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

By

Graeme Horsman and Lynne Conniss

Presented At

The Digital Forensic Research Conference

DFRWS 2015 EU Dublin, Ireland (Mar 23rd- 26th)

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

Dr. Graeme Horsman
Lynne Conniss
Northumbria University
g.horsman@northumbria.ac.uk

Background

- Recent UK government surveys estimate around 1.6% of drivers in England and Scotland use a hand-held mobile phone whilst driving [1].
  - Number of cars licensed for use on the road in UK – 35million [2].
  - Van drivers identified most often.
  - 17-29 key age group.

- Department of Transport states road deaths have increased by 1% in 2014 to 1730 [3].
- 192,910 road casualties reported for year ending September 2014 [3].

Sources:
1. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/406723/seatbelt-and-mobile-use-surveys-2014.pdf
2. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302409/vls-2013.pdf
3. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401295/quarterly-estimates-jul-to-sep-2014.pdf

Background

- Why is mobile phone usage a problem…'**driver distraction**'.

- 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.
- Reduction of concentration levels and situational awareness.
- Slower reactions times during adverse events which could result in as much as a 50% reduction in response rates.
- Failure to maintain a high standard of driving etiquette, resulting in acts such as tailgating or improper road position.

The Law

- Since 2003, the use of a hand-held mobile device whilst driving is prohibited.
  - Hand-held – a device being in one's hand when observed.
  - Performing an interactive communication function.
    - SMS, Calling, sending data, **providing access to the Internet**.
    - Penalty – 3 points, £100 fine.

- An offence of death by dangerous driving?
  - Judged against the '**careful and competent driver**'
  - Do they use their mobile phone in any way whilst driving?
    - doubtful

Mobile Phone Usage

- Standard usage analysis.
  - Time and date messages/ emails were sent.
  - Time and date calls were made.
  - Internet History records.
  - Social media posts etc.

  - But what about activity which occurs on a handset but leaves less obvious traces on the device?
    - For example, Reading the headlines on a news-bulletin application?

Passive Activity

- Passive activity is coined to denote actions which leave behind a less obvious evidential traces.

- Examples:
  - Re-reading SMS in the inbox/sent folder.
  - Scrolling through a twitter feed.
  - Reading news articles on applications such as BBC News.
  - Simply activating the handset to view the dash-board of a device.

- Passive actions still distract a driver as their eye-sight is directed to the handset, not the road for a period of time.

Investigation

- Statistics indicate Android and iPhone devices are the two leading manufacturers.
- The investigation into the acquisition of evidence denoting passive activity therefore took place on both these platforms.

- Test Devices:
  - iPhone 4 – running iOS 7
  - HTC One – Kit Kat 4.4
- Test Kit:
  - Microsystemation XRY

iPhone Analysis

iPhone Analysis

- This investigation will focus on the iPhone's `CurrentPowerlog.powerlog (CPL)` system file, and the `PLArchive` directory, both located at `/var/mobile/Library/Logs/`.

- The CPL consists of system events on the handset.
  - Each entry is prefixed with an ‘attribute tag’ making it possible to scan the CPL for similar event types.

- The CPL runs for a 24 hours period.
  - Handsets usage can be profiled for activity.

iPhone Analysis

- The period in which the CPL covers is defined at the start of the file under the attribute `[Log]`.

- At the end of its logging period (rollover date), it is moved to the `PLArchive`.
  - Each CPL is placed within a `.gz` archive and its naming convention represents the starting date of the log (e.g. `PL_2014-08-04-`).
  - `PLArchive` does not store all of the CPL files, but after the limited experimentation, CPL archive entries were present for up to 3 weeks.

- **Further testing on newer iPhone devices where only a file-system extraction type was available through Cellebrite indicated that both the CPL and PLArchive files were only available when the device was jail broken.**

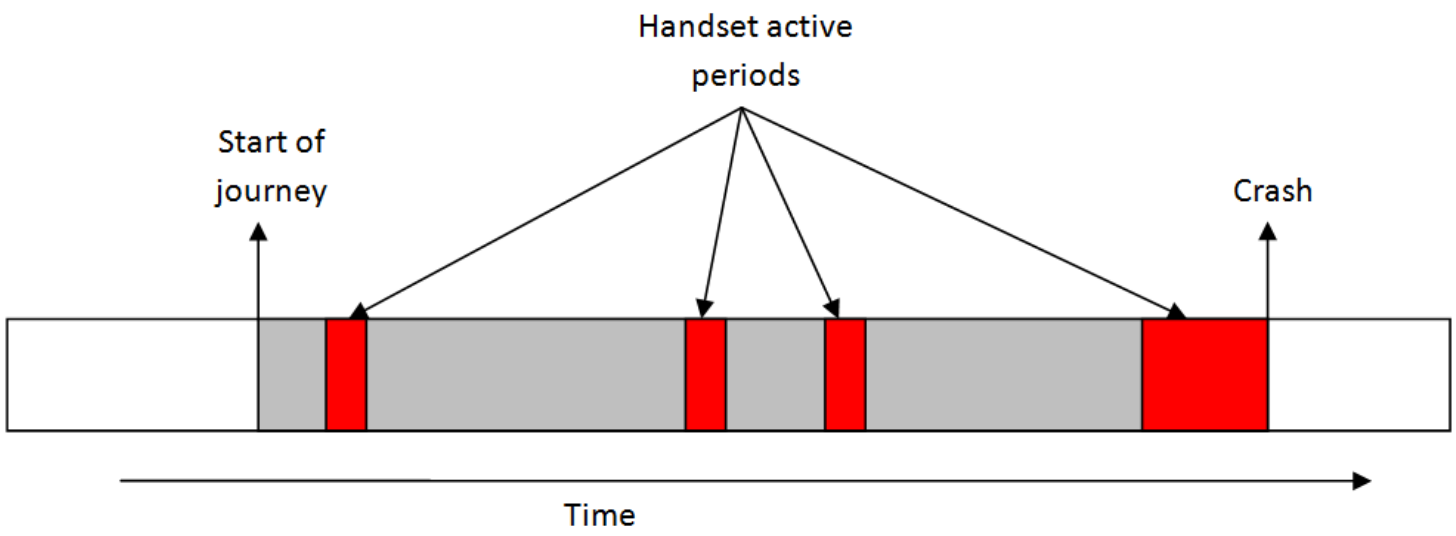
IPhone Analysis

- Pressing the power button:
  - [Display] active=yes; brightness = 50.0%;
  - [Display] active=yes; brightness = 0.0%;

- Unlocking the handset:
  - [Springboard-states] Screen_state=unblanked; lock_state=locked;
  - [Springboard-states] Screen_state=unblanked; lock_state=unlocked;

- In-car charging
  - [Battery] log entries indicate when the device is connected to a charging facility
    - Proceeding log entries show the continuous charge of the iPhone's battery.

iPhone Analysis



iPhone Analysis

- Identifying the usage of applications
- `[Application]`
- `Executable=` – Application in use
- Modes:
  - Foreground Running
  - Background
  - Running
  - Terminated
  - Suspended

iPhone Analysis

```
07/28/14 00:00:48.181 [Network Connections Symptoms] procName=com.apple.facebo; bundleName=<
07/28/14 00:00:48.190 [Network Connections Symptoms] procName=syncdefaultsd; bundleName=<unkr
20:55:26.239;
07/28/14 00:00:48.191 [Network Connections Symptoms] procName=itunescloudd; bundleName=<unkn
07/28/14 00:00:48.196 [Network Connections Symptoms] procName=Phantom; bundleName=7324EM48KV.
22:22:34.705;
07/28/14 00:00:48.203 [Network Connections Symptoms] procName=Preferences; bundleName=com.app
21:00:44.148;
07/28/14 00:00:48.205 [Network Connections Symptoms] procName=fakemsg; bundleName=com.fakems
21:47:34.414;
07/28/14 00:00:48.209 [Network Connections Symptoms] procName=libidtool; bundleName=<unknown>
07/28/14 00:00:48.211 [Network Connections Symptoms] procName=CommCenterClassi; bundleName=<
11:40:36.326;
07/28/14 00:00:48.215 [Network Connections Symptoms] procName=aosnotifyd; bundleName=<unknow
07/28/14 00:00:48.222 [Network Connections Symptoms] procName=mstreamd; bundleName=<unknown>
07/28/14 00:00:48.224 [Network Connections Symptoms] procName=ubd; bundleName=<unknown>; wif
07/28/14 00:00:47.704 [Application] id=de.andi.syslogman; pid=<unknown>; mode=Foreground Run
07/28/14 00:00:48.413 [Application] id=com.apple.mobilemail; pid=212; mode=Background Runnin
07/28/14 00:00:48.905 [Application] id=com.facebook.Facebook; pid=217; mode=Background Task
executable=Facebook; version=12.1;
07/28/14 00:00:48.995 [Application] id=com.apple.mobilecal; pid=227; mode=Background Task Su
07/28/14 00:00:51.294 [Display] active=yes; brightness=10.5%; user_brightness=<unknown>; als
07/28/14 00:00:51.311 [SpringBoard-states] screen_state=unblanked; lock_state=unlocked;
07/28/14 00:00:51.310 [Application] id=de.andi.syslogman; pid=347.00; mode=Foreground Runnin
07/28/14 00:00:52.165 [SpringBoard-screens] Screens=3;
07/28/14 00:01:06.559 [Battery] level=74.96%; voltage=3941 mV; current=-230 mA; current_capa
adapter_info=0; connected_status=0;
07/28/14 00:01:06.651 [Network Statistics] interface=en0; tcpNoConnNoList=23; tcpCleanup=8;
```

iPhone Analysis

- Hand's free kits
  - Not illegal – BUT, must be used!
  - Its presence in the car does not suggest that the device was paired with it.

- Testing with a 'Plantronics M20' hands-free kit when simulating call activity showed Telephony records indicating a call and audio had been routed to a 'headset

```
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
```

Android Analysis

Android Analysis

- No equivalent of the CPL could be located on the android handset.
- Focus was maintained on the Androids' buffer logs accessible under `/dev/log`.
- Volatile – when power is removed from the handset, content is gone.
- Access is provided by Android Debug Bridge (ADB).

Android Analysis

- Type and size considerations…

Table 1
Types of buffer log

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

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)

Android Analysis

- Buffer logs contain records of activity on the handset, similar to the CPL.
- Entries are prefixed with a Process ID (PID) which can be used to filter logs for activity.
- Using the `logcat` command buffer logs can be extracted for further analysis

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

ADB

Android — adb — 80×24

```
668,52250009,430441,1426774637062]

[ 03-19 14:17:10.159   712: 1085 I/am_create_service ]
[0,1120755792,.WeatherIntentService,10253,3041]

[ 03-19 14:17:10.429   712:  712 I/notification_cancel ]
[com.htc.sense.mms,123,NULL,0,0,64]

[ 03-19 14:17:10.429   712: 1352 I/am_create_service ]
[0,1117277488,.ProductivityService,10078,933]

[ 03-19 14:17:10.429   712:  712 I/notification_cancel ]
[com.htc.sense.mms,123,NULL,0,0,64]

[ 03-19 14:17:10.499   712: 1085 I/am_destroy_service ]
[0,1117277488,933]

[ 03-19 14:17:10.769  1048:17102 I/content_query_sample ]
Binder:22814

[ 03-19 14:17:11.250   712:  924 I/am_destroy_service ]
[0,1120755792,3041]

_
```

Android Analysis

- Some examples:

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.

Android Analysis

- Is this approach practical in an accident investigation?
- ADB can access log information even if handset is locked – providing debugging mode is enabled.
- All that is required are drivers for the handset and the ADB application.
- Time is the issue….

Android Application

- The buffer logs are volatile and of a small size.
  - More activity on the handset increases overwritten data.
  - Handset must remain on until investigated therefore activity is constantly changing.

  - How long do you have?
    - Depends on make/model for size of buffer logs.
    - Activity on handset
    - Potential for about a 2-6 hour period where buffer log content denoting the activity on a device directly prior to an incident will still be present.

Device Integrity

- As the device must stay on for buffer logs to be acquired, the device will change and possibly received outside communications.
- Analyse at the scene.
  - Forensic laptop
- Analyse in the lab
  - Speed at which device can be transferred there.
  - Faraday technology.
    - Battery considerations.
    - More battery activity, potential for logs to be overwritten quicker.

Future work

- In-built engine management systems with hands-free/phone synching capabilities.

- Passive activity on different handsets
  - Windows phone
  - Blackberry

Any Questions?