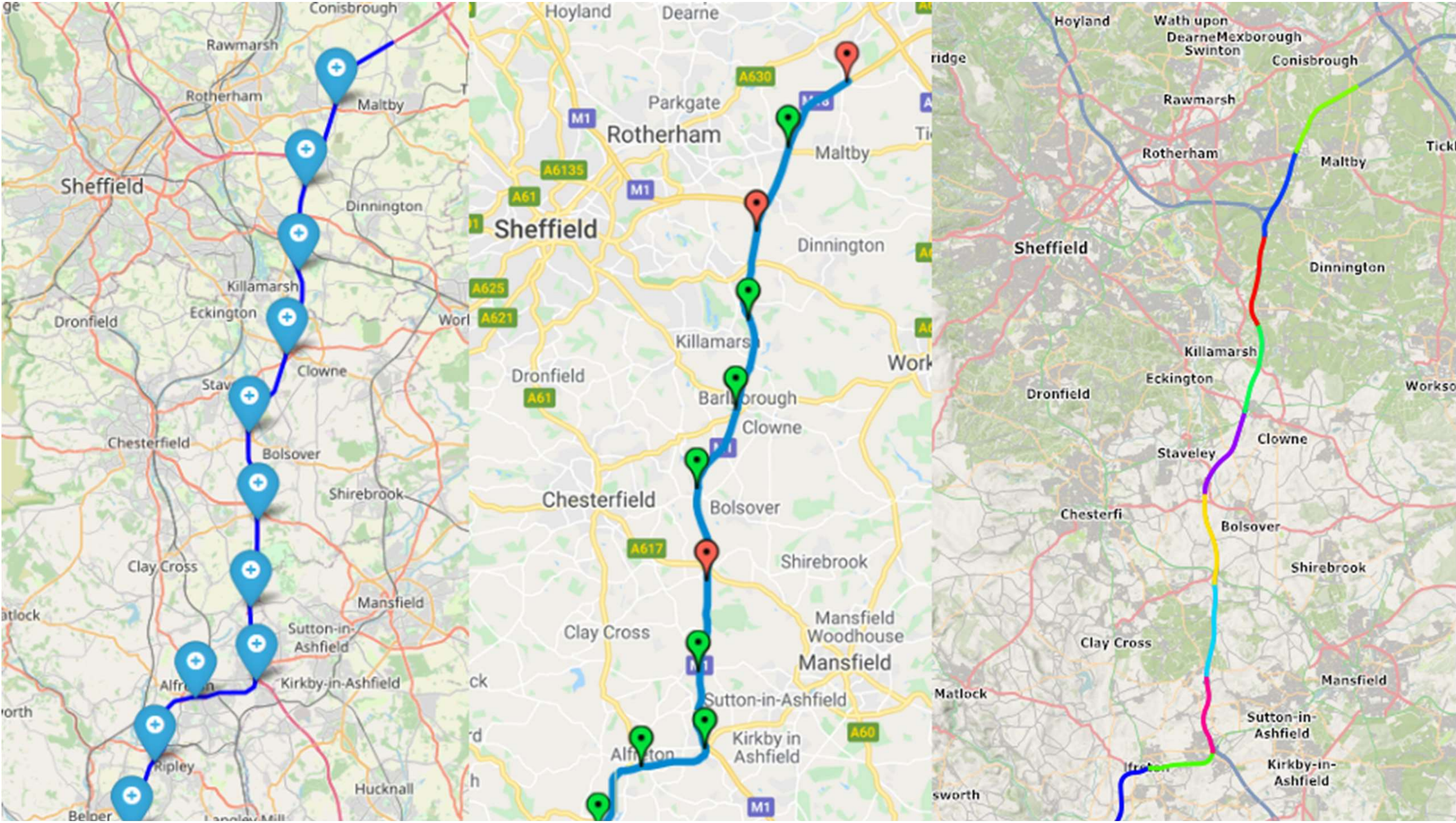
```
Track Layer                     : 0
Track Volume                    : 100.00%
Matrix Structure                : 1 0 0 0 1 0 0 0 1
Media Header Version            : 0
Media Create Date               : 2018:10:07 06:06:15
Media Modify Date               : 2018:10:07 06:06:15
Media Time Scale                : 32000
Media Duration                  : 0:03:00
Handler Class                   : Media Handler
Handler Type                    : Audio Track
Handler Description             : SoundHandler
Balance                         : 0
Handler Class                   : Data Handler
Handler Type                    : URL
Handler Description             : DataHandler
Audio Format                    : sowt
Audio Channels                  : 1
Audio Bits Per Sample           : 16
Audio Sample Rate               : 32000
Format                          : Nextbase
Information                     : NBDVR312GW
GPS Date Time                   : 2018:10:07 06:03:25Z
GPS Latitude                    : 52 deg 28' 9.93" N
GPS Longitude                   : 1 deg 58' 22.40" W
GPS Speed                       : 11.4268
GPS Speed Ref                   : km/h
GPS Track                       : 189.75
GPS Track Ref                   : True North
GPS Date Time                   : 2018:10:07 06:03:25Z
GPS Latitude                    : 52 deg 28' 9.93" N
GPS Longitude                   : 1 deg 58' 22.40" W
GPS Speed                       : 11.4268
GPS Speed Ref                   : km/h
                                : 189.75
                                : True North
                                : 2018:10:07 06:03:28Z
GPS Latitude                    : 52 deg 28' 10.52" N
GPS Longitude                   : 1 deg 58' 23.17" W
GPS Speed                       : 10.149
GPS Speed Ref                   : km/h
GPS Track                       : 199.52
GPS Track Ref                   : True North
GPS Date Time                   : 2018:10:07 06:03:29Z
GPS Latitude                    : 52 deg 28' 10.28" N
GPS Longitude                   : 1 deg 58' 23.26" W
GPS Speed                       : 10.1119
GPS Speed Ref                   : km/h
GPS Track                       : 193.71
GPS Track Ref                   : True North
GPS Date Time                   : 2018:10:07 06:03:30Z
GPS Latitude                    : 52 deg 28' 10.14" N
```



1-FILE140101-015710.NMEA - GPXSee

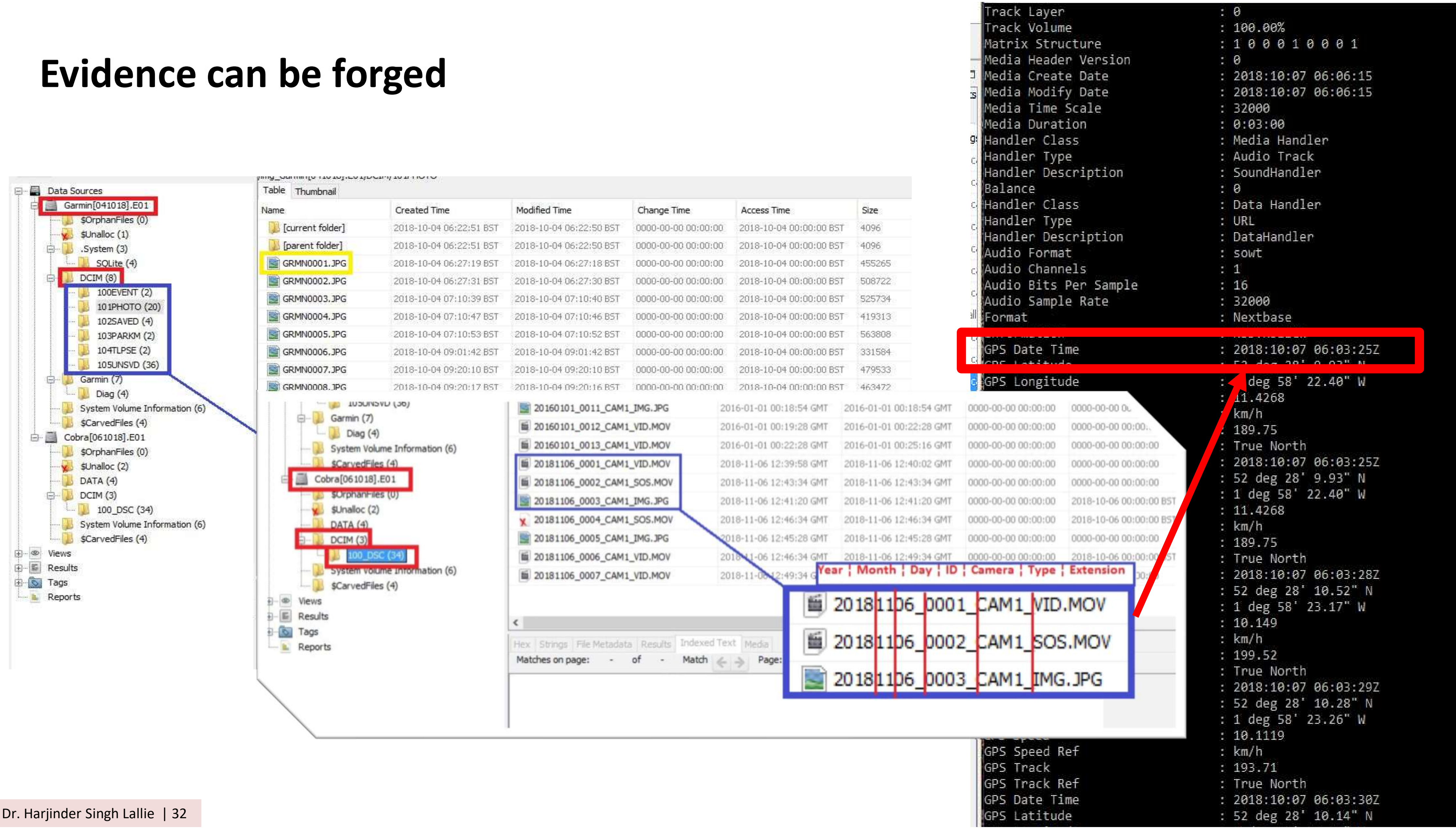
Average: 19.8 km/h | Maximum: 80.8 km/h | Pace: 03:01 min/km

Tools can be combined to produce ‘a result’


Conisbrough
Rawmarsh
Rotherham
Maltby
Sheffield
Dinnington
Killamarsh
Eckington
Dronfield
Clowne
Worl
Stav
Chesterfield
Bolsover
Shirebrook
Clay Cross
Mansfield
atlock
Sutton-in-Ashfield
Kirkby-in-Ashfield
Alfreton
orth
Ripley
Hucknall
Belper
Langley Mill
Hoyland
Dearne
A630
Parkgate
M1
Rotherham
Maltby
A6135
A61
Sheffield
Dinnington
A625
A621
Killamarsh
Work
Dronfield
A61
Barlborough
Clowne
M1
Chesterfield
Bolsover
A617
Shirebrook
Clay Cross
Mansfield Woodhouse
Mansfield
M1
Sutton-in-Ashfield
Kirkby in Ashfield
A60
Alfreton
M1
Hoyland
Wath upon Dearne
Mexborough
Swinton
ridge
Conisbrough
Rawmarsh
Rotherham
Maltby
Tick
Sheffield
Dinnington
Killamarsh
Eckington
Dronfield
Workso
Clowne
Staveley
Chesterfi
Bolsover
Shirebrook
Clay Cross
Mansfield
Matlock
Sutton-in-Ashfield
Kirkby-in-Ashfield
lfreton
sworth

Can the evidence be forged?

Evidence can be forged



```
Data Sources
  Garmin[041018].E01
    $OrphanFiles (0)
    $Unalloc (1)
    .System (3)
      SQLite (4)
    DCIM (8)
      100EVENT (2)
      101PHOTO (20)
      102SAVED (4)
      103PARKM (2)
      104TLPSE (2)
      105UNSVD (36)
    Garmin (7)
      Diag (4)
    System Volume Information (6)
    $CarvedFiles (4)
  Cobra[061018].E01
    $OrphanFiles (0)
    $Unalloc (2)
    DATA (4)
    DCIM (3)
      100_DSC (34)
    System Volume Information (6)
    $CarvedFiles (4)
Views
Results
Tags
Reports
```

Table | Thumbnail

Name	Created Time	Modified Time	Change Time	Access Time	Size
[current folder]	2018-10-04 06:22:51 BST	2018-10-04 06:22:50 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	4096
[parent folder]	2018-10-04 06:22:51 BST	2018-10-04 06:22:50 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	4096
GRMN0001.JPG	2018-10-04 06:27:19 BST	2018-10-04 06:27:18 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	455265
GRMN0002.JPG	2018-10-04 06:27:31 BST	2018-10-04 06:27:30 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	508722
GRMN0003.JPG	2018-10-04 07:10:39 BST	2018-10-04 07:10:40 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	525734
GRMN0004.JPG	2018-10-04 07:10:47 BST	2018-10-04 07:10:46 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	419313
GRMN0005.JPG	2018-10-04 07:10:53 BST	2018-10-04 07:10:52 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	563808
GRMN0006.JPG	2018-10-04 09:01:42 BST	2018-10-04 09:01:42 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	331584
GRMN0007.JPG	2018-10-04 09:20:10 BST	2018-10-04 09:20:10 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	479533
GRMN0008.JPG	2018-10-04 09:20:17 BST	2018-10-04 09:20:16 BST	0000-00-00 00:00:00	2018-10-04 00:00:00 BST	463472

```
      105UNSVD (36)
    Garmin (7)
      Diag (4)
    System Volume Information (6)
    $CarvedFiles (4)
  Cobra[061018].E01
    $OrphanFiles (0)
    $Unalloc (2)
    DATA (4)
    DCIM (3)
      100_DSC (34)
    System Volume Information (6)
    $CarvedFiles (4)
Views
Results
Tags
Reports
```

20160101_0011_CAM1_IMG.JPG	2016-01-01 00:18:54 GMT	2016-01-01 00:18:54 GMT	0000-00-00 00:00:00	0000-00-00 0(
20160101_0012_CAM1_VID.MOV	2016-01-01 00:19:28 GMT	2016-01-01 00:22:28 GMT	0000-00-00 00:00:00	0000-00-00 00:00:
20160101_0013_CAM1_VID.MOV	2016-01-01 00:22:28 GMT	2016-01-01 00:25:16 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00
20181106_0001_CAM1_VID.MOV	2018-11-06 12:39:58 GMT	2018-11-06 12:40:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00
20181106_0002_CAM1_SOS.MOV	2018-11-06 12:43:34 GMT	2018-11-06 12:43:34 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00
20181106_0003_CAM1_IMG.JPG	2018-11-06 12:41:20 GMT	2018-11-06 12:41:20 GMT	0000-00-00 00:00:00	2018-10-06 00:00:00 BST
20181106_0004_CAM1_SOS.MOV	2018-11-06 12:46:34 GMT	2018-11-06 12:46:34 GMT	0000-00-00 00:00:00	2018-10-06 00:00:00 BST
20181106_0005_CAM1_IMG.JPG	2018-11-06 12:45:28 GMT	2018-11-06 12:45:28 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00
20181106_0006_CAM1_VID.MOV	2018-11-06 12:46:34 GMT	2018-11-06 12:49:34 GMT	0000-00-00 00:00:00	2018-10-06 00:00:00 BST
20181106_0007_CAM1_VID.MOV	2018-11-06 12:49:34 GMT			

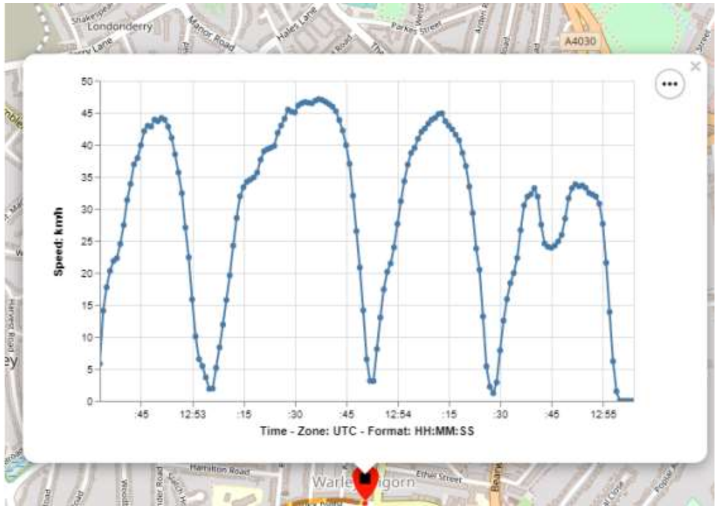
Year	Month	Day	ID	Camera	Type	Extension
2018	11	06	0001	CAM1	VID	.MOV
2018	11	06	0002	CAM1	SOS	.MOV
2018	11	06	0003	CAM1	IMG	.JPG

```
Track Layer                     : 0
Track Volume                    : 100.00%
Matrix Structure                : 1 0 0 0 1 0 0 0 1
Media Header Version            : 0
Media Create Date               : 2018:10:07 06:06:15
Media Modify Date               : 2018:10:07 06:06:15
Media Time Scale                : 32000
Media Duration                  : 0:03:00
Handler Class                   : Media Handler
Handler Type                    : Audio Track
Handler Description             : SoundHandler
Balance                         : 0
Handler Class                   : Data Handler
Handler Type                    : URL
Handler Description             : DataHandler
Audio Format                    : sowt
Audio Channels                  : 1
Audio Bits Per Sample           : 16
Audio Sample Rate               : 32000
Format                          : Nextbase
GPS Date Time                   : 2018:10:07 06:03:25Z
GPS Longitude                   : 1 deg 58' 22.40" W
                                : 11.4268
                                : km/h
                                : 189.75
                                : True North
                                : 2018:10:07 06:03:25Z
                                : 52 deg 28' 9.93" N
                                : 1 deg 58' 22.40" W
                                : 11.4268
                                : km/h
                                : 189.75
                                : True North
                                : 2018:10:07 06:03:28Z
                                : 52 deg 28' 10.52" N
                                : 1 deg 58' 23.17" W
                                : 10.149
                                : km/h
                                : 199.52
                                : True North
                                : 2018:10:07 06:03:29Z
                                : 52 deg 28' 10.28" N
                                : 1 deg 58' 23.26" W
                                : 10.1119
GPS Speed Ref                   : km/h
GPS Track                       : 193.71
GPS Track Ref                   : True North
GPS Date Time                   : 2018:10:07 06:03:30Z
GPS Latitude                    : 52 deg 28' 10.14" N
```

Research Directions

Challenges

- There are no tools
- Some (watermark) evidence can be forged
- 3rd party open source tools (Exiftools) will extract data but it has to be pre-processed. GPS data recorded every 1/10s = 1800 records for a 3 minute clip, 36,000 for each image
- Evidence exists in multiple places in multiple formats



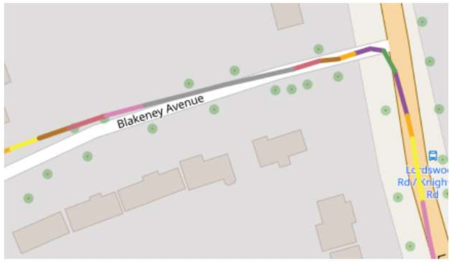
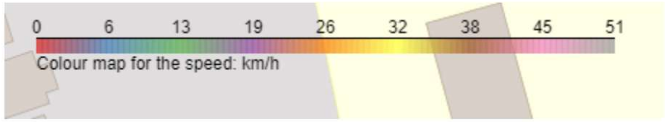


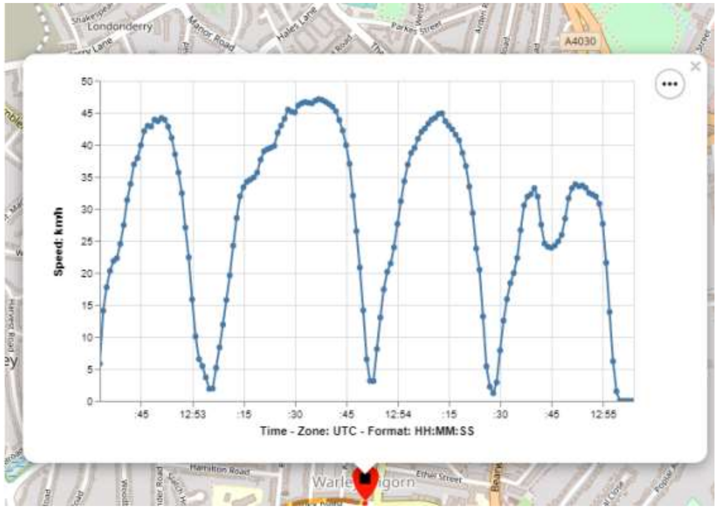
Figure 24, showing a route line with the colours representing speed



Challenges

We now have working tools which can read .E01 and automate the process of data extraction and map generation

- There are no tools
- Some (watermark) evidence can be forged
- 3rd party open source tools (Exiftools) will extract data but it has to be pre-processed. GPS data recorded every 1/10s = 1800 records for a 3 minute clip, 36,000 for each image
- Evidence exists in multiple places in multiple formats



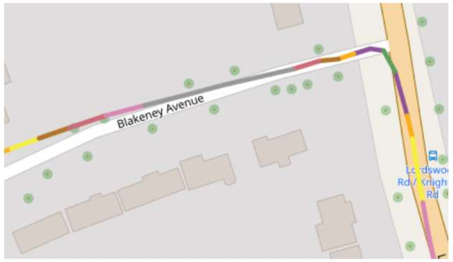
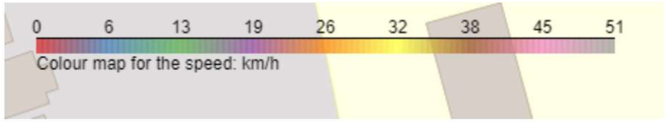


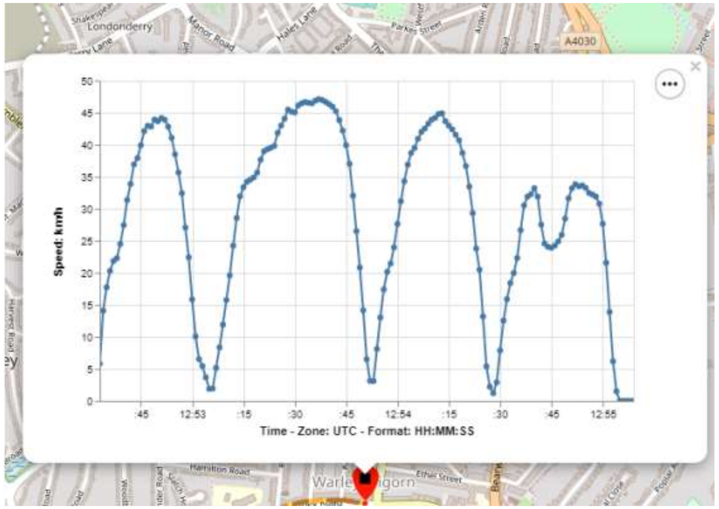
Figure 24, showing a route line with the colours representing speed



Challenges

- There are no tools
- Some (watermark) evidence can be forged
- 3rd party open source tools (Exiftools) will extract data but it has to be pre-processed. GPS data recorded every 1/10 = 1800 records for a 3 minute clip, 36,000 for each image
- Evidence exists in multiple places in multiple formats

We are working on an audio keywork searching tool



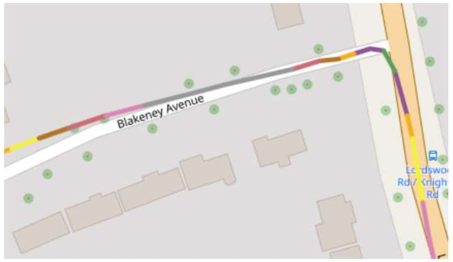
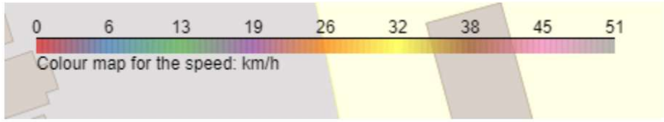


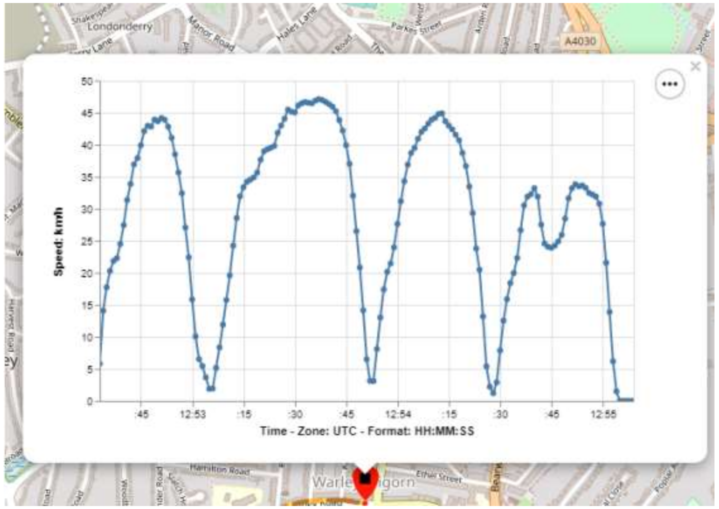
Figure 24, showing a route line with the colours representing speed



Challenges

- There are no tools
- Some (watermark) evidence can be forged
- 3rd party open source tools (Exiftools) will extract data but it has to be pre-processed. GPS data recorded every 1/10s = 1800 records for a 3 minute clip, 36,000 for each image
- Evidence exists in multiple places in multiple formats

We are working on a geospatial triaging tool



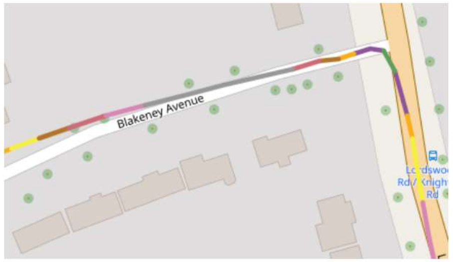
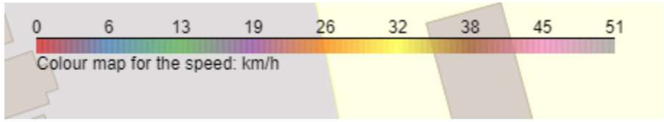


Figure 24, showing a route line with the colours representing speed



Dashcam Forensics

Dr. Harjinder Singh Lallie
Associate Professor
University of Warwick
HL@warwick.ac.uk

Thank you

RATE MY PROFESSORS LinkedIn facebook