Digital Data Extraction for Vehicles Forensic Investigation

Corey Stathers
Cyber Technology Institute
De Montfort University
Leicester , UK
corey.stathers@googlemail.com

Musa Muhammad
Cyber Technology Institute
De Montfort University
Leicester, UK
musa.muhammad@dmu.ac.uk

Adebamigbe Fasanmade
Cyber Technology Institute
De Montfort University
Leicester, UK
alex.fasanmade@dmu.ac.uk

Ali Al-Bayatti
Cyber Technology Institute
De Montfort University
Leicester, UK
alihmohd@dmu.ac.uk

Jarrad Morden
Cyber Technology Institute
De Montfort University
Leicester, UK
jarrad.n.morden@gmail.com

Mhd Saeed Sharif
School of Architecture, Computing and Engineering, UEL
London, E16 2RD, UK.
s.sharif@uel.ac.uk

Abstract - **In a criminal investigation, vehicles are quickly becoming another crucial source of digital evidence. When a car is involved in a criminal offensive such as road traffic accidents, drunk driving even a robbery or a terrorist attack, investigators typically focus on the capture of DNA, fingerprints, and other non-digital identifying materials. (e.g. calls, contacts, messages, pictures, videos and even web history). This paper is to present our findings undertaken on a 2008 Mitsubishi colt with non-factory fitted equipment which in the 2000s many drivers wanted extra comfort while driving to their own music and even connect the mobile device to their vehicles to call others. By using Mobile forensic techniques and On-board Diagnostics (OBD) software to read the vehicles engine status we can show what data is stored within a vehicle and if there is enough to support a case. This Investigation involves a Maxtek Dashboard camera, Ankeway Head unit, the ECU within the vehicle, a Samsung galaxy Android tablet and it's our goal to show the techniques used to show the different types off data receivable from the vehicle mentioned.**

Keywords – Data extraction: Android device; ECU Data; OBDII port; XRY; XAMN; Autopsy; Hacking; Smart Cities; Smart Devices; Dashboard Camera

I. INTRODUCTION

The procedure of locating evidence within vehicles, often known as automotive, has advanced significantly over the years, from swiping prints or scanning through number plates. Prosecuting lawbreakers has gone from being a simple forensic investigation to a highly complex one due to technological advancements [1]. Additionally, as automobiles become more technologically advanced, digital investigators must be more versatile in their approach to locating evidence within the vehicles from now and in the future. As autonomous vehicles become more popular, they will provide an enormous amount of value in digital investigations. It is estimated that 1.35 million people are predicted to die each year as a result of traffic collisions as the number of cars on the road increases [2]. 1.5 million vehicles were recalled in 2015 due to cybersecurity issues. Within the same year, a Jeep was involved in an accident after its engine was remotely deactivated while the driver was stuck in traffic. [3]. Vehicle forensics is an increasing method that police investigators are increasingly adopting, as vehicles can reveal roughly as much information as a smartphone [4]. Sometimes criminals can get away with the crimes commit as there was not enough evidence. This new method off retrieving data maybe the answer which modern day investigators need to put a water-tight case together against a criminal to convict them off their crimes.

When we think of the internet of things, we think of smartphones, cameras, televisions, smartwatches, gaming consoles, and amazon/google speakers, but not of vehicles.

Vehicles are a critical component of the Internet of Things and of smart city planning. The public use vehicles for domestic use as well as the transportation sectors for a variety of purposes, including improving quality of life, moving commodities, and travelling across long distances for vacations, work, and other reasons. The main contribution of this paper provide three solutions as follows:

- Provide cost-Effective way off extracting data from a vehicle showing the techniques used to complete the investigation as well as the tools used.
- The actual data Extracted from the vehicle by using the basic techniques described in this paper.
- A detailed description of data produced by 3 components within a vehicle

II. LITERATURE REVIEW

A. Computer Systems within vehicles

There are several devices in modern day vehicles that assist with everything from, traditional driving to a pleasurable drive, yet they are all admissible as evidence. These are computerized components that operate in conjunction with the engine to maximize efficiency. Which in turn allows the engine to create the maximum amount of power necessary to move the car along the road. Then there's the entertainment system, which includes a radio to listen to music and in some parents install tablets which are integrated into the back headrests. Additionally, airbags, E-call, and factory assistance are included in some cars and the devices keep logs which again can be used as evidence. However, many of these devices are volatile, which means that if the power to the device is cut off, no data can be retrieved from them. Finally, some insurance companies put black-boxes in their customers vehicles to monitor their driving. This is to improve the price the customer pays for their insurance, this device includes built-in GPS monitoring, monitors how they brake and accelerate which this data is then fed back to the insurance company as well as sending this data to the customer's phone. A comparable system called digital tachograph used by lorries and heavy machines requires drivers/operators to scan their machine card to start the engine, the machine will take the name on the card to establish if the operator is permitted to use the equipment.

A.i. Engine Computers

Engine control units (ECU) are chips used by the many computers in the vehicle to make the car function. The car's nervous system is a system called, a controller area network (CAN bus), which connects all the sensors to many ECUs installed in a vehicle. The system can send up to 10 megabits per second to each network node. The ECUs are the nodes, and current cars can have up to 70 ECUs. CAN buses are straightforward, inexpensive, completely centralized (one point of entry), extremely durable, and efficient.

Cloud computing and the advent of the internet of vehicles (IoV) in the future will necessitate the adaptation of CAN buses. These nodes will be able to communicate with traffic lights, smart highways, and smart cities in addition to the cars in which they are installed; certain cars are equipped with E-call, an emergency call system that broadcasts information about accidents to the emergency services. Following that, the crash data recorder (CDR) will save the details of the accident which can then be investigated just like a planes black box. These CAN-buses are a critical component of the automotive industry's next step toward autonomous driving.
Automobiles, buses, trucks, and heavy gear such as cranes all contain these networks.

A.ii. Driver Entertainment Computers

Cars have had basic entertainment such as radios in them since the 1930s, However, it was not until the 2000s when car manufacturers - installed Bluetooth and GPS navigation which became a very common occurrence. This was a significant advancement for the automobile industry and digital investigators, as these devices included data that may aid in case resolution. The hard discs in these stereos were used to store GPS data and contacts. Newer head units save data such as music, contacts, home addresses, last visited destination, photographs, movies, and bank account information on the cloud (particularly for Android-based head units), and use Bluetooth to link individuals [6]. These android head units are simply tablets/ smart phones but on your dashboard.

B. Recovering Data of Head Units

To extract data from head units, you can use a device called a Jtag, which attaches to the circuit board of the head unit and communicates to a computer through USB. The Jtag can be used in a method called chip off, in which the memory chip is removed and placed on a circuit board designed to power and extract data from it. The Jtags is desirable because it preserves the unit, however removing and replacing the chip may cause the chip to fail which would lead to a costly repair or even in some cases a new unit all together. Some boards come with pre-installed Jtags; however, you may need to solder cables to the Jtags, and you will need to use a Jtagulator to discover the proper connectors. The issue with using this type off method is that you need extensive knowledge within this type off data extraction or you will damage the unit or the chip.

C. On-Board-Diagnostic (OBD)

On-Board-Diagnostics (OBD) ports are classified as either OBD or OBD-ll. OBD-ll is now a standard since the port's initial purpose was to manage the electronic fuel injection system. However, because nothing happens when the engine is turned off, it now provides information about the vehicle when it is working. Cars with carburetors (abbreviated as 'Carb') did not require OBD because it was all mechanical, but electronic fuel injection requires the use of a system to regulate the combustion process in the engine. These ports are mostly positioned on the driver's side of the vehicle, directly beneath the driver's steering wheel (Some different car manufacturers place this port in a different place though). These are now a standardized system that enables external devices to communicate with vehicles in order to diagnose issues, reprogram the engine such a remaps. Many modified car enthusiasts do this to chuck flames out of the exhaust or to save fuel as well as to unlock the vehicle's performance by altering the air and fuel mixture in order to increase speed while also increasing the amount of power produced by the engine. Certain manufacturers are even developing dongles that convert the OBDll port to a wireless port [6].

D. The Framework of the Internet of Vehicles

The internet of things, big data systems, and a variety of sensors are all used to fuel the future of smart cities. Automated Vehicles intercommunicate with city towers with data processed to make smart decisions. The goal of 'Smart' technology is to create something that is dependable and solves problems which us humans do every day, such as slow down if theres traffic, completely stop if there are pedestrians waiting to cross and ect... When we talk about smart cities, we talk about smart places that employ technology to provide services and address problems in real time, whether it's traffic or waste reduction [7]. However, we will only look at the Vehicles and Technology side of things. For example, connected vehicles, often known as smart vehicles, are employed by the vehicle to vehicles (V2V) and the vehicle to infrastructure (V2I) networks. V2V communication delivers data wirelessly between vehicles, whereas vehicle to infrastructure communication sends data from the vehicle to the environment around it, such as traffic lights, sensors, parking allocation, remote diagnostics, and telematics. The V2I communicates using an ad hoc network and powerful management technologies to make the decision. V2V, on the other hand, communicates through vehicle networks [8]. Dynamic networks, multi-protocol networking, and tamper-resistant packaging are the three types of network topologies used within in these types of environments.

Dynamic Network Topology refers to the fact that a vehicle can join or exit the network at any moment and from any location. When people join or depart a network, it becomes dynamic. Unfortunately, digital forensic technologies are not built to manage such changes in order to examine them**.** Multi-Protocol Networking is a term that refers to automaitcally communicating over an ad hoc network using non-IP protocols. They could also be connected to the cloud via the IP networking protocol at the same time. It is tough for digital investigators to discover a means to take into considerations all of the properties of multi-protocol in order to produce readable logs. The Tamper Resistant Packaging Topology is used to prevent forensics support on the network during a criminal investigation. The concept is that unattended roadside devices are placed on the side of the road, but these devices are equipped with anti-tamper packaging to prevent cyber-attacks [9].

E. Critical Analysis

We have covered the basics of what digital forensics is and what it entails in this Review. Many of the sources we have looked at have done and stated similar things to ourselves. If we have a firm grasp on the fundamental concept of the Internet of Vehicles, whether it is smart cities or a simple case study documenting what they did to get the hardware out and what they wanted out of it, we can build a report on the subject. Many of these sources refer to the internet of vehicles and smart cities, which is crucial given that everything is connected, from the road to the car, via traffic signals, to the cities itself. Everything, from vehicles that are connected to one another to cars that are connected to infrastructure [9]. The proposed Trust IOV goes into detail regarding how the system works and how attackers can get access to infrastructures and systems in order to install malicious code and view data that is not intended to be viewed. On the other hand, the Smart vehicle forensic case study employs a more physical approach to locating data on the vehicle's system [1]. To summarize, our initial thoughts on the subject of 'Digital Vehicle Forensics' are that it is becoming a much more necessary topic than it was previously, and that the subject is becoming increasingly desired as more vehicles incorporate more technology, and that it is critical that we are prepared for when it is required. Is it better to have an older car with no trace of connectivity if you prefer privacy or is it better that everything/ ayone can know your next move. Without technology, you are regressing, as all of this technology exists to aid in the system's progress while also making our lives more efficient and convenient.

We can also gather from the research completed that no one has yet explained what data can be retrieved from a modern day vehicle and how it can be done with a cost effect method. This paper is here to fill the gap to increase the knowledge off digital forensics in a new way.

III. EXPERIMENTAL DESIGN

During this project, we used software which we haven’t used before but having the knowledge prior to know how this type off investigation should be conducted, we can have a firm grasp on the final desired outcome. GUYMAGER, OBD auto doctor, and EOBD-Facile are among the software included within this investgiation. On the contrary, we have previously utilised VirtualBox, Kali, XRY, XAMN, and Autopsy, all of which were chosen based on our prior expertise with other applications and operating systems. Finding software capable of creating images of the dashboard camera and the head unit was critical. The initial goal was to use the FTK imager, but due to a lack of access to this software, an alternate was needed. Kali Linux is a Linux distribution that is specifically designed for digital forensics and penetration testing, as discovered through studying. Kali Linux comes with digital forensics tools preconfigured, which was just what was needed for this investigation. The Kali Linux version used was 2020.4, which was the most recent version at the time this investigation began. VirtualBox version 6.0.24 was used to generate the virtual machine, which was then used to produce an image of the devices. On Kali Linux, the imaging software used was GUYMAGER version 0.8.12. Due to the multi-threaded pipeline design and data compression, this software is extremely fast and has a very user-friendly interface.

Autopsy version 4.17.0 was used to analyse the image obtained by GUYMAGER. The initial plan was to finish the imaging and analysis on the Kali virtual system, but the.dd file was rejected by the Linux version of Autopsy. By creating a shared file on the host machine, the image file from the dashboard camera was sent to the host machine, which was a Windows. The autopsy software on Windows can then be used to investigate GUYMAGER's.dd file.

It was possible to do a car analysis via the OBD port, by utilizing applications such as OBD auto doctor and EOBD-Facile. This necessitated the use of both hardware and software. This inquiry need us to purchase a OBDII male conection to USB converter. The EOBD-facile programmed was initially ran, but it was incompatible with the car because there were only a limited number of profiles from which to choose, and the car was not one of them. EOBD-facile, on the other hand, can mimic what when a vehicle is attached as a proof of concept and to show people what the software can do but still not quite what we needed. The next step was to switch to Auto Doctor, which provided more promising outcomes. Because this programe was simply an evaluation version, OBD auto doctor was not the best option, however, it was still possible to use the software for certain activities, but not to its full capabilities. For the purposes of this project, this was acceptable as we want to see how much data can be retreived. Using XRY version 9.3, an image of the device was produced. It was then used in conjunction with XAMN version 5.3 to inspect the images created. The reason for using this software over free software is that it is readily available. The experiment also adhered to the Association of Chief Police Officers' (ACPO) principles.

V. ACPO Guidelines

When digital evidence is to be utilised in court, it must be handled with the utmost care and attention, as defined by the ACPO guidelines. The primary criterion is to prevent modifying data, which can be accomplished using a write blocker. Since generating an image of the device includes working with a duplicate rather than the original, the dashboard camera can be considered under the first rule. In legal practise, a write blocker would be utilised; unfortunately, this resource could not be secured, hence a write blocker was not conceivable. Other pieces of evidence, on the other hand, must be handled in accordance with the second guideline due to data changes and the fact that imaging android devices requires the device to be turned on, which modifies the device's metadata. The third rule is to maintain an audit trail and to evidence everything you do. This proves that the evidence was properly handled and who had it at the appropriate time. Concurrent notes were created for all devices, including the head unit, the ECU port, and the dashboard camera. Only the chain of custody paperwork for the head unit and dashboard camera were prepared, as the OBDII port gathers live data and so is not evidence. One way around this is to complete a vehicle seizure form that would be used in practise.

VI. COLLECTING THE EVIDENCE

The most critical element of an investigation is gathering evidence, as one false step could result in the case being dismissed in court due to faulty evidence. Following the ACPO guidelines is critical for a successful inquiry, as previously stated.

There have been complications that were beyond our control during this project/investigation; yet, the evidence taken from the vehicle was legally obtained because the vehicle is in our ownership. Data could be retrieved from two of the three targeted evidence sources. While the dashboard camera and ECU port gave the data which was desired, the android stereo head unit was unable to communicate with the laptop. This may be because the USB A cable connecting the PC to the head unit cable was damaged (this cable was purchased specifically for this project), the type of software used to extract data from the device is incorrect, or the USB A extension cable connecting the head unit to the USBA on the computer was damaged.

A. Vehicle ECU Port

The memory capacity of automotive ECUs is limited; as they can only store fault codes and not much else. This means that if you're driving down the road and a light comes on your dashboard, you'll be able to see a fault code via the OBDII connector and a light on your dashboard. This data is volatile because it can only be extracted from the ECU when the car is running or ignition. The below picture is the 2009 Mitsubishi Colt, which was used in the research.

Figure 1: Mitsubishi colt used in the research.

The OBD-II port in this vehicle is located underneath the steering wheel on the driver's side; there is a trim panel covering it that can be removed for easy access. Every vehicle has a separate location for this port. Some are in the glove box on the passenger's side, but finding the port is simple if you consult the vehicle's user handbook or go online. In this case, the panel was held in place by two fasteners underneath the steering wheel, adjacent to the driver's left knee. After locating the OBD port, the software OBD auto doctor was used to establish a profile for the vehicle. Some vehicles are listed in the software database, but this one was not. The car was fitted with a generic Mitsubishi profile that was then tweaked to fit the vehicle. The next stage was to get the vehicle to communicate with the laptop after building a profile. The OBD adapter was plugged into the laptop and the automobile, and the programme took care of the rest. When the software recognises the vehicle, it displays a message indicating that it is a new vehicle, and after you click OK, the software will automatically configure for a new car. After this stage is complete, the analysis can begin.

B. Dashboard Camera

By constructing a virtual computer on Kali Linux, an environment was created for the creation of a DD images of the dashboard camera. After connecting the dashboard camera to the desktop and then transmitting the camera's signal directly to the virtual machine, the virtual machine did not see the dashboard initially because the host saw this device first and we didn’t tll the virtual machine to see it. But by reconfiguring the virtual machine it observed it immediately. While the camera was imaging, a case was constructed using the Linux version of Autopsy, and once the evidence was added, it became a waiting game until GUYMAGER completed the imaging process. After the second imaging operation was done, the file was added to Autopsy. The image file was then moved to the shared drive of the virtual machine, which is also connected to the host. Following that, the evidence was imported into Autopsy's Windows version, which accepted the same file as the Linux version did.

C. Stereo/ Head Unit

The android head unit was the most essential piece of evidence in this car for this endeavour. These head units feature Bluetooth connectivity and pair with the user's or driver's smartphone. They offer GPS, music, previous locations, home addresses, videos, and photographs, in addition to the standard features of a tablet or phone. This type of evidence is critical to an investigation, and this one made extensive use of it. Because prior research suggested that it was doable and we had previously achieved it, the objective was to utilise the same programme that imaged the dashboard camera to scan the head unit. With this in mind, we began the process of retrieving data from this device.

The first step was to confirm that the gadget was in developer mode, which by default enables USB debugging and enables the user to tailor the device to their exact requirements. Developer mode is accessed by repeatedly touching on the build number. To locate the build number, navigate to settings -> about device (for this device, about vehicular platform) -> build number. The device was then linked by USB A to a laptop. The virtual machine was then used in the same manner as the dashcam was previously.

The dashcam was immediately visible on GUYMAGER, but not the head unit. After testing all connections, the head unit would not connect to the laptop. A study was conducted on the use of ADB tools. ADB tools enable a developer to connect to and modify a device remotely, either wired or wirelessly. These utilities were installed and then executed. When all the procedures are finished, the device should appear in the ADB devices list; but, after numerous attempts, the laptop was unable to locate the head unit.

VII. EVALUATION ANALYSIS & RESULTS

A. Dashboard Camera

To begin examining this device, it was determined that it records in 5-minute intervals. The files then self-destruct. Due to the device's self-erasing nature, it was expected to detect only one or two deleted files, if any at all. However, upon closer inquiry, it was discovered that this was not the case. After the data was sorted by the software, the file types were reviewed to determine if anything other than videos were identified during the imaging process. Autopsy can offer a summary perspective of the investigation's origins. This device has five videos, as well as 66 additional unknown files.

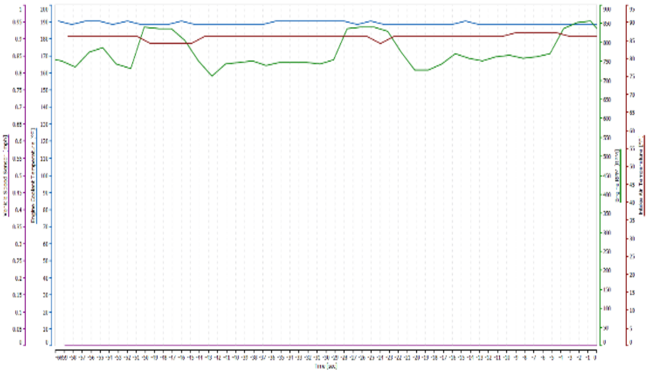
Due to the fact that this is a dashboard camera and not a standard camera, its principal function is to continuously record, which means that no images will be discovered on this gadget. The software identifies only five readable videos, with the remainder being erased or overwritten. Further analysis revealed that the five videos discovered had been reduced to three, with the last two files (_ME00084.mov and _ME00056.mov) unable to be viewed. WKA and EME are the two sorts of files. EME stands for Encrypted Media Extension and WKA is for Weak Key Authentication. The software's videos can be viewed on any video player. The videos can be viewed using the built-in Windows Films and TV Player software. The device has 56 erased files on it. This is due to the fact that the ‘deleted' files are not actually removed. This informs the device that the space used by the file in the storage can be freed and used to store other data by previous education this makes perfect sense. This does not always work because the camera will pop up while driving to format the memory, which is inconvenient, and if an accident occurs, the camera's evidence will be lost. The software displays the hash values of files, their position on the storage device when they were last edited, as well as the file type and size. The range of sizes is 0 to 660751759. The image below depicts how this appears during autopsy. There was also unallocated space on the device. This is empty space that cannot be written to because it does not have a partition. In other terms, it is a place in an operating system that does not exist. The entire storage capacity is 2.13GB (2 decimal places). While looking over the subheadings, it's worth noting that there were 18 email addresses, which seems excessive for a camera that has no connection to the internet. A search of these putative email addresses revealed that they were actually random strings, not email addresses. Autopsy searches for email addresses using the '@' symbol and it was for this reason this was flagged.

B. Vehicle ECU Port

After establishing the investigation for the ECU port, a second party drove the vehicle to acquire readings from it. Due to the vehicle's limited number of digital gadgets, it was thought that little data would be recorded; yet it's fascinating to see what the programme revealed.

The study began with the ignition switched on in order to observe the car's idle behaviour. The graph below illustrates the vehicle's idle appearance. The purple line indicates the vehicle's speed is zero miles per hour (stationary), the blue line indicates the engine coolant temperature is approximately 186–190°F, the red line indicates the air intake temperature is approximately 83–86°F, and the green line indicates the engine RPM (Revolutions Per Minute).

Figure 2: OBD-Auto Doctor map reading when the vehicle is idle



A path was planned for the investigation that included pausing at traffic lights, going above 30 mph, hill starts, stopping for a while, and then returning to where we started. Because the graph could not be saved using the free version of the software, screenshots had to be taken at various points within the journey. Some areas included the vehicle exceeding 30 miles per hour. A strong uphill hill start was also included. The vehicle was halted for a while to see how the car reacts being stationary for a while after driving. The analysis of the graphs at 2 points of the journey will be examined in further depth.

Stopping at a traffic light as well as normal driving is included in graph below. The graph illustrates that the engine coolant temperature stays around 188°F after the vehicle has been running for a while. Unless the engine is stressed, once a vehicle reaches operating temperature, it usually stays there. Deflated tyres, travelling up a hill, varied road textures, the weight of the vehicle, and if it is towing something could all cause stress on the engine.

The graph also indicates that as the vehicle's revs rise, so does its speed, and that as the vehicle's rpm fall, so does its speed. The revs drop rapidly from 1800 RPM to 700 RPM as the graph reaches 22 seconds. When the vehicle's clutch is disengaged, something occurs. The vehicle's engine then resumes its idle state. Although the vehicle will not stop without breaking, you can see that it is slowing down steadily due to friction.

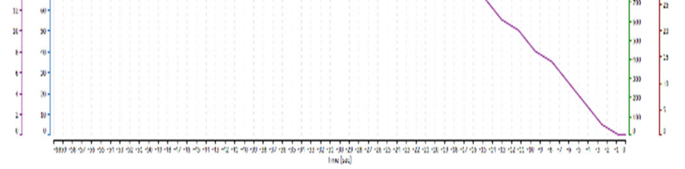


Figure 3: OBD-Auto Doctor graph reading while driving normally

On the map above, point 6 shows the vehicle's appearance after completing a difficult junction leading to a hill start and then completing it. Figure 4 shows a graph that demonstrates how the vehicle speed lowers when the clutch is disengaged, and because we were on a hill, the revs and speed were steeper than on a flat road or a gentler slope. The car shifts gear from 23 seconds to 1 second, as shown by a brief break in revs.

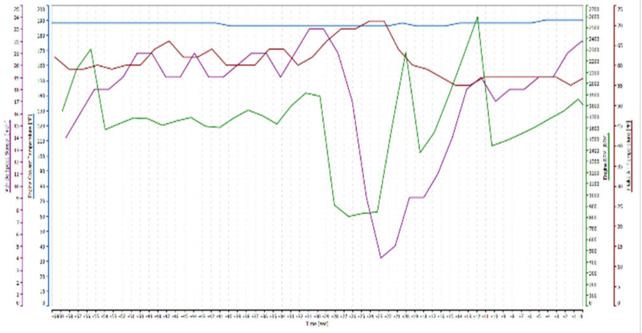


Figure 4: OBD-Auto Doctor graph reading while completing a hill start

From this ECU analysis, we can see that the software continuously displays the vehicle's speed, engine temperature, and the temperature of the air being sucked into the engine. If the full licence for the software had been obtained, the oxygen and fuel mixture could also have been plotted on the graph.

C. Concept of analysis against the android device

Due of the difficulty of obtaining software and connecting the head unit to the laptop, this component of the inquiry was deemed to be a concept. Following some research and watching clips on the internet, it was revealed that an android tablet resembles an android stereo head unit quite a bit. This created an image of a tablet running the XRY software. The tablet, which was empty of data, was provided by the De Montfort University (DMU) cybersecurity centre. Before the inquiry began, the tablet was used to simulate a head unit in a vehicle. The inquiry would begin with this configuration, which included watching YouTube videos and use Google Maps.

C.I. Imaging

Using the XRY programme, an image of a Samsung GT-P5100 running Android 4.2.2 was produced (version 9.1.2). A profile for this specific tablet was used to extract the image. However, because the software did not produce the desired findings, the process was repeated, this time using a generic android profile, and the data required for this stage of the inquiry was obtained. To be able to image the tablet, the debugging option had to be turned on. On this device, searching for the build number is similar to searching for it on the head unit. The developer mode is activated by repeatedly tapping the build number of the device seven times in the about device settings. The developer menu becomes visible after this step is completed, USB debugging can then be enabled

After imaging the device, the XRY file can be analysed with the XAMN application, which organises the evidence in subviews and categories such as Autopsy. As previously stated, the head unit shares a significant amount of capability with a tablet. The Android head unit is capable of streaming videos from YouTube, Netflix, and Spotify, as well as receiving Bluetooth photographs and, under certain circumstances, snapping images (if you had an extra camera fitted). The tablet from which the photograph was taken had been factory reset. The day before the study, a path around Leicester city centre was created using the tablet in the typical manner to replicate the head unit of a vehicle. Despite the fact that the trail did not directly follow highways, it provided a good overview of the area. The generic information retrieved using the XRY software was examined initially. In the subview general information, the manufacturer of the device and the international mobile equipment identity (IMEI) number are presented. A sim card slot was present on this gadget, but it was not used for this inquiry. If a SIM card is utilised, however, the software will be able to access call logs and texts. The device's serial number and random strings are also displayed in the subview.

The investigation then turned to the accounts that this device used. To download specific apps from the Google Play Store, you must first create an account. You must also log into these apps before you can use them. This device has a dedicated account for this project, which can be found at dmucybercenter@gmail.com. The next step was to examine the images on the gadget. Photos can be seen in a different window in the XAMN viewer. 35495 images, including icons and images, were discovered by the software. Additionally, the software extracted and analysed the device's web history. This may be deemed critical evidence in a court of law because it provides investigators with the information necessary to conduct and organise their investigation. Additionally, investigators will be able to determine which networks the gadget is connected to. This evidence may be used to establish a suspect's connection to a crime. The device used DMU's guest network, as well as another device hotspot dubbed the Honor 20, were also shown, along with the password used and when they were used. Additionally, the device logs events such as system upgrades, system crashes, and device resets and reboots; the log file records the type of event, the time, and the date.

GPS is also included in a head unit with a built-in satnav. This is another important piece of evidence since it can reveal if the vehicle/device was at a specific location. This information is not entirely accurate, but it provides a fair ballpark estimate. A more accurate reading can be obtained if Google Maps and the device are both fully updated with new GPS location tracking and software upgrades from the appropriate venders. This experiment demonstrates that a device's position can be determined. To determine the location, the software uses latitude and longitude to pinpoint a location but again it’s not as accurate as it could be due to it being an outdated device.

Finally, this tablet, like all Android devices, can save music and audio files. Figure 28 illustrates when the audio file was updated and added, the file's size, the location of the file via the path, and the file's hash value. This audio view contains music, voice notes, ring tones, and the following file types: mp3, Wav, and Ogg. Ogg is a file format similar to MP3 but with additional compression.

VIII. EVALUATION AND COMPARISON

As stated earlier, the idea of digital vehicle forensics is becoming increasingly needed due to all the data and evidence which is available from newer vehicles. While researching this project we came across an article called ‘Smart vehicle forensics’ by Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang Raymond Choo. [1] This paper excellently discussed challenges with vehicle data forensics which this paper was published in June 2018. Their idea of Digital vehicle forensics was a very hands-on approach where they removed devices from the vehicle such as the head unit and they themselves approached some challenges like we did. However, they took the investigation more physically to resolve an issue by removing the memory chip as they could not find a JTAG. This is a very destructive test and the goal is to find an evasive way off extracting data from such devices. Their approach was also costly as researching online, Jtagulator are roughly between £190 - £420. At the start of this investigation, we as a team wanted to create an approach which was less evasive and cost effective but reach the same or even better results. We only had the chance to retrieve only 3 devices however our techniques were cost effective and less damaging to the vehicle. The cost off our investigation came to £10 for the ODB cable. Comparing that to the extreme £420 we as a team have proved that our methodology is cost effective and can be done.

IX. CONCLUSION

The vehicle used in this project is almost ten years old and equipped with aftermarket parts. Thus, if this analysis were done on a newer, higher-specified car, there is reason to believe that further data may be collected. This experiment demonstrated evidence gathered from one vehicle out of 35,168,259 registered in the United Kingdom. Each vehicle may have fewer or more data available for extraction. [10]. What we have found is on the right track, however, to get a more accurate understanding, a larger number off vehicle is needed to further back up our theory.

From this investigation we can clearly state that a vehicle contains, videos off the driving from the dashboard camera and how the dashboard camera deals with running out of storage by overwriting already made video files in the form off EME and WKA files. The Vehicle head unit compared to the tablet shows that just as much data can be found on a head unit as a mobile. With data such Geo-location, contacts, website history, videos, music, photos, device logs and general information about the device as well as accounts on the device. Finally, the ECU, the software which was used for this investigation shows the correlation of revs and speed. When the engine has been running for periods of time, we can see that the engine becomes warmer and the temperature off the engine coolant. This project has been a success of finding a less evasive as well as cost effective way of analysing and investigating a vehicle.

REFERENCES

[1] Le-Khac, N.-A.et al., 2020. Smart Vehicle forensics: Challenges and case study. Future Generation Computer Systems, pp. 1- 11.

[2] World Health Organization, 2021. Road Traffic Injuries. [Online] Available at: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries
[Accessed 05 March 2021].

[3] Team, T. R. N., 2017. Smart Vehicles Are Vulnerable to Hacking. [Online]
Available at: https://www.danielrrosen.com/beware-of-hackers-in-your-car-system/
[Accessed 05 March 2021].

[4] Chen, C., 2021. privateinternetaccess. [Online] Available at: https://www.privateinternetaccess.com/blog/police-are-increasingly-using-digital-vehicle-forensics-to-solve-cases/
[Accessed 05 March 2021].

[5] Laukkonen, J., 2020. Lifewire - A breif history on the car radio. [Online] Available at: https://www.lifewire.com/brief-history-of-the-car-radio-534718
[Accessed 05 November 2020].

[6] Edelstein, S., 2020. Digital Trends. [Online] Available at: https://www.digitaltrends.com/cars/everything-you-need-to-know-about-obd-obdii/
[Accessed 05 November 2020].

[7] Bismart, 2019. Bismart. [Online] Available at: https://blog.bismart.com/en/what-is-a-smart-city
[Accessed November 06 2020].

[8] HereMobility, 2020. HereMobility. [Online] Available at: https://mobility.here.com/learn/smart-city-mobility/smart-city-car-connected-intelligent-integrated
[Accessed 06 November 2020].

[9] Hossain, M., Hasan, R. & Zawoad, S., Unknown. Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV), Alabama: -.

[10] Pollard, T., 2020. carmagazine. [Online] Available at: https://www.carmagazine.co.uk/car-news/motoring-issues/2020/how-many-cars-are-there-in-the-uk/#:~:text=It%20might%20be%20a%20fiendishly,1.0%25%20on%20the%20previous%20year.
[Accessed 19 April 2021].

[11] 3EF, 2021. 3EF. [Online] Available at: https://www.3ef.co.uk/contact.html
[Accessed February 2021].

[12] Alexakos, C. et al., 2021. ScienceDirect. Enabling Digital Forensics Readiness for Internet of Vehicles, 52(-), pp. 339-346.

[13] Andriod Studio, 2021. Developers. [Online] Available at: https://developer.android.com/studio/run/device
[Accessed February 2021].

[14] Android Studio, 2020. Developers. [Online] Available at: https://developer.android.com/studio/intro/update#sdk-manager
[Accessed February 2021].

[15] Android Studio, 2021. Developers. [Online] Available at: https://developer.android.com/studio/command-line/adb
[Accessed Febuary 2021].

[16] Athena Foreniscs, 2021. athenaforensics. [Online] Available at: https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/
[Accessed 24 April 2021].

[17] BD, P., 2020. HOW TO INSTALL ADB ON KALI LINUX 2020 [EASY STEPS] (Youtube). [Online] Available at: https://www.youtube.com/watch?v=IsQXyFHNGl0&list=PL0bPw2tC4JsaDoYZ1glfYsHP2Fme0Wyz8
[Accessed February 2021].

[19] Computer Security Student, Unknown. Lime Forensics. [Online] Available at: https://www.computersecuritystudent.com/FORENSICS/LIME/lesson1/index.html
[Accessed February 2021].

[20] CPS, 2019. Road Traffic: Mobile phones. [Online] Available at: https://www.cps.gov.uk/legal-guidance/road-traffic-mobile-phones
[Accessed 25 April 2021].

[21] Daily, J. S., 2019. ACM Digital Library. [Online] Available at: https://dl-acm-org.proxy.library.dmu.ac.uk/doi/10.1145/3309171.3309181
[Accessed February 2021].

[22] DFIR.Science, 2016. Youtube. [Online] Available at: https://www.youtube.com/watch?v=mqHx7HutQLo
[Accessed 3 February 2021].

[23] Digital Forensics, 2021. Digital Forensics Corp. [Online] Available at: https://www.digitalforensics.com/blog/how-to-make-the-forensic-image-of-the-hard-drive/
[Accessed 29 January 2021].

[24] DIGITPOL, 2021. DIGITPOL. [Online] Available at: https://digitpol.com/contact-us/
[Accessed February 2021].

[25] IACP, 2021. Law Enforcement Cyber Center. [Online] Available at: https://www.iacpcybercenter.org/prosecutors/digital-search-warrants/
[Accessed 24 April 2021].

[26] İbrahim Gülataş, S. B., 2018. DOAJ. [Online] Available at: http://dergipark.gov.tr/jnse
[Accessed February 2021].

[27] Johnson, J., 2014. On the Digital Forensics of Heavy Truck Electronic Control Modules. SAE International journal of commercial vehicles , 7(1), pp. 72-88 .

[28] Kopencova, D. & Rak, R., 2020. IEEE Xplore. [Online] Available at: https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/9293516
[Accessed February 2021].

[29] Lohrum, M., 2014. Free Android Forensics. [Online] Available at: http://freeandroidforensics.blogspot.com/2014/08/live-imaging-android-device.html
[Accessed February 2021].

[30] nidirect, 2021. nidirect. [Online] Available at: https://www.nidirect.gov.uk/articles/police-procedures
[Accessed 24 April 2021].

[31] Source Forge, 2021. GuyMager. [Online] Available at: https://guymager.sourceforge.io/
[Accessed February 2021].

[32] Encase Forensic, 2018. User guide. -: Guidance Software.

[33] Feng, X., Dawam, E. S. & Amin, S., 2020. A New Digital Forensics Model of Smart City. -, pp. 1 – 6

[34] Forensic Science Investigations Ltd, 2017. 3EF. [Online] Available at: https://www.3ef.co.uk/vehicle-data-forensics.html
[Accessed 05 November 2020].

[35] Larson, U. E. & Nilsson, D. K., 2008. Securing Vehicles against Cyber Attacks. Tennessee, Unknown.

[36] Nelson, B., Phillips, A. & Steuart, C., 2010. Guide to Computer Forensics and Investigations. Boston: Course Technology.

[37] Nilsson, D. K. & Larson, U. E., 2008. A Roadmap for securing Vehicles against Cyber Attacks, Synopsys: Research Gate.