

Digital Forensics for Automobile Systems: The Challenges and a Call to Arms

James Moos^{1*}, Gareth Davies^{2*}, Elinor Lewis³, Nathan Williams³,
Brian Gichohi³, Rebecca Lane³, Andrew Bellamy³

Research Article

Volume 1 Issue 1

Received Date: May 13, 2016

Published Date: June 06, 2016

¹Department of Computer Forensics, University of South Wales, UK

²Lecturers of Digital forensics at the University of South Wales, UK

***Corresponding author:** Gareth Davies, University of South Wales, UK, Email: gareth.davies@southwales.ac.uk

Abstract

Vehicles nowadays contain computer systems that enable navigation and entertainment. These units have the potential to generate evidence for an investigation. This paper presents the research work undertaken to apply the field of digital forensics to 4 different automobile entertainment systems, both genuine manufacturer and aftermarket. A number of challenges were faced and are presented here along with some findings and suggestions for future work.

Keywords: Digital Forensics; Vehicles; Automobile Systems; Infotainment Systems

Methodology

Introduction

Digital forensics is a field that has advanced rapidly since its birth just decades ago. Skills, processes and tools were developed in order to give the ability to retrieve evidence of a digital nature for investigations, potentially leading to court. This originally handled 'ordinary, straightforward' computer data. Nowadays, digital forensics spans a much more vast area, including games consoles, smart phones, network traffic and smart watches, to name a few. Technology is evolutionary in nature and new devices and technologies continue to be released to the consumer world. Amongst recent releases are highly capable computer systems that now appear in cars. These offer users advanced features such as GPS navigation, entertainment (CD/DVD/SD Card/USB device), communication (SMS, phone calls, phonebook), mobile phone sync capabilities and also stand alone Internet browsing (via an embedded SIM card) and WiFi hotspot capabilities (Motavalli, 2010; Ford, 2015; Laird,

2012). These are all artefacts that are likely to be extremely relevant to an investigation. The capabilities of in-car 'infotainment' systems are only developing further and yet to date, no real efforts have been taken in the UK to research digital forensics for automobile systems. This project was created in order to further the understanding of the digital forensics community about applying this discipline to vehicle infotainment systems.

Vehicle Infotainment

Cars as a concept began many years ago and focused on the transportation of people and baggage. Comprising of relatively basic components such as a frame, wheels, axis and engine, when problems occurred, it was likely to be a mechanical issue. By contrast, nowadays a car problem is often related to electronics. Multiple Electronic Control Units (ECUs) can exist in a car as part of a CANBUS, which is a dedicated car network (Right Connections, n.d). It is this same network that all infotainment devices are ordinarily connected to. When diagnosing vehicle faults, a computer is normally connected to the OBDII (On Board

Diagnostics) port in order to identify the issue (Stevens and Goodwin, 2010). A list of common features for infotainment systems has been produced below in order to summarise some of the common features and capabilities that are readily available in cars today. Digital investigators will quickly be able to identify from this list a number of potential artefacts. At this point, a number of key observations must be made. The infotainment systems vary between manufacturers and so therefore different systems may hold different artefacts. No research work appears to have been done in the UK to date to examine just how much data from the above capabilities may be retained. There is some movement towards vehicle investigations in the US however, with a toolkit named iVe (Berla, n.d) available to support a limited number of vehicle makes and models.

Digital Forensics

Just like the older, more traditional field of forensic science, digital forensics is all about the collection, preservation, analysis and presentation of evidence. The difference between the two disciplines is the nature of the evidence being processed. As the name suggests, digital forensics handles electronic/digital devices and data. The end goal for this process is often legal proceedings, meaning that sound forensic processes must be followed in order for the evidence to remain admissible in court. Digital forensics, although originally intended for computer systems, is now applicable to any device that contains computing abilities. This includes mobile phones, tablet computers, smart TVs and games consoles. As technology develops, more research and focus is required within the field of digital forensics in order to ensure evidence can be retrieved and analyzed in a controlled and secure manner. Digital forensics in the UK follows guidelines such as the Association of Chief Police Officers (ACPO) Best Practice Guide for Digital Evidence (Williams, 2012). As new devices are researched, the importance of meeting such standards cannot be overstated. This ensures that aspects of the work such as integrity and repeatability are not compromised. Sub - disciplines of digital forensics have emerged in recent years, most notably: mobile phone forensics, in order to provide specialist skill sets for frequently seen devices that require differing approaches. Given the rise in integrated vehicle infotainment technology and its capability, it is not unimaginable to perceive a future sub -discipline specializing in the retrieval, analysis and presentation of evidence in this area.

Digital forensics however has not yet been applied to vehicles in a regulated manner. An open source trawls through sources such as www.Forensicfocus.com suggests

that occasional ad-hoc investigations may have been attempted, but no formal research or capability exists in the UK. Research underpins the ability for casework to be conducted with confidence that processes and tools used are appropriate. As a result of this clear gap, a team of digital forensics students at the University of South Wales decided to tackle this problem and provide a first insight into what this area holds.

Vehicles Used

This project focused on a variety of vehicle infotainment systems in order to gain exposure to different systems and technologies. This included Original Equipment Manufacturer (OEM) units and also aftermarket devices. The OEM units were all 2nd hand units removed from vehicles, while the aftermarket devices were purchased new. This research work made use of both traditional digital forensics tools and also some specialist equipment, all of which are presented in Section D. A table summarizing the vehicle infotainment systems used by this project can be found at Table 1. It is important to acknowledge at this stage that for the 2nd hand devices that were purchased for this research, there was absolutely no knowledge of how these systems were used prior to this point. As a result, these units may have had little or no use, resulting in a severe lack of data. This is often the case in such research work with an unknown system. The 2 Pioneer devices were purchased brand new as they were relatively new to the market, offering advanced interaction with Android mobile operating systems and Apple CarPlay support for iOS devices.

Infotainment Feature
GPS Navigation
CD/DVD Player
USB Port
SD Card Slot
Bluetooth
WiFi Hotspot
Internet Browsing (via embedded SIM card)
Internal Memory Storage
Phone Sync (SMS, calls, phonebook, email)
Reverse Parking Camera
Voice Control
Automatic Emergency Dial
Apps (e.g. Calendar)

Make:	Model:	Age:	Additional Information:
Vauxhall	Insignia	2014	OEM, 2 nd hand device
Vauxhall	Zafira	2012	OEM, 2 nd hand device
BMW	4-Series	2014	OEM, 2 nd hand device
Pioneer	SPH- DA120	2015	New aftermarket system
Pioneer	SPH- DA120	2015	New aftermarket system

Table 1: Vehicle Infotainment Systems Used.

Vauxhall Systems

Modern-day Vauxhall systems offer capabilities such as OnStar (Vauxhall, 2016). This offers a suite of features including remote control via a Smartphone, GPS tracking if stolen, a WiFi hotspot and diagnostic features. Also supporting emergency phone calls in case of a collision, it is quite possible that some modern Vauxhall units contain an embedded SIM card. As the Vauxhall systems used in this project (Zafira and Insignia) were models from 2012 and 2014 respectively, it was quite possible that some of these features would not be present, particularly in the older model Figure 1. Parkers (2011), a reputable car review website, suggest that a 2012 Zafira could contain USB connectivity, front and rear camera packs and satellite navigation system. This is of course, dependent on the particular version of the Zafira. The same car website also offers an insight into the 2013 edition of the Insignia, with a satellite navigation system and touchpad, front and rear cameras, blind spot monitoring and forward collision warning as just some of the features that might be available (Parkers, 2013).



Figure 1: Vauxhall Insignia Cockpit (Express.co.uk, 2013).

BMW

BMW is popular German vehicle manufacturers that are recognized internationally as a luxury brand. In line with this perhaps, it is not surprising that a number of infotainment features are available with these cars. Just like the later Vauxhall models, BMW offer an emergency services call system named 'BMW Intelligent Emergency Call' (BMW, 2015a). This is able to send data to a BMW centre detailing the position of the car, the number of passengers and other important information. All of this can then be passed to the emergency services if required. Figure 2: BMW Cockpit (Driving.co.uk, 2015). Through USB connectivity, driver profiles are used by BMW to allow personal settings (BMW, 2015b). A messaging capability is also present through BMW Connected Drive, along with Internet browser and connectivity.



Figure 2: BMW Cockpit (Driving.co.uk, 2015).

Pioneer

Pioneer is a well-known brand not just in the automotive industry but also sports and music equipment. Pioneer's products include car entertainment systems, of which the SPH-DA120 originates from. This unit is a double DIN (Deutsches Institut für Normung - a size specification) touch screen device. It is one of the first to offer Apple's CarPlay system, which allows advanced interaction with newer models of Apple iPhone. As a result, features from the iPhone such as Messages, Phonebook and Phone calls can appear on the SPH-DA120 (Pioneer, n.d). This unit also offers Android handset connectivity through the 'AppRadio' application, Bluetooth and USB connectivity. Figure 3: Pioneer SPHDA120 (Pioneer, n.d). Despite not being OEM, many drivers purchase aftermarket systems. With advanced features such as Apple CarPlay now available, this may become even more popular in order to upgrade a vehicle's infotainment features at a relatively affordable price. These units cost considerably less than specifying an OEM

infotainment unit as an extra when ordering a brand new vehicle.



Figure 3: Pioneer SPH-DA120 (Pioneer, n.d).

Vehicles Summary

It is apparent just from examining the range of features available on each system that an extensive number of artefacts may be present on vehicle infotainment systems. This paper only presents the main features for each unit, while investigations may benefit from lesser features too. A vehicle infotainment system could assist an investigation by demonstrating a connection between a subject and a vehicle, the location of a vehicle at a particular time, or hold a host of mobile phone artefacts as an alternative data source. When you put this into a particular scenario such as CT (counter terrorism) investigation, it suddenly becomes high priority information. Again, this only briefly explores the vast range of ways the information from one of these systems could impact an investigation.

Tools Used

This research work sought to identify to what extent traditional digital forensics tools and processes could be applied to vehicle infotainment systems. As a result, some well - known industry tools were used to facilitate both acquisition and analysis. Alongside this however, the requirement arose to find and utilize alternative operating systems and software tools that were specialist in nature and already geared towards interacting with a particular vehicle system. Both the traditional tools used and the specialized tools can be found below in Table 2. Software tools cannot do the work alone in this type of challenge. The vehicle units had already been removed from the vehicles and so there was no requirement during this work to physically remove these units from

dashboards. However, deconstructing these devices was important as a first step towards identifying the technology used and in particular, the memory storage type. This involved a series of screwdriver kits (Philips heads) and also screwdriver heads that are often used in mobile phone forensics, such as 'T' style screws. Also in line with mobile phone forensics, the technique of 'chip-off' was also used. This involves heating the memory chip with a heat gun in order for the solder beneath to melt, allowing the chip to be lifted. It can then be read through an adapter and analysed as a raw dump of data.

Tool Name	Version	Use
Thumbscrew		
FTK Imager	-	USW Write Blocker
QNX Neutrino RTOS	v.4.0.0	Acquisition
PhotoRec	v.6.6	Operating System
WinHex	v.7.0	Data Carving
Linux Ubuntu	v.18.7	Hex Viewer
Mac OS X	v.	Operating System
Windows	v.10.10.1	Operating System
Power Unit	v.7	Operating System
Berla iVe	-	Power Supply
Autopsy	v.	Vehicle Forensics
ArcGIS	v.2	Analysis
Sleuthkit	v.	Map Analyser
HxD	v.2	Analysis
PC3000	v.1.7.7.0	Hex Viewer
	-	Data Recovery

Table 2: Tools Used.

Observation

In order to understand the various systems from a digital forensics perspective, it was first necessary to gain an understanding of the underlying technology. This was to provide initial knowledge about what memory storage types were used and to gain an insight into what acquisition methods might be possible. Each infotainment unit was photographed as entire devices, before being deconstructed to Printed Circuit Board (PCB) level. Throughout the entire process from here on, contemporaneous notes were kept to maintain best practice.

Acquisition

The acquisition process varied for each device, unsurprisingly. With different vehicle manufacturers using completely different unit types, no single method of acquisition would be appropriate for all. Decisions were made for each device's acquisition based on a variety of considerations that included best practice, least destructive method and also time limitations available for this research.

Analysis

Once again, due to the variety of systems, analysis methods and tools used varied between the different infotainment devices. Once acquisition had been performed, the first priority was ensuring integrity, as this will always be a critical component of an investigation. Beyond this, completely different approaches were made based on open source research, technologies identified during the 'Observation' stage and other information learnt during the observation and acquisition.

Deleted Data

Efforts were made where possible to perform data carving. This was an extra measure taken in order to gain a more in-depth understanding of the systems by looking at how data was retained, deleted and what could still be recovered even after the system had marked items for deletion.

Applied Methodology

Observation

Vauxhall Zafira



Figure 4: Zafira 2012 Infotainment Unit (bird's eye view).

This unit was a small, touchscreen unit that houses everything together – the touchscreen, memory capability and processing components. The sticker on the unit identifies this as a 'sat nav unit', but this may be from the reseller and not a manufacturer's label. Figure 4 It's connection ports at the rear appear to include an ISO socket and two other unrecognised ports that may relate to antenna connections. It is noted that this, perhaps due to being older than the other infotainments used in this research, is more limited in the connection ports offered. It does not appear to offer USB connectivity. ISO ports may vary in layout between manufacturers, models and age, but usually offer power and audio feeds for speakers Figure 5.



Figure 5: Zafira 2012 Infotainment Unit (rear view).

The front of the unit alone indicates the presence of Bluetooth in this particular model. This confirms that some level of interaction with mobile phones is possible and that the data could potentially exist if it was used for this purpose. A phone symbol can be seen on one of the buttons, suggesting it may be a dedicated button to answer and hang up phone calls. A 'Nav' and 'Map' button confirms that this is indeed a satellite navigation system. As users are often able to save locations, input new destinations for a journey and save contacts, underlying data from this could become an artefact Figure 6. This device was then stripped down to the PCB in order to examine the technology beneath. It should be highlighted at this point that the researchers have a digital forensics background and are not specialists in electronics. Examining the PCB led to quick identification of a MicroSD card. No other memory sources were found on the PCB.

Vauxhall Insignia

This unit comprised multiple parts, simply due to what was provided by the seller. This included a main dash (possessing a touchscreen component along with air vents), a lower dash unit (power and control buttons), a

touchpad, a CD/DVD unit and a Bosch Human Machine Interface (HMI) control unit for navigation and infotainment Figure 7. The Bosch unit labels provide clear identification of the model number, as well as an indication of some capabilities/ features it offers. 'NG 2.0 HMI' can be seen clearly along with '2342 7519'. This identifies the particular model. Small text printed indicates this relates to 'car multimedia' and a quick open source search of the unit details confirms the item to be a control unit for navigation and infotainment. Opening up the Bosch unit (via removal of 4 screws and some clasps) allows the PCB to be examined. A variety of ports appear on the PCB, including 3 miniUSB ports. Connection points on the PCB itself could be seen, which could indicate JTAG points, or similar manufacturer testing connectivity. Multiple unrecognised ports also reside at various locations on the PCB Figure 8.



Figure 6: Zafira 2012 Infotainment Unit (front view).

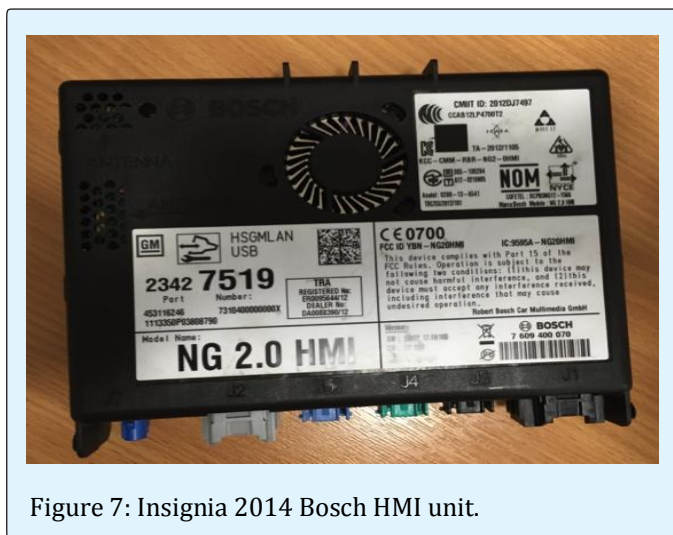


Figure 7: Insignia 2014 Bosch HMI unit.

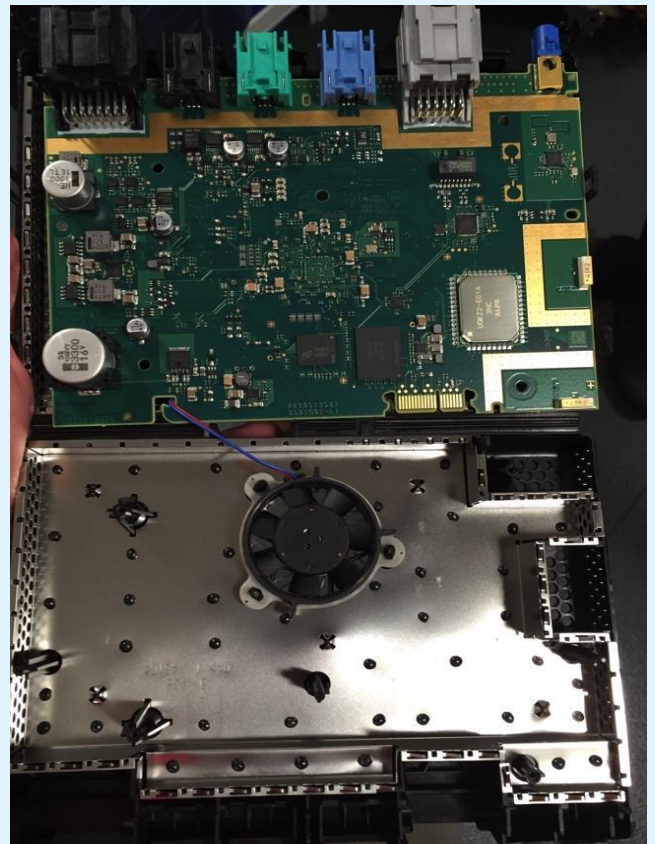


Figure 8: Bosch HMI unit internals.



Figure 9: Insignia 2014 Main Dash Unit

Open source information provides a good examination of the technology within a previous model of this device, the NG 1.1 HMI (IHS Electronics360, 2013). While this was an older unit teardown, it could provide some guidance as the two units do not visually appear to be all that dissimilar. The NG 1.1 HMI reportedly has a 32GB electronic Multimedia Card (eMMC) chip as its storage method, boasting features such as Bluetooth, Wireless

Local Area Network (WLAN) as well as support for CD, DVD and SD card. Figure 9 eMMC chips are frequently found on mobile phone PCBs and so this information was encouraging. The main dash unit presented two main connection ports at the back, one of which was identified as a mini-USB port. This suggests that the cables used between the Bosch control unit and associated devices such as the touch screen are mini-USB cables. Dismantling this device did not result in any further findings Figure 10. This lower dash unit seen above for the Insignia bore no relevance to the investigation of this vehicle's infotainment system, as there was no storage. This panel simply hosts a number of buttons. That said, the On/Off button seen could be advantageous for future research in order to interact with the system and plant data as a user would. The CD/DVD unit was dismantled but no further features or components were found - this is a straightforward disk drive.



Figure 10: Insignia 2014 Lower Dash Unit.

BMW 4 Series

The BMW 4 series infotainment system is an 'all in one' unit. The CD/DVD drive can be observed at the front of the unit, along with a unit label on the top. The label identifies this as a BMW unit and also contains symbols for Bluetooth and WiFi. The label indicates the unit is made for BMW by 'Harman Automotive' Figure 11. The system's connection ports at the rear of the unit include an ISO port, and then 12 further unidentified ports. These may offer input for other parts of the vehicle such as antenna, however this cannot be confirmed. Dismantling the device produces a CD/DVD drive and a 200GB Toshiba SATA hard drive. This hard drive contains a label as practitioners would expect, which gives manufacturer and model details. Figure 12, 13.



Figure 11: BMW 4 Series Infotainment Unit (front view).



Figure 12: BMW 4 Series Infotainment Unit (rear view).



Figure 13: BMW Toshiba SATA Hard Drive.

Pioneer SPH-DA120

The 2 Pioneer devices purchased for this research differ from the other units as they are brand new and are aftermarket units, rather than OEM supplied. As a result, relevant connection cables were provided in the box. As

both units were identical, only one was dismantled Figure 14. The Pioneer offers a number of connection ports at the rear that includes USB, HDMI and audio. This is to support a variety of functionality that it appears to offer Figure 15. Undoing a number of screws, loosening clips and finally detaching a ribbon cable can remove the inner unit from the outer casing. This exposes the PCB along with a 4GB SD card. This particular vehicle unit, being new, required data to be planted. In order to do so, an electronic power supply was used to provide the required power input. From there, a series of interactions were made with the device via Bluetooth using an Android handset.



Figure 14: Pioneer SPH-DA120 (front view).

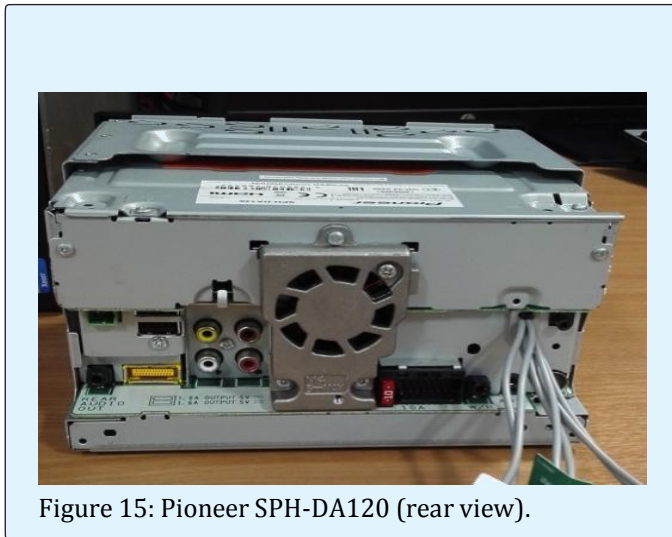


Figure 15: Pioneer SPH-DA120 (rear view).

Acquisition

Vauxhall Zafira

The 8GB MicroSD card, being a common storage device, was straightforward to extract data from. The MicroSD card was forensically imaged using FTK Imager and at this

point, MD5 and SHA-1 hash values were also captured and recorded in the contemporaneous notes. This was done using software USB write blocker and a USB adapter for MicroSD cards, but could have been done using a MicroSD card write blocker. The write-blocking software was tested on a dummy USB by attempting to write files to the USB. This process failed, confirming that the software was fully functional. As no other memory storage was identified for this device, this acquisition was the only process to conduct for the Vauxhall Zafira acquisition stage.

Vauxhall Insignia

The memory chip on the Bosch HMI unit was identified as a BGA chip and a 'chip - off' was performed due to time constraints. It is believed that if potential JTAG ports could be confirmed, this could be an alternative, non-destructive route into extracting data. At the time of writing, the required memory chip adapter (in order to read and extract the data) is currently en-route having been purchased, but has prevented the analysis of this system.

BMW 4 Series

The Toshiba SATA hard drive removed from the BMW 4 series was another 'traditional' evidence source that investigators are familiar in dealing with. That said, initial attempts to image the drive using software write blocker and a SATA docking station failed, despite the drive spinning when powered. Further examination using PC3000 identified an ATA password, which was subsequently removed. This then enabled the drive to be imaged successfully using FTK Imager. MD5 and SHA-1 hash values were captured and recorded just as an investigation would require. It is important to note that the ATA lock should be re-applied if the hard drive is to be returned to its original vehicle - without this it will not work. It was later discovered that the ATA password on this unit is comprised of unique IDs. This may provide an alternative solution to bypassing such a password for those who don't have access to specialist tools such as PC3000.

An online forum member going by the name of '2Real4u' describes how the ATA password consists of hard drive and device details in the following format: Ethernet MAC address: Bluetooth MAC address: long serial number (2Real4u, 2015). The long serial number can be recovered from a sticker on the exterior of the unit. Similarly, the Ethernet MAC address can also be seen on a sticker on the exterior of the unit. At present, no indication of the Bluetooth MAC address has been found.

Pioneer SPH-DA120

As an SD card was removed from this device, once again traditional methods that are well known and understood should be applicable to perform an acquisition. This proved not to be the case in as much as the SD card could not be imaged using Linux, Mac OS X or Windows 7 as it would not register on the host operating system. This issue could have been down to a number of different causes. The SD card provided by the manufacturer could have been faulty or could rely on a special flavor of an operating system (most likely Linux) in order to be recognized/compatible. Powering up the SPH- DA120 without a memory card in provided an error message, suggesting that the SD card was functional and that some part of the boot process or device operating system resided on the SD card. The intention for these 2 Pioneer devices, considering they were purchased brand new, was to perform an image of the blank system initially. This would give an insight to any standard directory trees or system layout. After this, the system could be populated and then reimaged in order to observe data appearing. Due to the lack of success in initially imaging the SD card, one Pioneer device was powered and some data planting was conducted using a HTC One M9 smart phone (Android 5.1) and recorded in contemporaneous notes. However, it was observed that after re-powering the device, no traces of any user activity from the previous session remained.

The SD card from the 2nd Pioneer device was analysed. This device had already been populated with data by interacting via the Apple CarPlay feature. If this SD card registered correctly and was able to be imaged, it would confirm the first SD card was faulty. The 2nd Pioneer's SD card however was also unable to be recognized and imaged, indicating that further work will be required in order to establish an operating system that will interact with the SD card. On a technology 'hacking' website named www.fail0verflow.com, Byer (2014a) provides an interesting insight into a similar Pioneer device. While his objective is to modify the firmware to deal with an error message, he shares valuable information pertaining to the SD card issue discussed and alternative ways to connect to the unit. Byer focuses on a slightly older Pioneer unit, the AVIC-500NEX, which, from his photos, has a similar PCB layout to the SPH -DA120 being considered here. He encountered the SD memory card reading problem as presented in this paper and suggests that CMD42 password protection could be a possibility. At this point, Byer circumvents the issue by examining alternative possibilities to interacting with the device. He identifies both JTAG and UART ports on the PCB, all of which can be found on the SPH-DA120 PCB too Figure 16. Byer

successfully connects to the device via JTAG and is then able to interact with the system. He recovers the CMD42 password from the firmware and as a result, gains access to the SD memory card. The file system directory structure can be seen below. At this point, it is worth noting that Byer's SD card is 8GB in size, whereas the unit in this research only has a 4GB SD card Figure 17. The directory named '/data' could potentially hold user data that you would expect to find, such as Bluetooth pairings, but as Byer is not examining this system from a digital forensics perspective, this remains unknown.

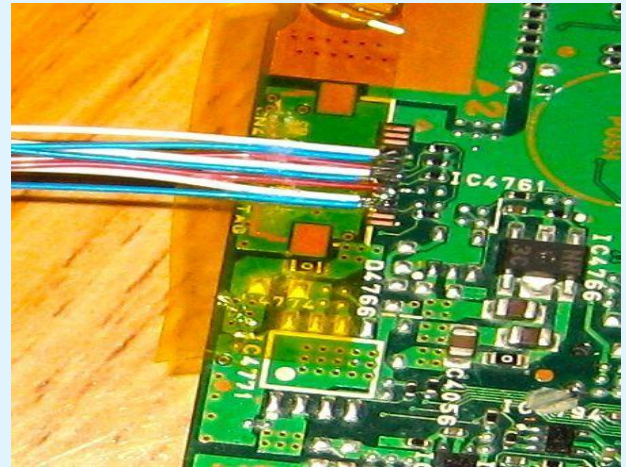


Figure 16: Pioneer AVIC-500NEX JTAG Ports Source: Byer (2014a).

```

Disk /dev/mmcblk1: 8069MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start  End      Size    Type   File system
 1      538MB  548MB   10.5MB  primary  android    boot A
 2      548MB  559MB   10.5MB  primary  android    boot B
 3      559MB  1830MB  1271MB  extended
 5      559MB  590MB   31.5MB  logical  android    recovery A
 6      590MB  622MB   31.5MB  logical  android    recovery B
 7      622MB  1159MB  537MB   logical  ext4       /system
 8      1159MB 1293MB  134MB   logical  ext4       /cache
 9      1293MB 1830MB  537MB   logical  ext4       /data
 4      1830MB 7702MB  5872MB  primary  ext4       /extdata

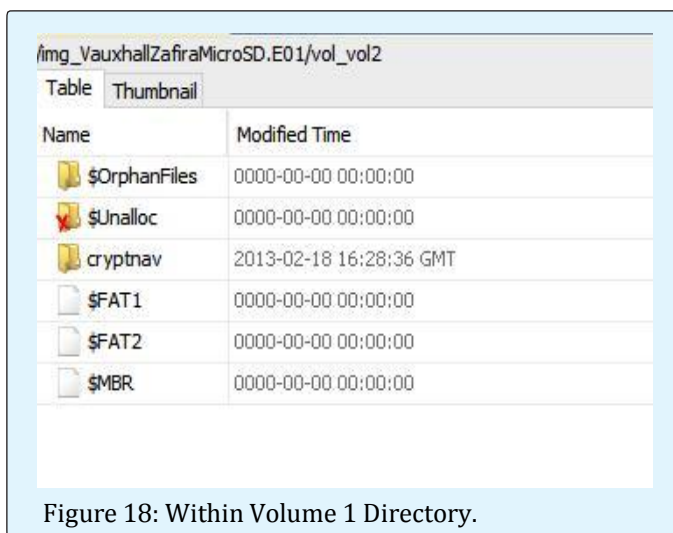
```

Figure 17: Pioneer AVIC-500NEX 8GB SD Card Directories Source: Byer (2014b).

Analysis

Vauxhall Zafira

Following the successful imaging of the MicroSD card from the Zafira, the Autopsy toolkit was used for analysis. One main partition was found, which had no associated name. This was in FAT32 format and will be referred to hereon as Volume 1. A second volume was also present but this represents unallocated space. Volume 1 contained three main directories within: '\$OrphanFiles', '\$Unalloc' and 'cryptnav'. Also within this partition, a '\$FAT1', '\$FAT2' and '\$MBR' can be found, as seen in the screenshot below at Figure 16. This presence of \$FAT1 (File Allocation Table), \$FAT2 (copy of File Allocation Table) and \$MBR (Master Boot Record) confirms that this is a FAT file system as these are recognizable artefacts for digital forensics practitioners. \$Orphan Files may contain metadata for deleted files and \$Unalloc refers to unallocated space Figure 18. Therefore, from the directories seen above, the only one that is not automatically created through FAT32 is the 'cryptnav' folder. Within the 'cryptnav' folder, 3 sub -folders exist. These are 'cfg', 'data' and 'dnl'.



Name	Modified Time
\$OrphanFiles	0000-00-00 00:00:00
\$Unalloc	0000-00-00 00:00:00
cryptnav	2013-02-18 16:28:36 GMT
\$FAT1	0000-00-00 00:00:00
\$FAT2	0000-00-00 00:00:00
\$MBR	0000-00-00 00:00:00

Figure 18: Within Volume 1 Directory.

Focusing on 'cfg' firstly, this has 2 sub- directories ('tima' and 'voice'). 'tima' contains a series of .etx files with naming conventions such as 'en-gb.etx'. This appears to be files that contain satellite navigation data in various languages. Text such as "slip roads closed", "slow traffic" and "obstructions on the road, danger" from the 'en-gb.etx' file indicate this. This .etx filetype observed is, according to ReviverSoft (n.d) a "Setext Structure Enhanced Text File". A text viewer or hex editor can open these and data is usually in ASCII format. In addition to the .etx files, 2 .cnf files were also observed. File-extensions.org (n.d) describes .cnf files as network

configuration files which can sometimes "store network configuration including user name, password, [and] server names". Both the .etx and .cnf files contain copyright marks for Robert Bosch GmbH – a well known vehicle parts manufacturer (the very same that produce the NG 2.0 HMI unit discussed in this paper). This may suggest that Bosch is responsible for the navigation system. Within the .cnf files, a series of hex appears with no other indication of what might lie within. This hex data was removed and placed within a hex editor, HxD, but no successful translation was obtained.

'Volume1/cryptnav/cfg/voice' (in line with the directory name) contained a number of .pkg package files which appear to hold voice data for a number of different voice types for the user to choose from. In summary, the 'Volume1/cryptnav/cfg' folder does not appear to contain any user data. 2 directories reside within 'Volume1/cryptnav/ data' – 'connect' and 'data'. These can be seen in Figure 17, along with further sub- directories. A variety of file types were found, including .idx, .map, .cls and .uli. The data within was not in a familiar format and this may be due to proprietary systems used by the manufacturer. An alternative possibility is that encryption has been used. Examining the final directory within 'Volume1/cryptnav/', the 'dnl' folder contains a sub -directory 'bin' and two subsequent sub-directories beneath this named 'common' and 'mcgm_eur'. Both these sub-directories contain .uli files that, once again, could not be translated into a meaningful form Figure 19. In summary for the Vauxhall Zafira MicroSD card, a severe lack of data was found. From the files on the system, no evidence of user data being present was found. However, a large number of files could not be interpreted into a form that was recognizable and so the possibility does remain that user data resides within.

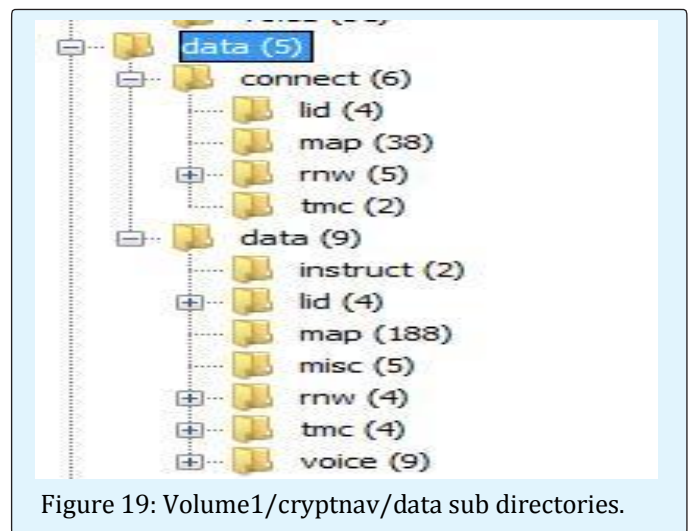


Figure 19: Volume1/cryptnav/data sub directories.

Vauxhall Insignia

At the time of writing, this project was not able to analyse the memory chip dump due to delays in the project timescale. The necessary adapter was purchased from China but due to further delays, resulted in the memory chip remaining un-investigated at the time of writing.

BMW 4 Series

The BMW Toshiba SATA hard drive was recognised as a QNX system. QNX produce In-Car Infotainment (INI) operating systems and further details can be found at <http://www.qnx.com/products/>. In order to successfully interpret the hard drive data, a QNX Virtual Machine (VM) environment was used and this allowed the file system to be recognised. Despite this, a number of file types were not recognised by the system. Attempts were made to install toolkits such as Autopsy and Sleuth Kit onto the QNX environment in order to assist analysis but this was not possible due to the inflexible nature of the operating system. A screenshot below at Figure 18 summarises the main directory structure of the BMW system. This is encouraging as some of the names give a promising indication of what might be held within. Due to the inability to install analysis tools onto the QNX system, little progress was made. Recognisable files such as .db, .mp4, .iso and .sqlite were not able to be examined in their native format which was a barrier to progress Figure 20. Whilst not a forensically sound method, attempts were made to copy files from this system onto a USB storage device in order to transfer and analyse files elsewhere. This proved somewhat successful and a MAC address (presumed to be for the vehicle) and telephone numbers with associated timestamps were found in a settings.dat file. Due to time limitations, it was not possible to take this progress further and look to overcome the challenges of the QNX system, but the small amount of information captured appears to be promising.

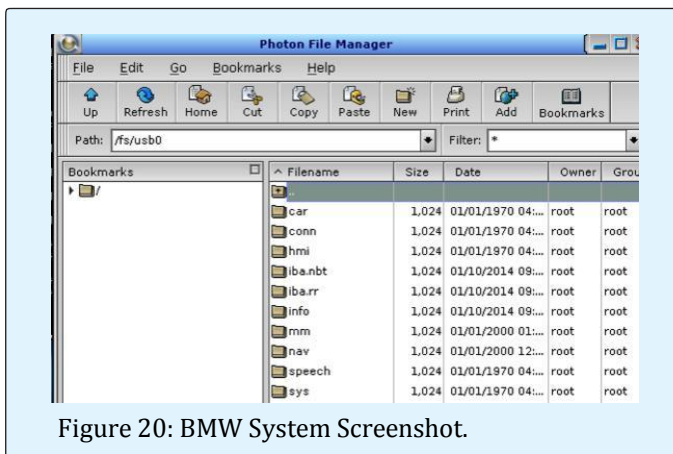


Figure 20: BMW System Screenshot.

Pioneer SPH-DA120

Due to the difficulty in successfully imaging the SD card removed from this system and time constraints for this research work, it was not possible to image and analyse this unit. Whether user data may remain on the SD card itself or perhaps in a memory chip on the PCB is a mystery that, for now, remains unsolved.

Deleted Data

Vauxhall Zafira

The Micro SD card that was removed and imaged from the Vauxhall Zafira was data carved in the hope of finding additional data. This was done using PhotoRec (see tools list) but this failed to recover any user data - related files.

Vauxhall Insignia

As the read of the memory chip has not yet been acquired, data carving was not performed on the Vauxhall Insignia system.

BMW 4 Series

QNX posed a barrier for digital forensics tools to be applied to the data set and this included performing data carving. The hard drive was mounted using FTK Imager and Photorec was used in a bid to recover files but no files were recovered. This is believed to be due to incompatibility with QNX rather than a lack of files. Pioneer SPH-DA120 No successful read was taken of the SD card from the Pioneer systems and so data carving was not possible.

Future Works

This research work was an initial insight into the potential for applying digital forensics to vehicle infotainment systems. While this paper focuses on methods used and background information on each system, results were admittedly lacking. This lack of results cannot be attributed due to a confirmed lack of data though; as barriers in each unit prevented advanced analysis. These barriers included both technology-related issues and also time limitations. With further work, the BMW system is likely to yield valuable evidential data, with the Vauxhall Insignia Bosch HMI unit also being a possible source of evidence that remains, for now, uninvestigated. The Vauxhall Zafira and Pioneer systems appear to be the least promising, but the focus of this paper is not necessarily to highlight individual limitations with particular systems, but rather to shine a light on digital forensics for automobile systems as a whole. This work alone cannot conclusively state whether this new

discipline is achievable or not; further additional work must be conducted in order to expand knowledge in this area and provide better information for the digital forensics community.

Conclusion

Despite the incredible technologies incorporated into vehicle infotainment systems, it appears there is no 'easy win' to recovering data for investigations. All systems faced barriers in the acquisition stage, either through an ATA password, memory chip removal or quite simply, a failure to interact with a memory storage device. Despite this seemingly disappointing first examination of these vehicle systems, lessons can be learnt and it is hoped this will pave the way for future works. This research project faced time restrictions, without which, further progress would likely have been made to overcome some of the challenges. Particularly in the case of the BMW system, positive indications appeared that important data does reside within the system. With further analysis, it is likely that plenty more evidential artefacts will be found. This work presented should give an insight into challenges faced when conducting research into vehicle systems. It is hoped that by identifying these challenges, future works can swiftly deal with such challenges and take the research above and beyond what is presented here.

Authors and Affiliations

James Moos, the author of this paper, was also the project lead for this research work and a researcher. He is a final year student reading an integrated Masters degree in Computer Forensics at the University of South Wales.

Elinor Lewis, Rebecca Lane, Nathan Williams and Brian Gichohi all worked as digital forensics researchers for this project, each undertaking a different vehicle system. Their work to tackle the problems identified provides the basis on which this paper was formed.

Gareth Davies and Andrew Bellamy are both digital forensics lecturers at the University of South Wales. They acted as project supervisors for this research and their help and experience was crucial in conducting this research work.

Acknowledgements

The authors would like to extend their thanks to Control-F Ltd for providing support with the chip off read for the Vauxhall Insignia unit.

References

1. BMW (2015) BMW Connected Drive: Intelligent Emergency Call. Available at: http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/services_apps/intelligent_emergency_calling.html (Accessed: 6 February 2016).
2. BMW (2015) BMW Connected Drive: Services. Available at: http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/services_apps/bmw_connectedrive_services.html (Accessed: 6 February 2016).
3. Berla <https://berla.co/products/ive/> (no date) (Accessed: 3 February 2016) iVe.
4. Driving.co.uk (2015) BMW SatNav Photo [Photograph]. driving.co.uk. Available at: <http://www.driving.co.uk/news/news-sat-navs-to-be-standard-on-all-bmws/> (Accessed: 6 February 2016).
5. Express.co.uk (2013) Vauxhall Insignia Interior Photo [Photograph]. Express.co.uk. Available at: <http://www.express.co.uk/life-style/cars/431050/Vauxhall-driving-forward-with-the-improved-Insignia> (Accessed: 6 February 2016).
6. File-Extensions.org <http://www.file-extensions.org/cnf-fileextension> (no date) (Accessed: 11 February 2016) .CNF File Extension.
7. Ford (2015) Ford SYNC: In-car Hands Free Mobile Phone Bluetooth Technology. Available at: <http://www.ford.co.uk/experience-ford/Technology/FordSYNC> (Accessed: 3 February 2016).
8. IHS Electronics360 (2013) Bosch NG 1.1 HMI Teardown. Available at: <http://electronics360.globalspec.com/article/3632/bosch-ng1-1-hmi-teardown> (Accessed: 7 February 2016).
9. Laird, J. (2012) 'BMW iDrive: The Ultimate Guide', TechRadar, 2 July Available at: <http://www.techradar.com/news/cartech/bmw-idrive-the-ultimate-guide-1085113> (Accessed: 3 February 2016).

10. Motavalli, J. (2010) 'Surfing The Web In The Car', Forbes, 13 April Available at: <http://www.forbes.com/2010/04/13/webbrowsing-wifi-technology-security-10-autos.html> (Accessed: 3 February 2016).
11. Parkers (2011) Vauxhall Zafira Tourer (2012 -) Equipment. Available at: <http://www.parkers.co.uk/cars/reviews/vauxhall/zafira/tourer/equipment/> (Accessed: 6 February 2016).
12. Parkers (2013) Vauxhall Insignia (2013 -) Equipment. Available at: <http://www.parkers.co.uk/cars/reviews/vauxhall/insignia/country-tourer/equipment/> (Accessed: 6 February 2016).
13. Pioneer <http://www.pioneer-car.eu/eur/products/sph-da120> (no date) (Accessed: 6 February 2016) SPH-DA120.
14. ReviverSoft '.etx File Format', Available at: <http://www.reviversoft.com/file-extensions/etx> (Accessed: 11 February 2016).
15. RightConnections <http://www.rightconnections.co.uk/canbus> (no date) (Accessed: 3 February 2016) CANBus.
16. Stevens, T. and Goodwin, A. (2010) Antuan Goodwin. Available at: <http://www.cnet.com/roadshow/news/a-brief-intro-to-obd-ii-technology/> (Accessed: 3 February 2016).
17. Vauxhall (2016) Vauxhall OnStar. Available at: <http://www.vauxhall.co.uk/onstar/index.html> (Accessed: 6 February 2016).
18. Williams, J. (2012) ACPO Best Practice Guide for Digital Evidence. Association of Chief Police Officers. Available at: http://www.digital-detective.net/digital-forensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 6 February 2016).