Digital Vehicle Forensics

by Eoin A. Bates, P.Eng.

INTRODUCTION

Common challenges in all investigations involving motor vehicles are establishing what happened, when it happened, where it happened and who was involved. Preserving all available evidence in a timely manner, including digital evidence, can often prove crucial to the development of future investigative leads and successful results. The newly emerging field of Digital Vehicle Forensics provides investigators with the capability of preserving a wide range of digital evidence from motor vehicles, and will become increasingly utilized in vehicle related investigations over the next decade.

WHAT IS DIGITAL VEHICLE FORENSICS?

Digital Vehicle Forensics involves the acquisition and analysis of digital data (digital evidence) from motor vehicles. Sources of digital evidence in a motor vehicle can include:

1) Event Data Recorders (EDR),
2) Telematics/Infotainment Systems,
3) Key Fobs,
4) Dash Cams (Front & Rear) with data storage capability,
5) Self-Driving and Autonomous Vehicle ECUs (electronic control units) with data storage capability,
6) Other ECU's that store data in the vehicle
7) After-market technology with data storage capability.

The most commonly used source of motor vehicle digital evidence, the EDR (also known as the vehicle "blackbox"), was introduced in the mid 1990's and is present in almost all new cars sold in North America. Typically, the EDR is triggered when the vehicle is involved in a collision. It generally records 5 seconds of precrash data, as well as data during the course of the collision. EDR data acquisition technology and analysis methods are well known. The EDR can provide an excellent source of digital evidence for collision reconstruction investigators but often is limited in relevance in vehicle theft, vehicle fraud or other vehicle related investigations. Key Fobs are increasingly becoming a potential source of useful digital evidence. Remote keyless entry systems and smart key systems can potentially store a range of investigative data such as VIN, time and date stamps as to when the key was last used, odometer reading of when the key was last used, and other types of data. Depending on who is requesting the data, and why it is being requested, data may be acquired through the local vehicle dealership, or using key fob forensic software. Whereas all the above listed sources of digital evidence should be considered in any investigation involving a motor vehicle, digital evidence from the Telematics/Infotainment System will likely have the most impact on vehicle related investigations over the next decade. Almost all motor vehicle manufacturers now incorporate some level of embedded Telematics/Infotainment System into their new vehicle designs. Sales of new cars equipped with these systems are projected to increase from 35% in 2015 to 90% in 2020 and approaching 100% in 2025.

WHAT ARE MOTOR VEHICLE TELEMATICS/ INFOTAINMENT SYSTEMS?

The word 'Telematics" is a combination of the words "telecommunications" and "informatics". Telecommunications involve the transmission of information physically (for example, electrical wiring) or wirelessly (for example, using radio waves in Wi-Fi or Bluetooth™ devices). Informatics relates to the science of processing data for storage and retrieval. As such, motor vehicle Telematics/Infotainment Systems have the capability to send, receive and store data. The term "Infotainment" is a combination of the words "information" and "entertainment". In the context of the motor vehicle, infotainment relates to the delivery of information and entertainment via the dashboard touchscreen, steering wheel controls, voice controls, Bluetooth™, Wi-Fi, USB devices, SD cards or other means that an occupant uses to connect with their digital environment.

ACCESSING DATA FROM EMBEDDED TELEMATICS/INFOTAINMENT SYSTEMS

Embedded Telematics/Infotainment Systems have been evolving in the motor vehicle industry over the last 30 years. For example, the 1st_generation of General Motors OnStar® was released in the mid 1990'S (the 10th_generation is the latest release on the market). Ford introduced Navigation Radio in the early 2000's, and the first SYNC® system in 2007. The quantity of data stored in these systems can vary significantly from one manufacturer to the next. A single manufacturer may provide many different Telematics/Infotainment Systems across their range of vehicle models.

Many types of data may be stored. This data can be categorized broadly into Vehicle/ System Information (Serial Number, Part Number, Original VIN, Build Number); Installed Application Data (Weather, Traffic, Facebook, Twitter); Connected Devices (Phones, Media Players, USB Drives, SD Cards, Wireless Access Ports); Navigation Data (Tracklogs, Trackpoints, Saved Locations, Previous Destinations, Active and Inactive Routes, Velocity Logs); Device Information (Device IDs, Calls, Contact, SMS, Audio, Video, Images, Access point Information) and Events (Doors Opening/Closing, Lights On/ Off, Bluetooth Connections, Wi-Fi Connections, USB Connections, System Reboots, GPS Time Syncs, Odometer Readings, Gear Shifts, Hard Braking, Hard Acceleration, Traction Events, Distracted Driving Warnings, and other events) Until 2014 these systems were relatively inaccessible to investigators.

Physical acquisition of the data from the system at the chipboard level or utilization of "chip-off" techniques that have been proven reliable in smartphone digital forensics were possible but not commonly carried out due to the lack of vehicle system forensic tools available. To address this problem, US based company Berla Corporation released their iVe™ Vehicle System Forensic toolkit in 2014. As the first of its kind on the market, the iVe™ Vehicle System Forensic Toolkit provides a vehicle look-up database to determine if a specific vehicle is supported for data acquisition; a toolkit and instructions for data acquisition (figures 1a-1d) ; and data analysis software. Importantly to note, even though released in 2014, the iVe™ software supports vehicle acquisitions for some models as far back as 2007. Depending on the vehicle model, the data acquisition file size can be greater than 25 GB. Acquired data is typically time-stamped with a GPS location. Data spanning many years can be stored and it is not uncommon to have multiple devices associated with a single system, reflecting who may have connected their device to the vehicle over it's lifetime. Such historical logs may provide crucial insight in investigations where other sources of evidence have been difficult to access.

EXAMPLE

For example, since 2007, Ford have introduced four systems with various types of data accessible using the iVe™ toolkit; the Ford Navigation Radio, the Ford Sync 1 released in 2007 (currently provided in some new vehicle models), the My Touch Ford® from 2012 to 2015 (also referred to as the Ford Sync 2), and the Ford Sync 3 released in 2015, and provided in some new vehicle models. By comparing the quantity and types of data available from the SYNC® 1 and SYNC® 3 systems, we understand that some systems will contain significantly more data than other systems. For example, data commonly available from the SYNC® 1 can contain useful information such as unique Bluetooth addresses for connected phones, phonecall logs (incoming, outgoing and missed) and SMS text messages; and some vehicle events. No Navigation data is stored in the SYNC® 1. In comparison, the SYNC® 3 can contain both unique Bluetooth and Wi-Fi addresses for connected devices; phone logs (incoming, outgoing and missed) and many types of time stamped (with GPS location) for vehicle events including if Apple CarPlay™ was enabled, if Android Auto™ was enabled, Bluetooth™ connections, device connections, doors (open/close), driver distraction alerts, gear shifts, hard acceleration, hard braking, traction, media, odometer, USB connections and Wi-Fi connections. In addition, the SYNC® 3 can include navigation data such as locations, routes, track logs and velocity logs. In addition to data stored in the vehicle, some data is likely transmitted from the vehicle and stored remotely in the "cloud" (collected by manufacturers, insurance companies or other third parties).

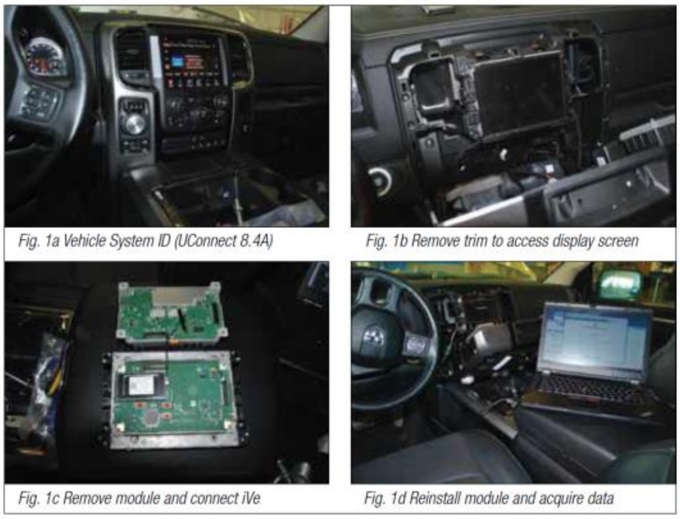

Fig. 1a Vehicle System ID (UConnect 8.4A)

Fig. 1b Remove trim to access display screen

Fig. 1c Remove module and connect iVe

Fig. 1d Reinstall module and acquire data

Figures 1a – 1d In-vehicle data acquisition of 2015 RAM 1500 UConnect 8.4A

This data has also become an increasingly valuable source of digital evidence. Ability to gain access to this data may vary depending on who is seeking the data and for what purpose. It is likely that an insurance company may be able to share this information with their in-house investigators. In other cases, the data may be available to law enforcement using appropriate judicial authorizations and production order requests to telecommunications, motor vehicle manufacturers, insurance companies or other third parties.

THE FUTURE OF DIGITAL VEHICLE FORENSICS

The evolution of Telematics/Infotainment Systems, combined with the evolution of other motor vehicle technologies such as self driving and autonomous systems, will present many opportunities and challenges in investigations involving motor vehicles in the future. The quantity and range of different data types available to investigators will likely increase significantly. The auto theft investigator will be presented with a number of new theft scenarios where digital data will become increasingly important in their investigation. As self-driving and autonomous vehicles gain popularity, theft of these vehicles by methods such as remote hijacking will likely increase. As vehicle functions become increasingly digitalized, the risk of ransomware type attacks against the vehicle computer system may also become increasingly common place. Digital evidence of remote hijacking and vehicle related ransomware attacks will likely exist in both the vehicle systems and stored remotely in the cloud. Acquisition and analyze of this data will be important to investigators and to motor vehicle security professionals defending against such attacks.

The evolution of blockchain as an underlying technology for managing motor vehicle data may also provide many opportunities and challenges for investigators in the future. In May 2018 BMW, Ford, Renault and GM joined MOBI (Mobility Open Blockchain Initiative), a working group focused on the role of blockchain in the automotive industry in the future. It is currently unknown how this new technology will impact the motor vehicle industry, or what specific attributes of blockchain may be applicable to motor vehicle related investigations.

CONCLUSION

Acquisition and analysis of digital data stored in a vehicles Telematics/Infotainment System can provide investigators with important digital evidence to establish what happen, when it happened, where it happened and who was involved. With some vehicle models over 10 years old now being accessible using the iVe™ Vehicle System Forensic Toolkit, it would be beneficial for investigators to establish what types of digital data may exist on a case by case basis, as early as possible in their investigation.

REFERENCES

(1) Bortles, W., McDonough, S., Smith, C., and Stogsdill, M., "An Introduction to the Forensic Acquisition of Passenger Vehicle Infotainment and Telematics Systems Data," SAE Technical Paper 2017-01- 1437, 2017, https://doi:10.4271/2017-01 -1437. (2) Vandiver, W. and Anderson, R., "Accuracy of Speed Data Acquired from FordSync Generation 2 and Generation 3 Modules Utilizing the Berla iVe System," SAE Technical Paper 2018- 01-1442, 2018, https://doi.org/10.4271/2018-01-1442.