Vehicle Conveniences Drive Criminals to Prison

By Stephen Murphy, DC3 Public Affairs

Modern vehicles contain upwards of 75 computer systems to aid with driver safety and provide conveniences such as remote access, location assistance, Bluetooth and Wi-Fi connectivity.

(Photo courtesy of Consumer Reports)

Infotainment systems include Bluetooth and Wi-Fi connectivity, Global Positioning System (GPS) and application interfaces. The DC3 Cyber Forensics Laboratory currently conducts about two vehicle infotainment system forensic examinations each year in support of Defense Criminal Investigative Organization customers and other DoD agencies.

No matter how much drivers may love and rely on these computer-enabled features, they are not advantageous to those who use the vehicles for criminal activities. Vehicle computer systems record and store data, and wherever there is data, there is opportunity for digital forensic examiners to locate, extract and analyze it to help determine where, how and by whom a vehicle has been used.

“Vehicle systems store a vast amount of data such as recent destinations, favorite locations, call logs, contact lists, SMS messages and the navigation history of everywhere the vehicle has been,” said Special Agent Bill Dent, DC3 CFL Director of Operations. “Many systems record events such as when and where a vehicle’s lights are turned on, and which doors are opened and closed at specific locations.”

Individual vehicle computerized components in vehicles are typically subparts of two overarching systems - telematics and infotainment. Telematics systems include features such as notification of vehicle collision and emergency calling. Infotainment systems include Bluetooth and Wi-Fi connectivity, Global Positioning System (GPS) and application interfaces. Through accessing and analyzing the stored data, forensic examiners are often able to identify devices that have been connected to infotainment systems via the USB ports, via Bluetooth or wireless networks, and all of the data associated with those devices including smart phones, tablets, laptops, etc.

“Traditionally, vehicles were used to transport the suspects to and from the crime scene, and occasionally became [crime scenes themselves] as a result of criminal activity,” said DC3 CFL

Acting Director Mike Ricucci. “Forensic evidence was obtained through conventional techniques such as fingerprinting, fiber analysis, and possibly hematology or toxicological methods. The electronic sophistication of the average vehicle now makes an automobile a treasure trove of real-time data. Devices such as accelerometers and GPS tracking can provide speed and location information which could be used as an information source. Potentially, this could refute or bolster the testimony of a witness or suspect."

(Photo courtesy of the Department of Homeland Security)

Modern vehicles contain upwards of 75 computer systems to aid with driver safety and provide conveniences such as remote access, location assistance, Bluetooth and Wi-Fi connectivity. The average vehicle today has 150 million lines of code and generates more than 25 gigabytes of data per hour.

The CFL currently conducts about two vehicle infotainment system forensic examinations each year in support of Defense Criminal Investigative Organization customers and other DoD agencies. Such examinations have been conducted in support of cases involving suspected crimes against children, sexual assault and murder.

Dent said the most common method of retrieving data from a vehicle is to remove the infotainment system and send it to the lab for examination. The CFL uses the “iVE” forensics hardware and software toolkit created by the Berla Corporation in nearby Annapolis, Md. The iVE forensics tools support examiners by providing a method of tapping into a vehicle’s data systems to find, organize and analyze a vast range of information.

“Currently, the Berla tool is one of a few tools to analyze infotainment systems,” said Dent. “The other method would be to disassemble the infotainment system and do an individual ‘chip-off’ reading of the stored data.”

Vehicular infotainment forensic examiners require specialized training outside of the normal realm of digital media forensics. Removing an infotainment system from a vehicle is intrusive and requires a significant amount of time and effort.

“Not only do you need the training on the tool from Berla, an examiner also needs to know how to access and remove the infotainment system from the dashboard area of a vehicle,” said Dent. “Great care is needed not to damage the vehicle in the removal process. Another risk is to ensure the unit is not damaged during shipment to the laboratory.”

Removing infotainment systems to acquire data is not the only challenge examiners face. According to the SANS Institute, a recognized firm specializing in information security and cybersecurity training, the lack of standardization regarding infotainment/telematics systems creates a need for forensic tools that are highly adaptable to the various types of systems found in today's vehicles. Unlike aviation data recorders used in crash investigations, which must comply with government data type and storage specifications, infotainment/telematics systems are not subject to standard requirements. It is common for data storage methods to vary significantly from one vehicle manufacturer or model to another.

Another common challenge is to be able to understand if data is missing or not present on the infotainment system.

"The lab had a case where there was no data recorded on the date of a murder," said Dent. "A separate examination of a laptop computer belonging to the suspect's girlfriend revealed he searched the Internet on how to disable the GPS/infotainment system of his vehicle before he committed the murder."

Dent further explained that the suspect was an active duty Air Force member who sought to murder his ex-wife. The CFL examination of the infotainment system revealed his vehicle's travel history from when the suspect left his home in North Carolina to a location several miles away from the crime scene in Florida, where the suspect disabled his infotainment/telematics systems. The fact that the systems had been disabled raised a red flag with examiners at DC3. This is not something the average person knows how to do. It also suggested the suspect was desperate to conceal the location of his vehicle.

The red flag led to an examination of a laptop belonging to the suspect's girlfriend. Examiners acquired data which revealed the suspect's Internet search for methods to disable his telematics and infotainment systems. It also revealed searches for plastic containers, acid, ways to dispose of a human body and maps of local areas suggesting where the suspect believed it would be best to do so. The data acquired from the infotainment/telematics systems and the laptop provided compelling evidence in support of the U.S. Air Force Office of Special Investigations case and helped put a murderer behind bars.

According to Berla, the average vehicle today has 150 million lines of code and generates more than 25 gigabytes of data per hour. Research from the SANS Institute estimates the average driver spends over 700 hours driving per year. This equates to more than 18 terabytes of data being generated per driver, per year.

As infotainment and telematics systems continue to evolve, so does digital forensics. Less than a decade ago, examiners were technologically limited to forensic tools that only worked with a handful of infotainment systems from a few automobile manufacturers. Since then, the growth of forensic tool scope has been dramatic. In 2016, the most advanced tool was able to support more than 3,400 vehicle models and today it can support more than 6,700 globally.

For more information on the DC3 Cyber Forensics Laboratory, go to https://www.dc3.mil/digital-forensics.