Investigating Evidence of Mobile Phone Usage by Drivers in Road Traffic Accidents

By

Graeme Horsman and Lynne Conniss

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2015 EU

Dublin, Ireland (Mar 23rd- 26th)

Digital Investigation 12 (2015) S30–S37

Contents lists available at ScienceDirect

Digital Investigation

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

Investigating evidence of mobile phone usage by drivers in road traffic accidents

Graeme Horsman*, Lynne R. Conniss

Northumbria University, Newcastle-upon-Tyne NE1 8ST, UK

Keywords:
Digital forensics
Road Traffic Act 1988
Investigation
Mobile phone forensics
Direct activity
Passive activity
Interactive communication

A B S T R A C T

The United Kingdom is witnessing some of the highest volumes of motor vehicle traffic on its roads. In addition, a large number of motor vehicle traffic accidents are reported annually, of which it is estimated that a quarter involve the illegal use of a hand-held mobile device by the driver. Establishing whether mobile phone usage was a causal factor for an accident involves carrying out a forensic analysis of a mobile handset to ascertain a timeline of activity on the device, focussing on whether the handset was used immediately prior to, or during, an incident. Previously, this involved identifying whether SMS messages have been sent or received on the handset alongside an examination of the call logs. However, with advancements in smartphone and application design, there are now a number of ways a driver can interact with their mobile device resulting in less obvious forms of evidence which can be termed as 'passive activity'. This article provides an analysis of iPhone's `CurrentPowerlog.powerlogsystem` file and Android device 'buffer logs', along with their associated residual data, both of which can potentially be used to establish mobile phone usage at the time of, or leading up to, a motor vehicle accident.

Introduction

Within the United Kingdom (UK) in 2013, 183,670 road traffic casualties were reported, 8% of which were children, whilst approximately 2% of crashes resulted in fatalities (Department of Transport, 2014). Further, trends highlighted by the World Health Organisation (2011) suggest road traffic injuries will rise to constitute the fifth largest global cause of death by 2030. In light of these statistics, with around 35 million licensed vehicles in operation on UK roads (Department of Transport, 2013), there seems to be an increasing need for investigation into causal factors that put drivers at risk of road traffic accidents.

It is vital to consider all possible factors when assessing events leading up to and during motor vehicle incidents, in order to establish the nature and order of events and importantly, whether a particular party is at fault. Although statistics identifying specific use of mobile phones during road traffic accidents in the UK is sparse, it is estimated that in the United States, drivers were using mobile phones in almost a quarter of all reported incidents (Pless and Pless, 2014; National Safety Council, 2014; Northern Ireland Statistics and Research Agency, 2013). These figures prove concerning, since the ability of a driver to operate their vehicle proficiently is significantly decreased whilst using a mobile device, thereby increasing the chances of an incident or accident occurring on the road (Horberry et al., 2006). Further, the driver's attention is diverted from the main goal of ensuring their safety and that of others through effective driving, towards a secondary activity, termed as 'driver distraction' (Hosking et al., 2009).

* Corresponding author.
E-mail address: g.horsman@northumbria.ac.uk (G. Horsman).

http://dx.doi.org/10.1016/j.diin.2015.01.008

Issues facing a driver arising from mobile device usage include, but are not limited to, the following:

- Restriction of sight; limiting the driver's ability to survey the road, potential obstacles or changes in traffic flow, since their line of vision is focused on the handset (Nasar and Troyer, 2013).
- Reduction of concentration levels and situational awareness (Nasar and Troyer, 2013).
- Slower reactions times during adverse events (The Royal Society for the Prevention of Accidents, 2012), which could result in as much as a 50% reduction in response rates (Think!, 2014).
- Failure to maintain a high standard of driving etiquette, resulting in acts such as tailgating or improper road position (The Royal Society for the Prevention of Accidents, 2012).

RAC (2014) surveys indicate that 75% of motorists have observed other drivers talking on their mobile phones whilst driving, however, only 8% admit to doing so themselves. In turn, surveys undertaken outside of the UK (yet still in jurisdictions where mobile phone usage when driving is illegal) by White et al. (2010) indicate that over 60% of participants professed to interacting with their mobile phone whilst driving without the use of a hands-free kit. Similarly, there are a growing number of younger drivers with an increased dependency on mobile devices resulting in them frequently being used whilst driving to access social media (Weller et al., 2013).

Due to the size of these devices it is likely that many cases remain unreported due to successful concealment of usage of the device whilst driving. The challenge surrounding mobile phone-related vehicle accident investigations lies with proving a device was used leading up to or during an accident, thereby ultimately becoming a causal factor and an element with which to potentially help establish blame. To achieve this requires the forensic analysis of the mobile handset and its residual data.

This article provides an analysis of UK law governing mobile phone usage whilst driving, followed by the discussion of the role of a mobile phone forensic analyst in road traffic accident investigations. An examination of iPhone's `CurrentPowerlog.powerlog` system file and Android device buffer logs will be presented and their relevance for detecting user activity on mobile handsets outlined.

UK law and mobile phone forensics

Since December 2003, the act of using a hand-held mobile device whilst driving has been prohibited within the UK. Amendments to the Road Vehicles (Construction and Use) Regulations 1986 (RVR86) via the Road Vehicles (Construction and Use) (Amendment) (No. 4) Regulations 2003 have now introduced the following regulation under 110(1) RVR86:

> "*No person shall drive a motor vehicle on a road if he is using (a) a hand-held mobile telephone*"

It is important to note that interaction with a mobile device via a hands-free device is legal provided its usage could be proven. Further, government guidance states that hands-free phones, two-way radios and satellite navigation devices can be legally used whilst driving, but if police believe the driver is being distracted and failing to sufficiently control their vehicle, prosecution may still occur (Gov.uk, 2014). Justice Lloyd Jones in *R v Curtis* (Regina v Phillipa Curtis [2009] EWCA Crim 1003) stated that driving requires 100% of the driver's concentration, and in the recent case of *R v Jaswinder Arora* (*Regina v Jaswinder Arora* [2014] EWCA Crim 104), it was highlighted that even drivers using hands-free kits are still up to four times more likely to be distracted and cause an accident. In addition, RVR86 regulation 110(6) (a) defines a device as being hand-held given the following:

> "*A mobile telephone or other device is to be treated as hand-held if it is, or must be, held at some point during the course of making or receiving a call or performing any other interactive communication function*".

On initial inspection, the term '*interactive communication function*' appears ambiguous given the array of features and functionalities of the modern mobile device/smart phone and associated applications. Therefore, it is useful to explore what this means in more depth.

What constitutes 'interactive communication function'?

RVR86 regulation 110(6)(c) provides guidance for identifying features and functionalities that may be involved:

> ""*Interactive communication function" includes the following*:
>
> *(i) Sending or receiving oral or written messages;*
>
> *(ii) Sending or receiving facsimile documents;*
>
> *(iii) Sending or receiving still or moving images; and*
>
> *(iv) Providing access to the internet.*"

Upon interpretation of RVR86 regulation 110(6)(c), and particularly the wide scope of regulation 110(6)(c)(iv), it would appear that almost all interaction with the device whilst driving is prohibited. Given that most smart phones now maintain fairly constant communication with data networks in order to update applications automatically (unless disabled by the user), even the act of waking a handset from a sleep state to view push notification alerts on the handset's display (see Section 'Interacting with the screen lock' below) could be deemed an interactive communication function. However, proving that these subtle interactions have taken place on the device whilst driving may be difficult.

Categorisation of offences

The offence of using a mobile device whilst driving also overlaps with offences of greater severity laid out in the Road Traffic Act 1988, notably the offence of causing death by dangerous driving under Section 1 and causing death by

careless or inconsiderate driving, under Section 2B. To be guilty of the offences, the behaviour of the driver is judged against that of 'the careful and competent' driver, a hypothetical representation of what would be required to ensure safe conduct. Research has frequently highlighted the dangers caused by mobile phone distraction but unlike those under RVR86 regulation 110(6)(c), where specific acts of interactive communication must be proven, for a prosecution under Sections 1 and 2B of the Road Traffic Act 1988, any trace of mobile phone usage or handling by a driver in a serious road traffic accident may suffice.

Mobile phone forensics

Various solutions have been proposed as methods of deterrence and prevention (Artan et al., 2014; Yang et al., 2011); yet, standard UK motor vehicles contain no standard or additional features for regulating the use of mobile phones whilst driving. As a result, law enforcement officials in the UK will seize all mobile devices from the scene of serious traffic accidents as standard protocol (Association of Chief Police Officers, 2014). At this point, a mobile phone forensic practitioner is tasked with establishing usage patterns and providing information identifying whether a driver has potentially interacted with the device prior to or during the motor accident. To achieve this requires establishing the timeframe of the accident and events immediately beforehand, to allow correlation with device timestamps and usage. The former can be done through the utilisation of multiple sources such as witness statements, police records, emergency service call logs and CCTV recordings (Redelmeier and Tibshirani, 1997).

The field of mobile forensics has developed significantly over the last 10 years and now, various extraction methods such as logical, physical, J-Tagging or chip-off extractions, allow practitioners to gain access to a large quantity of residual data on the handset, both live and deleted, including protected operating system files. At the close of an investigation, practitioners can frequently establish the following types of evidence, which may indicate, prohibited usage of a mobile phone whilst driving:

- SMS messages, received, sent, drafts: both live and deleted;
- Make/receive calls, including live and deleted call records;
- Access to social media applications for the purpose of communication (e.g. Facebook, Snapchat, Twitter etc.);
- Sending and receiving emails, Internet browsing.

These types of 'direct activity' involve interaction with the operating system of the device, executing events that leave behind clear physical traces that the user has interacted with their handset. A typical and obvious example of direct activity would be when a user sends a message from their device, leaving a record in their sent box, including an associated timestamp. However, it is possible for a user to operate their mobile phone and leave behind less obvious traces of their actions through what this article coins 'passive activity', which may still contravene UK driving legislation.

Passive activity on a mobile phone

It has been established that all forms of interaction with a mobile handset by a driver whilst driving, could lead to prosecution. Whilst the use of interactive communication functions on mobile devices results in direct and traceable interactions with system files and application data, other forms of handset use may result in little residual data or change to system files and as such, these types of activity may be defined as being 'passive'.

Passive activities, such as viewing the contents of the SMS inbox, without disturbing the status of any unread messages, are generally harder to detect yet may provide sufficient distraction for a driver to cause a serious road traffic incident, but then go unpunished if evidence of the activity can't be sufficiently established.

Whilst driving, any interaction on a mobile device with an application that provides access to the Internet is prohibited. Many social media and news applications would fall into this category. For example, Twitter may be configured to automatically update content via available network connections. The passive act of scrolling through and viewing a Twitter feed whilst driving would breach the aforementioned legislation, yet determining when this application was accessed, how frequently and how long the driver potentially spent viewing it, in the run up to an accident, may prove difficult. Oulasvirta et al. (2012) indicate that some of the most frequently carried out tasks on a device include checking social media updates and reading news or articles. Such activities are often part of habitual and autonomous actions, triggered when the user is bored, killing time or subject to lapses in concentration (Oulasvirta et al., 2012). These are all actions, which may remain undetected during analysis of the device as practitioners may look for more obvious traces of user interaction involving communication.

The consequences of failing to detect passive activity on the handset may lead to a failure to prosecute drivers for mobile phone-related offences. Therefore the following sections below will now provide the findings of an investigation into the discovery of evidence highlighting user interaction for a given time frame on iPhone and Android devices, such as may be required for the purposes of road traffic accident investigation. The devices were chosen based on the dominant shares of the mobile phone market both handset types maintain (Statista, 2014).

Analysis of an iPhone

This investigation will focus on the iPhone's `CurrentPowerlog.powerlog` system file and the `PLArchive` directory, both located at `/var/mobile/Library/Logs/` and accessed via a physical extraction of the handset. The test device was an iPhone 4 running iOS version 7 which was analysed using Microsystemation's XRY to acquire a physical extraction of the handset.

CurrentPowerlog.powerlog

The `CurrentPowerlog.powerlog` is a system file consisting of records denoting system events on the

handset. Each record entry is prefixed with an attribute tag, indicating the type of activity that has been carried out on the handset, thus prompting a log entry. The relevance of this file in road traffic accident investigations is that almost all user interaction with the handset is recorded within it including passive activity; with entries ranging from when the user has pressed the power button and unlocked the handset, to the execution and closure of applications on the handset. Records within the `CurrentPowerlog.powerlog` allow a mobile forensic practitioner to profile an iPhone's usage by its owner. Each `CurrentPowerlog.powerlog` file records activity for a 24-h period on the device (as specified in the `[Log]` entry at the start of every file; see Fig. 1). This enables a practitioner to profile the device's usage throughout this period, and thus, by selecting the relevant `CurrentPowerlog.powerlog` file, the period leading up to a motor vehicle accident.

As the file continuously records device activity throughout the defined [`Log`] period, the file can be in excess of 5 MB, subject to the amount of activity on the handset. Once the file has reached its defined [`rolloverDate`], the file is not deleted but moved to the `/var/mobile/Library/Logs/PLArchive` directory and placed within a `.gz` archive, prefixed with the starting date of the log (e.g. `PL_2014-08-04-`). This means that handset activity from previous days can also be access and examined.

However, the `PLArchive` directory does not indefinitely maintain all `CurrentPowerlog.powerlog` files from the first time the handsets was used, and although it cannot be confirmed in all models of iPhone handsets and iOS versions, logs on the test iPhone were maintained for at least 3 weeks. Therefore, investigating practitioners must ensure that the device is interrogated as soon after the road traffic incident as possible to prevent the handset overwriting these files. Of course, it may be possible that, if a handset was jailbroken, users could download or write scripts or applications which could delete or tamper with some or all `CurrentPowerlog.powerlog` files leaving little or no trace evidence.

Providing the `CurrentPowerlog.powerlog` files are retrieved from a suspect handset, the following sections provide an indication of the relevance of data they may contain.

Hands-free connectivity

As noted previously, hands-free mobile handset usage is permitted whilst driving, however, the presence of a hands-free kit within a motor vehicle does not indicate that it was in operation during or leading up to an accident meaning it must be proven that any such calls were received legally via the hands-free device at the time in question. For the purposes of detecting hand-free usage, a series of calls were made to the iPhone test device and answered using the device handset. A further set of calls were made and instead answered using a 'Plantronics M20' Bluetooth hands-free headset. After analysing `[Telephony]` log entries in the `CurrentPowerlog.powerlog`, calls answered through the Bluetooth headset maintain an additional `[Audio]` entry (see Fig. 2.), denoting audio for the call being routed via the Bluetooth headset as opposed to the handset speaker. Although only one hands-free device was tested, given that these devices route audio to the Bluetooth headset, it is presumed similar log entries would be available for other manufacturers. This distinction between methods of answering calls is not shown in standard mobile handset call logs where the handset speaker is employed, therefore an analysis of the `CurrentPowerlog.powerlog` could identify if an actual hand-free device was in use at the time of the accident.

```
07/28/14 00:00:47.281 [Log] state=roll;
existingLogdate=07/27/14 14:13:16.000;
periodStart=07/28/14 00:00:00.000;
rolloverDate=07/29/14 00:00:00.000;
```

Fig. 1. Log timespan entry.

```
09/03/14 13:46:21.744 [Telephony]…
call_status=Active;
09/03/14 13:46:21.801 [Audio]
active=YES; route=HeadsetBT;
09/03/14 13:46:32.350
[Telephony]…call_status=Inactive
```

Fig. 2. Log entries for a call routed through a Bluetooth headset.

Charging the device in-car

The use of in-car charging facilities has now increased to cope with demand and the widespread use of mobile phones. In turn, the act of plugging in the mobile handset into these devices whilst driving may provide sufficient distraction from the road. The `CurrentPowerlog.powerlog` provides the following entries for when the device is connected to a charger and when it's not, shown in Fig. 3.

Profiling the `[Battery]` log entries can indicate the time a device was connected to an in-car charging facility.

Interacting with the screen lock

The lock-screen of an iPhone handset is displayed to the user when the power button is pressed following sleep mode (see Fig. 4). Typical information displayed includes time, date and any notifications from applications on the handset (received SMS, social media posts, emails etc.). The iPhone offers the ability to preview messages in the notification screen without directly accessing them. From the perspective of a forensic analysis of a handset, previewing these messages on the lock-screen does not alter the

```
07/28/14 19:17:17.273 [Battery]
level=97.14%; … charging_state=Active;
07/28/14 22:00:17.406 [Battery]
level=75.04%; …
charging_state=Inactive;
```

Fig. 3. Log entries for device charging.

Fig. 4. Example of notification screen content.

```
07/28/14 18:11:31.601 [Display]
  active=yes; brightness=50.0%;
07/28/14 18:11:36.611 [Display]
  active=no; brightness=0.0%;
```

Fig. 5. Log entries for power button presses.

timestamp of data stored within the application (for example, previewing a received SMS message still leaves the message marked as unread on the handset). The implication of this is that it may not be obvious that the user has illegally interacted with their handset at the time of the accident and in turn, a user could argue the fact that the message remains in an unread state indicating that they have not actually read it.

However, the `CurrentPowerlog.powerlog` records shown in Fig. 5 indicate when the user has pressed the power button, initialising the lock-screen display.

In addition, the lock state of the phone is also recorded (see Fig. 6.), indicating whether the user has proceeded to unlock their device.

A combination of the `[SpringBoard-states]` and `[Display]` entries document whether the user has simply looked at their phone (for the time, notifications etc.) or entered the device by unlocking it for further interaction with handset features and applications. Profiling the entire log for entries can lead to the identification of subsets of time throughout a 24-h period in question where the device is being actively used. In turn, the timestamp information could correlate to relevant times prior to, or during an accident. Using the previous example of a received message, correlating lock-screen log entries with inbox message timestamps could indicate that the user has actually used their handset prior to or during an accident to unlock their device and proceed to read a message.

```
07/28/14 18:11:31.630 [SpringBoard-
  states] screen_state=unblanked;
      lock_state=locked;
07/28/14 18:16:24.585 [SpringBoard-
  states] screen_state=unblanked;
      lock_state=unlocked;
```

Fig. 6. Log entries for screen lock status.

Use of applications

Once the user has accessed the device, it is likely that they will proceed to initiate applications that are installed on the handset. The `CurrentPowerlog.powerlog` records all access to applications installed on the device using the `[Application]` tag (see Fig. 7). The following example provides a record entry for the user initiating the Facebook application on their device.

Key data contained in the `[Application]` entry include '`executable=`' which indicates the name of the application which has been executed. This corresponds to the name shown under the application's icon on the main screen of the handset. In addition, the '`mode=`' syntax provides an indication of the application's current running state. Modes include '`Foreground Running`', '`Background Running`', '`Terminated`' and '`Suspended`'. Given that entries in the `CurrentPowerlog.powerlog` are timestamped, it is possible to profile application usage on the handset to see when they are executed, and, in turn, closed by the user. The difference in time between entries gives an indication of the duration that the application was in use (see Fig. 8 for example of log content). These log entries can indicate when the user initiates, for example, a social media or news application solely for browsing purposes, and, for how long; a passive act which could be overlooked during a mobile forensic investigation yet is prohibited whilst driving.

Establishing a device has been inactive

The `CurrentPowerlog.powerlog` retains information about interactions with the device, and as may be expected, the number of monitored events reduces when the device is in sleep mode or during periods of inactivity (although battery and network connectivity may be recorded whilst the device is in sleep mode). In addition, when the handset is powered off, all logging activity ceases.

```
07/28/14 18:23:06.453 [Application]
id=com.apple.mobilephone; pid=486.00;
      mode=Foreground Running;
        reason=<unknown>;
UIBackgroundModes=audio,continuous;
        display_name=Phone;
  executable=Facebook; version=36;
```

Fig. 7. Log entries for the 'Phone' application state.

Therefore, the practitioner can also identify periods where the device was inactive through an analysis of the entry timestamps, which may prove crucial for refuting claims that a driver has interacted with their handset.

Analysis of the Android operating system

Handsets using Android operating systems present a different challenge to the practitioner. Unlike the iPhone device, there is no equivalent `CurrentPowerlog.powerlog` file stored within the file system monitoring daily activity. The challenge of identifying direct and passive activity requires an analysis of volatile system buffer logs stored under the file location `/dev/log`. However due to their volatility, a live analysis of the device is required at the scene of the accident or shortly after, in order to access buffer log content within data retention restrictions; analogous to physical memory in computer devices, when power is removed from the mobile handset, buffer log content is purged. For this investigation, the extraction from the Android handsets was via the Android Debug Bridge (ADB) which will be discussed below.

Buffer logs

For the purpose of application development and debugging, the buffer logs maintain records of system messages on the handset, similar to that of the iPhone's *CurrentPowerlog.powerlog*. As a result, log content denotes system messages generated by the user as they interact with their device and buffer logs are constantly in operation whilst the handset is powered on. It should also be noted that there are multiple buffer logs in action on the handset, which can all be extracted as shown in Table 1.

Each log contains a series of entries signifying specific events on the handset, which can be distinguished via their process ID (see Section 'Analysis of buffer log content' below). As with the *CurrentPowerlog.powerlog*, log entries include when the user accessed their handset including the opening and closure of applications,

```
07/28/14 18:00:07.913 [SpringBoard-screens] Screens=3;
07/28/14 18:00:10.817 [WiFi Notifications] SB-SpringBoard=NO;
07/28/14 18:00:10.831 [SpringBoard-screens] Screens=homescreer
07/28/14 18:00:10.829 [Application] id=com.facebook.Facebook;
display_name=Facebook; executable=Facebook; version=12.1;
07/28/14 18:00:10.975 [Application] id=uk.co.bbc.newsuk; pid=4
07/28/14 18:00:15.466 [SpringBoard-screens] Screens=3;
07/28/14 18:00:15.500 [Battery] level=66.27%; voltage=4027 mV;
adapter_info=16384; connected_status=1;
07/28/14 18:00:21.150 [SpringBoard-screens] Screens=3;
07/28/14 18:00:21.174 [SpringBoard-screens] Screens=3;
07/28/14 18:00:21.183 [Assertion] state=created; pid=33; id=1c
Type=NoIdleSleepAssertion; TrueType=PreventUserIdleSystemSleep
07/28/14 18:00:21.189 [Assertion] state=released; pid=33; id=1
07/28/14 18:00:21.158 [Application] id=uk.co.bbc.newsuk; pid=4
07/28/14 18:00:21.375 [Application] id=uk.co.bbc.newsuk; pid=4
07/28/14 18:00:21.428 [Application] id=de.andi.syslogman; pid=
07/28/14 18:00:21.429 [Application] id=de.andi.syslogman; pid=
07/28/14 18:00:22.548 [Assertion] state=released; pid=33; id=1
07/28/14 18:00:22.526 [Application] id=com.facebook.Facebook;
executable=Facebook; version=12.1;
```

Fig. 8. Example of CurrentPowerlog.powerlog content.

Table 1
Types of buffer log (Developers, 2014a).

Type	Main buffer log
System	System messages for debugging
Main	Main log buffer by default
Events	System events-related messages
Radio	Radio/telephony-related messages

complete with any intervening timestamp information denoting when an application event has occurred.

However, a restriction of the buffer logs is that they maintain a finite size, and once filled, previous content is overwritten. The volatility of the buffer logs poses the greatest challenge to the mobile forensic practitioner, and, as a consequence, if more activity is carried out on the handset there is a greater chance of activity in the log being overwritten. In addition, if the handset encounters heavy activity in a short space of time, the log will contain records of the user's actions over a shorter time period due to size restrictions (see further discussion in Section 'Buffer size considerations').

Accessing/dev/log/

The volatility of buffer logs means that in order to capture the maximum available information, the handsets seized at the scene of a motor accident must be examined immediately. The device's current charge capacity must also be assessed and if necessary, connected to an auxiliary power supply to prevent data loss. The Association of Chief of Police (ACPO) guidelines for mobile phone seizure recommend either turning the device off to prevent changes to resident data or placing the device within a shield environment (Association of Chief Police Officers, 2007). In the case of the former, buffer log data will be lost. In the latter, the mobile forensic practitioner must also consider the difficulties posed by Faraday technology, which causes handsets to lose their charge at a faster rate and auxiliary power may be needed.

The */dev/log* file location must be accessed through the Android Debug Bridge (ADB), a command line application for communicating with an Android device (Developers, 2014b). The necessary drivers for the specific make and model of handset being investigated must be installed on the host computer being used for the access in order to support communication with that particular Android device. As part of the ADB, the *logcat* command can be used to read the log messages currently stored in the handset buffer and export their contents to a text file (see Fig. 10).

Buffer size considerations

To determine buffer size, the '`logcat -g`' command should be run (see Fig. 9). The larger the buffer, the more information it is likely to retain. In addition, it is likely that this information covers a larger timescale, increasing the chance of retrieving information denoting handset usage at the time of the motor vehicle accident. Testing showed that buffer log information from a Galaxy S3 running Jellybean

```
Adblogcat-b events -g

/dev/log/events: ring buffer is 256kb
(255kb consumed), max entry is 5120b,
max payload is 4076b
```

Fig. 9. ADB command to establish the size of the events buffer log.

4.3 held log information for events from 6 h prior to the point of extraction. In comparison, an HTC One handset running Kit Kat 4.4 held log information for events from 2 h prior to the point of extraction, demonstrating the impact buffer log size can have on an investigation. Although buffer sizes can be increased, it is unlikely that the average user will have done so, therefore all buffer sizes referred to in this article have been left as the handset default.

Table 2 documents the results of an examination of a sample set of Android operating systems to show the difference in default buffer log sizes.

Analysis of buffer log content

Results provided in this section are the result of an analysis of an HTC One handset running Kit Kat 4.4.

Log entries within the buffer logs contain a number of metadata fields which should be extracted for examination. For the purposes of maximum data acquisition, Fig. 10 denotes the use of the '`long`' command, accessing all available fields for log messages in the events buffer, exporting data to a text file for subsequent analysis.

As buffer logs record all actions on the handset, it is likely that a number of entries will be redundant for the purpose of profiling a device's usage; filtering the log content via Process ID (PID) entry information can allow relevant events to be identified. Table 3 provides an overview of some of the basic PIDs associated with initiating the handset and the actions of opening and closing and applications.

To provide an example of buffer log content in context, the act of viewing SMS messages in the inbox of the handset was carried out (all messages had previously been read). Afterwards, handset buffer logs were extracted and analysed, providing evidence of the SMS application being executed, followed by the thread for the 'Vodafone' contact being opened to view the SMS messages.

Table 2
Default buffer log size variations by operating systems.

OS version	Log size
4.4 (Kit Kat)	All logs 256 kb
4.3 (Jelly Bean)	Main (2048 kb), system & events (256 kb), radio (1024 kb)
2.3 (Gingerbread)	All logs 64 kb; except events log (256 kb)

```
Adblogcat -b events -v long >
output.txt
```

Fig. 10. ADB command to extract log content with all metadata fields.

Table 3
PID entries and description.

PID	Description
`screen_toggled(752):0`	Handset sleeping.
`screen_toggled(752):1`	Handset active but locked.
`screen_toggled(1065):2`	Handset unlocked.
`am_proc_start`	Indicates application has been executed.
`am_destroy_service`	Indicates application has been closed.
`Am_on_resume_called`	Indicates application previously running in the background has been executed.

The information shown in Fig. 11 is not available in a physical or logical extraction of the handset. Despite these actions clearly documenting device usage, which may impact upon prosecution of mobile device-related driver offences, a failure to collect buffer log data would leave these actions of a driver undetected.

A further example includes the use of social media applications, for example, the user who synchronises their Twitter feed whilst driving and proceeds to read tweets, an act breaching legislation. A practitioner viewing the extracted buffer needs first to find the PID for the Twitter application execution (prefixed `am_proc_start`). As the buffer logs are chronological, the proceeding log entries, notably PID '`sync:[com.twitter …`' will indicate that the user has synchronised their feed. Immediately preceding this entry, '`ScribeService`' entries are generated when the user scrolls through their Twitter feed (see Fig. 12).

```
Am_on_resume_called…
[0,com,htc,sense,mms,ui,ConversationLis
t] …
Notification_cancel[com,htc,sense,mms,0
,Vodafone]
```

Fig. 11. PID information for opening the SMS application and looking at the Vodafone contact SMS thread.

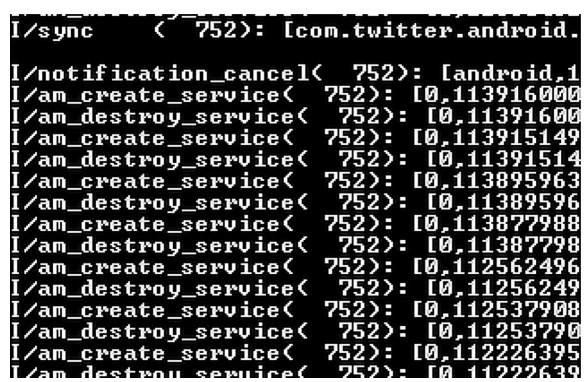

Fig. 12. Twitter newsfeed sync and scroll.

Hands-free device usage

As with the iPhone, it is necessary to establish whether a handset was accessed through a hands-free headset. The tests documented in Section 'Hands-free connectivity' for the iPhone, were replicated on the test Android device. Extraction and analysis of the '`events`' buffer showed no distinction between a call answered on the handset and one answered via a hands-free headset. However, an extraction and analysis of the '`main`' buffer log indicated the use of the Bluetooth headset to answer the call. However, the relevance of this information is limited. Due to the volume of events recorded in the '`main`' buffer, events only had a timespan of 4 min. Therefore, given the time it would take to respond to a motor incident and extract data from the handset, log information would be overwritten. Therefore, unlike the iPhone, information denoting hands-free usage, tracing similar usage on an Android device is too volatile and would likely not be available to mobile forensic practitioners.

Conclusion

One of the key difficulties in a road traffic investigation involves establishing a timeline of events along with causal factors for the road traffic accident. UK legislation effectively prohibits all drivers from using hand-held mobile devices whilst operating a motor vehicle. After a motor vehicle incident, mobile phone forensic practitioners are tasked with establishing whether a driver has broken the law by looking for signs of mobile device activity leading up to or during an accident, typically consisting of an analysis of call and text message records as a minimum.

This article has presented an analysis of the iPhone's `CurrentPowerlog.powerlog` and Android's buffer logs, highlighting the types of information relating to user-interaction on the handset, which are stored in these areas and can be retrieved for the purposes of identifying potential causal factors. Activity recorded in these areas could highlight a driver's direct or passive activity on their handset, which, in turn may provide an explanation for events leading up to a motor vehicle accident. Alternatively, analysis of these log files may indicate that a driver did not use their mobile device prior to, or during a road traffic incident.

The analysis of mobile handsets in relation to road traffic accident investigations leads to a number of areas which require further investigation, particularly as technology continues to evolve. Accident investigators will need to factor in peripheral or integrated technology. For example, on-board car computers/management systems with Bluetooth integration (e.g. Ford SYNC) will need to be analysed in order to identify whether a driver's interaction with the device was truly hands-free at the time of an incident. Similarly, voice-activated applications used to access and interact with handset functionality (e.g. send SMS, make calls etc.) in a hands-free capacity will also need to be factored into road traffic accident investigations. As a result, establishing a robust account of how such technologies work will be a key area for future research and development.

References

Artan Y, Bulan O, Loce R, Paul P. Driver cell phone usage detection from HOV/HOT NIR images. In: Proceedings of the IEEE conference on computer vision and pattern recognition workshops; 2014. p. 225–30.

Association of Chief Police Officers. Good practice guide for computer-based electronic evidence. 2007. p. 46 [Online] Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

Association of Chief Police Officers. Reports of police seizing mobile phones after every road traffic collision are inaccurate [Online]. Available at: http://www.acpo.presscentre.com/Press-Releases/Reports-of-police-seizing-mobile-phones-after-every-road-traffic-collision-are-inaccurate-2e8.aspx; 2014.

Department of Transport. Vehicle licensing statistics: 2013 [Online]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302409/vls-2013.pdf; 2013.

Department of Transport. Reported road casualties in Great Britain: main results 2013 [Online]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/324580/rrcgb-main-results-2013.pdf; 2014.

Developers. Reading and writing logs [Online]. Available at: http://developer.android.com/tools/debugging/debugging-log.html; 2014.

Developers. Android debug bridge [Online]. Available at: http://developer.android.com/tools/help/adb.html; 2014.

Govuk. Using mobile phones when driving: the law [Online]. Available at: https://www.gov.uk/using-mobile-phones-when-driving-the-law; 2014.

Horberry T, Anderson J, Regan MA, Triggs TJ, Brown J. Driver distraction: the effects of concurrent in-vehicle tasks, road environment complexity and age on driving performance. Accid Anal Prev 2006;38(1):185–91.

Hosking SG, Young KL, Regan MA. The effects of text messaging on young drivers. Hum Factors J Hum Factors Ergon Soc 2009;51(4):582–92.

Nasar JL, Troyer D. Pedestrian injuries due to mobile phone use in public places. Accid Anal Prev 2013;57:91–5.

National Safety Council. NSC releases latest injury and fatality statistics and trends [Online]. Available at: http://www.nsc.org/Pages/NSC-releases-latest-injury-and-fatality-statistics-and-trends-.aspx; 2014.

Northern Ireland Statistics and Research Agency. Northern Ireland road safety monitor [Online]. Available at: http://www.doeni.gov.uk/road-safety-monitor-2013-report.pdf; 2013.

Oulasvirta A, Rattenbury T, Ma L, Raita E. Habits make smartphone use more pervasive. Pers Ubiquitous Comput 2012;16(1):105–14.

Pless C, Pless B. Mobile phones and driving. BMJ Br Med J 2014;348.

RAC. RAC report on motoring 2014. 2014 [Online]. Available at: http://www.rac.co.uk/RAC/files/eb/eb140396-0385-49db-a9e7-3a5b02dd28fd.pdf.

Redelmeier DA, Tibshirani RJ. Association between cellular-telephone calls and motor vehicle collisions. N Engl J Med 1997;336(7):453–8.

Regina v Jaswinder Arora [2014] EWCA Crim 104.

Regina v Phillipa Curtis [2009] EWCA Crim 1003.

Statista. Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 4th quarter 2013 [Online]. Available at: http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/; 2014.

The road vehicles (construction and use) regulations 1986. Available at: http://www.legislation.gov.uk/uksi/1986/1078/contents/made.

The road vehicles (construction and use) (amendment) (no. 4) regulations 2003. Available at: http://www.legislation.gov.uk/uksi/2003/2695/made.

The Royal Society for the Prevention of Accidents. Road safety information [Online]. Available at: http://www.rospa.com/roadsafety/info/mobile_phones_2011.pdf; 2012.

Think!. Mobile phones [Online]. Available at: http://think.direct.gov.uk/mobile-phones.html; 2014.

Weller JA, Shackleford C, Dieckmann N, Slovic P. Possession attachment predicts cell phone use while driving. Health Psychol 2013;32(4):379.

White KM, Hyde MK, Walsh SP, Watson B. Mobile phone use while driving: an investigation of the beliefs influencing drivers' hands-free and hand-held mobile phone use. Transp Res Part F Traffic Psychol Behav 2010;13(1):9–20.

World Health Organisation. Mobile phone use: a growing problem of driver distraction [Online]. Available at: http://www.who.int/violence_injury_prevention/publications/road_traffic/distracted_driving_en.pdf?ua=1; 2011.

Yang J, Sidhom S, Chandrasekaran G, Vu T, Liu H, Cecan N, et al. Detecting driver phone use leveraging car speakers. In: Proceedings of the 17th annual international conference on mobile computing and networking; 2011. p. 97–108.