Forensic Acquisition and Inspection of Aftermarket Vehicle Infotainment Systems

Jett Brandes*, M.S., Joshua Brunty, Ph.D., Andrew Lewis Clark IV M.S., Robert Boggs, WVSP
Marshall University Forensic Science Graduate Program, 1401 Forensic Science Drive, Huntington, WV 25701

Abstract

Many modern vehicles contain infotainment systems that provide users with access to features such as Apple CarPlay, Android Auto, bluetooth audio, and radio, among others. These systems were introduced in 2015 and have been standard in the car industry since 2021. For vehicles manufactured before 2015 or those that do not come equipped with infotainment systems, aftermarket options are available, allowing individuals to purchase and replace their original equipment manufacturer (OEM) stereo. Popular brands offering aftermarket infotainment systems include Sony, Pioneer, and Google. These infotainment systems are designed to pair with an individual's phone, facilitating data transfer between the mobile device and the vehicle through either a wired or wireless connection.

This presentation focuses on popular aftermarket infotainment systems. While it has become a new standard for the car industry, many vehicles lacking "upgrade packages" and older models do not come equipped with infotainment systems featuring Android Auto or Apple CarPlay. In such cases, individuals often opt to purchase these aftermarket options. Various applications are offered such as music apps, contacts, and text messaging through the infotainment system. Android Auto also provides a developer option that allows the addition of extra text messaging apps like Skype, Whatsapp, and Facebook Messenger. Additionally, some apps have the capability to record GPS data, such as Google Maps, Apple Maps, and Waze.

Introduction

When you think about vehicles in forensics your mind probably goes to fingerprints, DNA, or accident reconstruction. An often-overlooked part of the vehicle is the computers in it. Infotainment systems can store user data that helps show who mobile device was connected to the vehicle. A few companies such as Berla support some infotainment systems depending on the make and model of the vehicle. The issue with this? They do not explore into aftermarket infotainment systems which can easily replace OEM infotainment systems.

A vehicle owner can swap to an aftermarket infotainment system for various reasons such as their vehicle's infotainment system is outdated, or they want to upgrade to a better one. These aftermarket systems, same as newer OEM, offer built in Android Auto and Apple Carplay which can make traveling more convenient and comfortable. We explored into the forensic acquisition of an aftermarket Google, Pioneer, and Sony infotainment system using In Series Programming (ISP) and coded readers.

References

1. Shin, Yeonghun, et al. "Digital Forensic Case Studies for in-Vehicle Infotainment Systems Using Android Auto and Apple Carplay." *MDPI*, Multidisciplinary Digital Publishing Institute, 22 Sept. 2022, https://www.mdpi.com/1424-8220/22/19/7196.
2. "SWGDE Best Practices for Vehicle Infotainment and Telematics Systems_v3.0.Pdf." *Google Drive*, 13 Jan. 2022, drive.google.com/file/d/1wSCuN3F-ZKifXWgXLTBja-Xs93mWpsGL/view.
3. Whelan, C. J., Sammons, J., McManus, B., & Fenger, T. W. (2018). Retrieval of Infotainment System Artifacts from Vehicles Using iVe. Journal of Applied Digital Evidence, 1(1). Retrieved from http://mds.marshall.edu/jade/vol1/iss1/2

Materials and Methods

There were two different phones used, one for Android Auto and one for Apple Carplay; a Pixel6 and an iPhone 13 were used respectively. They're three aftermarket infotainment systems used for the project. A Pioneer DMH-1770NEX, A Sony XAV-AX3250, and an Universal Infotainment System purchased from amazon. These were powered by two different 12V power sources. Text messages were sent back and forth between a Pixel6 and iPhone 13 to ensure that each infotainment system had been connected to Android Auto and Apple Carplay while receiving/sending text messages and phone calls. Text messaging occurred across multiple apps that were supported by the infotainment systems such as WhatsApp, Skype, and Facebook Messenger (for Android Auto only). The next step was to collect location data on the phones and potentially the infotainment systems. Android Auto comes with Google Maps preinstalled and Apple Carplay comes with Apple maps preinstalled. These are the default direction apps for the infotainment systems. These direction apps, as well as a third party direction app 'Waze' was used to create directional and travel data with the phones. The infotainment systems were hooked up in the car based on the following method. A power inverted was plugged into the cigarette lighter of a vehicle, which a 12V power supply was plugged into the power inverter, the infotainment system was then connected to the power supply to ensure that the infotainment system was powered. Directions were then typed into Google Maps, Apple Maps, and Waze for a variety of locations in which the vehicle traveled to. Approximately 50 trips were taken total between the three directional apps.

For the infotainment systems we investigated the memory chips attached to each board. The Universal Infotainment System contained a NOR flash memory chip designated as cFeon QH64A-104HIP. The Sony infotainment system contained two Winbond 25Q128JVSQ NOR flash memory chips. The Pioneer infotainment system contained a TC58CVG1S3H NAND memory chip.

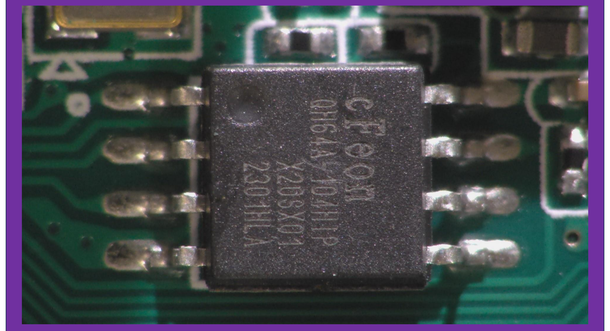
A device called a Revelprog, which is a code reader, was used to read the Universal and Sony systems as it supported those chips. We used a method called In Series Programming (ISP) to attempt to pull data from the chip but were unsuccessful with both chips.

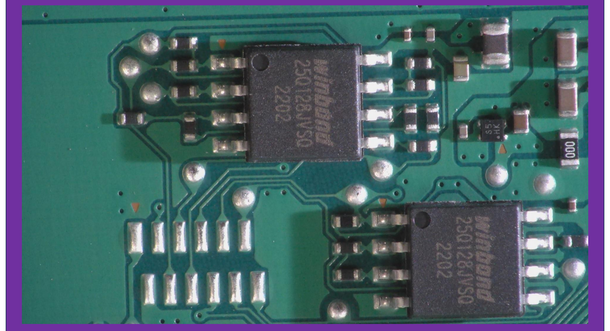
Another device called Dediprog was purchased which is another coded reader. This device supports the Sony and Pioneer memory chips.

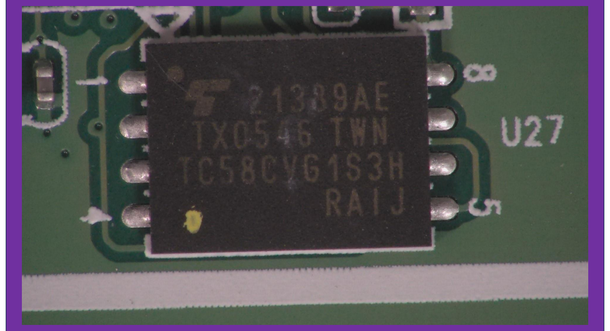
A heat gun was used to unsolder the memory chips from the board after the unsuccessful ISP attempts. Socket adapters were used for each coded reader that helped read the specific memory chips.

With the TC58CVG1S3H removed from the board. The chip was placed into the adapter in the Dediprog. The Dediprog graphic user interface (GUI) was pulled up on a computer. The TC58CVG1S3H was selected in the program. The Read ID was clicked to ensure that the Dediprog could recognize the flash memory chip which was successful. The Read button was clicked in the software. After approximately five minutes the flash memory chips contents were displayed in hexadecimal format in a new window. From this new window, a binary file was created and saved with the contents. This same procedure was done with the Universal Infotainment System with the QH64A-104HIP chip. The contents were also saved as a binary file.

The Winbond 25Q128JVSQ memory chip was placed into a 200-208mil SOP8 adapter for the Revelprog. After powering up the device and loading the software. The Winbond 25Q128JV chip was selected in the GUI options. The voltage level was set to 2.8 volts as per the datasheet a blank test was conducted to ensure that the flash memory chip had contained data. The read button was then selected and the data from the memory chip was displayed on the Revelprog GUI. This data was saved into a bin file. Since the Sony infotainment system had two memory chips that were the same brand; this process was completed the example same for both memory chips with their contents being labeled and saved to two separate bin files.







Results

The iPhone 13 was extracted using GrayKey and the Pixel6 was extracted using Cellebrite Premium. Full file extractions were able to be received from both phones.

After processing through Magnet Axiom, we were able to obtain text messages, phone calls, WhatsApp messages, Facebook Messages, and Skype messages between the two test phones. All infotainment systems were located under the 'connected devices' artifact of Magnet Axiom. They were also located on the device identifiers portion of the phone. Location data was found with Google Maps and Waze on the Pixel6. While location data was found, only 1 location was found which the Sony infotainment system was involved, and all of the Pioneer results were found. There was no direction results for the Universal Infotainment System. However, all of the Waze directions were found with the Pixel6 using Android Auto. For the iPhone 13, all trips recorded with Apple Maps were found except for 1 trip was missing that was taken with the Sony infotainment system. All Waze trips were found for the iPhone 13.

The binary files with the saved contents of the infotainment systems were placed in Binwalk.. The Universal binary file was attempted to be placed also in Binwalk, but the file was compressed, and a file system could not be located. We then moved onto the Pioneer binary file. Using Binwalk we were able to extract four file system files. The operating system of the Pioneer appeared to be Linux based. There appears to be no saved folder which stores memory from connected devices. The two binary files for the Sony infotainment system were placed in Binwalk. The first memory chip did not appear to have any operating system within the bin file. We were able to find files of the preloaded images within the memory contents. Examples of these loaded images are the Sony logo, Android Auto logo, and Apple Carplay logos. The second memory chip for the Sony infotainment system did not appear to contain any operating system or stored files on it.

Due to several limitations on the lack of knowledge of aftermarket infotainment systems we were unable to find identifiers to the mobile devices such as the MAC address, telephone number, or IMEI from the internal storage of the infotainment systems.

Future directions are to search for tools that are able to read the contents of the binary files for the aftermarket infotainment systems better than Binwalk. Artifacts from the binary files are not easily found/displayed such as artifacts from OEM infotainment systems can be easily found with the proper tools from Berla.

Acknowledgements

Special thanks to AJ Clark for helping with his knowledge on Magnet Axiom, Cellebrite, and extracting data from memory chips. The author appreciates the help from Russell Tomblin for his experience with electronics and infotainment systems. The author thanks Corporal Boggs from the West Virginia State Police for his knowledge on extracting data from infotainment systems. Additionally, the author thanks Dr. Lauren Waugh and Dr. Josh Brunty for their review, advice, and expertise.