

# Journal of Applied Digital Evidence

Volume 1 | Issue 1

Article  
2

2018

## Retrieval of Infotainment System Artifacts from Vehicles Using iVe

Celia J. Whelan

Marshall University, [whelan4@live.marshall.edu](mailto:whelan4@live.marshall.edu)

John Sammons

Marshall University, [sammons17@marshall.edu](mailto:sammons17@marshall.edu)


Brian McManus

National White Collar Crime Center, [bmcmanus@nw3c.org](mailto:bmcmanus@nw3c.org)

Terry W. Fenger

Marshall University, [fenger@marshall.edu](mailto:fenger@marshall.edu)

Follow this and additional works at: <http://mds.marshall.edu/jade>

 Part of the [Data Storage Systems Commons](#), and the [Other Computer Engineering Commons](#)

### Recommended Citation

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>

This Article is brought to you for free and open access by Marshall Digital Scholar. It has been accepted for inclusion in Journal of Applied Digital Evidence by an authorized editor of Marshall Digital Scholar. For more information, please contact [zhangj@marshall.edu](mailto:zhangj@marshall.edu), [martj@marshall.edu](mailto:martj@marshall.edu).

# Retrieval of Infotainment System Artifacts from Vehicles Using iVe

---

Celia J. Whelan\*, B.A., B.S.; John E. Sammons, M.S.; Brian K. McManus; Terry Fenger, Ph.D.

## Abstract

The analysis of mobile devices and hard drives has been the focus of the digital forensics world for years, but there is another source of potential evidence not often considered: vehicles. Many of today's "connected cars" have systems that function like computers, storing information they process including user data from devices synced to the system. There has been little to no research done regarding what types of user artifacts can be found on the system, how long these artifacts remain, whether or not the user can remove those artifacts, and whether certain systems provide more information than others. For this study, two different makes and models of vehicle infotainment systems were used for data acquisition: a Uconnect® system and a Toyota™ Extension Box. It was found that the Toyota™ system provided a significant amount of user information (contacts, call logs, media file information, and locations), while the Uconnect® system provided only locations. This indicates valuable user data can be obtained in this manner.

## Introduction

More commonly thought of sources for digital evidence are computer hard drives, mobile devices (cell phones, tablets, iPods, etc.), or gaming devices (Wii, Xbox, PlayStation, etc.), but vehicles may also be potential containers for a large quantity of valuable digital evidence [2, 3]. Recently, modern vehicles have transformed from machines of transportation to "computers on wheels," containing built-in storage, Wi-Fi connectivity, satellite radio, syncing capabilities, and the ability to communicate with other vehicles and/or infrastructures. A vehicle possessing some combination of these features, in the form of an infotainment system, is referred to as a "Connected Car" [3]. An infotainment system is formally defined as:

A factory original or aftermarket console system that uses some form of connectivity to provide drivers and passengers with vehicle specific information, navigation, and standalone or integrated applications and/or multimedia entertainment including audio and video [3].

In other words, an infotainment system is a combination of GPS, Bluetooth sync, satellite radio, Wi-Fi, etc. The system can have some combination of the aforementioned capabilities, or it can have other connection capabilities that were not previously mentioned [16]. The infotainment system is what stores any of the user data that may be transferred during a syncing process with a device and/or infrastructure, such as satellites, the Internet, and mobile devices, among others.

That stored data can either be vehicle event data (brakes applied, gear changes, connections to or disconnections from Bluetooth or Wi-Fi, etc.), navigation data (saved or recent locations, trackpoints, etc.), or user data (call logs, SMS messages, social media feeds, etc.) [4]. The field of vehicle forensics encompasses collecting and analyzing these types of vehicle data and the evidence obtained can prove just as useful in crimes involving vehicles as other types of digital evidence can in other crimes [4, 5]. The problem is that vehicle forensics is not commonly utilized because it is such a new field that attorneys, investigators, and law enforcement may not even realize the wealth of digital information cars can provide.

As these connected cars become more prevalent and more connected, there will likely be a rise in the number of digital crimes targeting vehicles, such as vehicle hacking or the use of vehicle malware. The potential for vehicle forensics to recover digital information from vehicle systems attacked in these types of crimes makes vehicle forensics that much more valuable. Further, as mobile phones collect and retain more and more personal information, manufacturers and developers are increasing the security that is placed on those mobile phones. This means the passcodes are harder to crack, the encryption is harder to decode, and thus the information stored on them is more difficult to access. But, by using Berla Corporation's *iVe*, a vehicle forensics tool, it should be possible to retrieve mobile phone user data from a vehicle if that mobile phone has been previously synced with the vehicle. It should be possible to retrieve mobile phone data from a vehicle if that phone has been previously synced with the vehicle, even if that mobile phone was password-protected and the encryption was turned on [4, 13, 14]. What many do not realize is that when the vehicle's system is used to make phone calls or send text messages, not only is that information stored in the phone and phone logs but on the vehicle infotainment system's hard drive

as well. This means it could actually be easier and less time-consuming to recover mobile phone data from a vehicle system than to recover similar data from the mobile phone itself [4, 13]. Thus, user data obtained in this manner has the potential to serve as valuable evidence in cases involving vehicles both now and in the future.

Not only can user data (e.g. texts, browsing history.) potentially be retrieved from a vehicle's infotainment system, but other artifacts may also be found on the infotainment system and can greatly assist law enforcement. Both vehicle event data (e.g. the car doors opening/closing or the car's gear state) and navigation data (e.g. GPS locations) have been previously used in court as evidence in both homicide and home invasion cases [4], and user data has the potential to serve as valuable evidence in future cases.

But obtaining user data artifacts from vehicle systems is not a simple task. Law enforcement and digital forensic examiners must go into the system themselves and acquire the necessary data; this is possible using iVe [4]. iVe is a proprietary tool developed by Berla Corporation and it is the only commercially available tool for vehicle forensics. While iVe is relatively new, the software is already stated to support data acquisition from the infotainment and telematics systems of over 4,600 models of vehicles [4, 14, 18]. iVe provides a vehicle lookup function, so as to allow the user to enter the year, make, model, trim, and style of the vehicle to determine whether a vehicle is supported by the tool. A vehicle's VIN (Vehicle Identification Number) can also be used to determine compatibility [4].

Acquisition of this user data from all of the various supported models can become complicated because all of the models of vehicle are different; thus, the acquisition method varies by the make and model of car. Once the specifics of the vehicle have been entered into iVe, detailed instructions are provided for identification of parts and ports, disassembly (if necessary), and acquisition [4]. If disassembly is required, it is detailed in such a way that the pieces should be able to be reassembled to its original condition [4, 14].

When iVe is used to acquire data from an infotainment system, either a logical or physical acquisition can be performed, which will depend on the infotainment system. Additionally, either a partial image (user data ONLY) or full image (all of the possible data) can be obtained. Regardless of the type of acquisition obtained using iVe, the acquired file can then be analyzed using iVe as well [4, 14]. The analyst can then view the information, search, bookmark, and graph

it, as well as generate a report, just as is done in other more well-known computer forensic tools such as Forensic Toolkit or Encase [4].

Berla Corporation states that iVe is capable of recovering user artifacts such as call logs, SMS messages, and connected devices [4, 14, 15, 18], but to the knowledge of the researchers, user data obtained in this manner has not been used in any adjudicated court cases to date. Additionally, there is little to no documentation regarding the amount of historical user data cached by the various infotainment systems. The amount of user data recoverable from the system and its age is a crucial aspect for law enforcement officers and investigators to be aware of. If this method of data acquisition proves successful and can give an indication of historical data on the vehicle system it could be a great asset to the law enforcement and forensic science communities.

### **Research Questions and Hypothesis**

It is the belief of the researchers that user data artifacts left on vehicles from the use of mobile phones and infotainment systems may provide valuable forensically relevant digital evidence. Additionally, it is the goal of this research to make law enforcement aware of the potential information that vehicle forensics may uncover. The following are the questions this research aims to address:

1. What user data artifacts are left behind on vehicles from the syncing of mobile phones to the vehicle's infotainment system?
2. Which of those artifacts may prove forensically relevant to law enforcement forensic investigations?
3. Do some infotainment systems yield a greater number of artifacts or types of artifacts than other systems?
4. How persistent are the artifacts?
  - a. Are user artifacts deleted when the phone is "un-synced" or unpaired from the vehicle via the on-screen interface?
  - b. Are user artifacts deleted when the "Remove User Data" function present in certain systems is used?

### **Materials and Methods**

In order to determine what mobile phone user data was recoverable from vehicle infotainment systems, data needed to be available on the systems so that researchers could note the general numbers and types of artifacts present. A generalized research protocol was developed outlining the various unpairings, data removal processes, and data acquisitions that were to be performed. This protocol was based on various published guidelines and manuals but the actual acquisitions of user data from the vehicle infotainment systems were performed as per the iVe instructions. Any acquired data was then analyzed using iVe and compared.

### **Test Vehicle Selection**

In order to use iVe to acquire user data, a compatible vehicle and infotainment system needed to be identified. In order to narrow down the list of potential candidate vehicles to a manageable number, it was necessary to narrow down the options to only vehicles that did *not* require disassembly *and* could be acquired using only a USB port. Based on this “USB only” criteria, a 2013 Dodge Dart Limited with a Uconnect 8.4 infotainment system and a 2013 Toyota Highlander Limited with a Toyota Extension Box system were chosen. The procedures outlined in the following section were followed for the syncing and acquisition processes performed on the two systems.

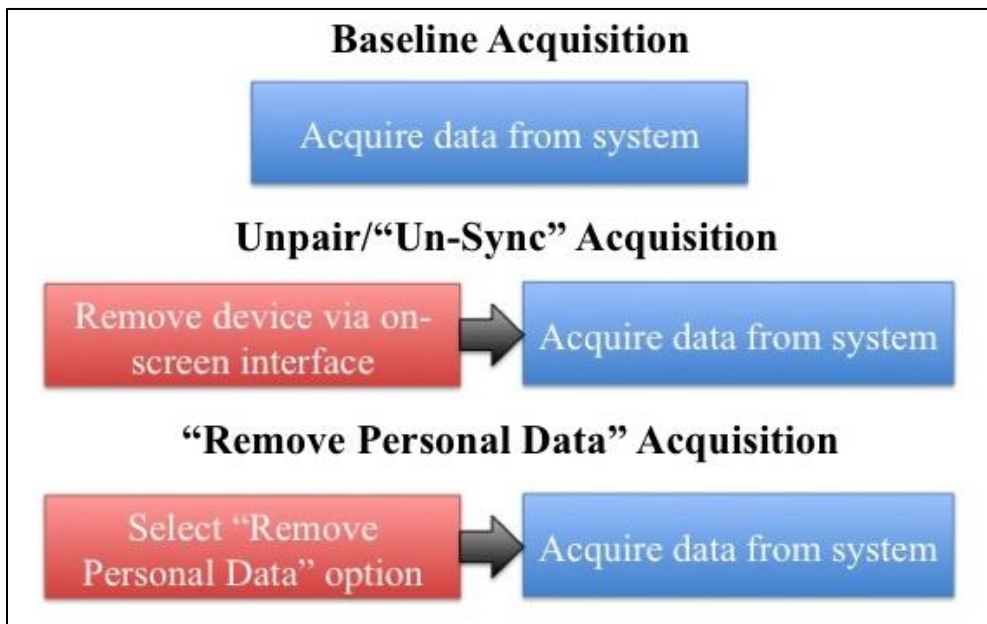
### **General Research Protocol for Device Sync and Data Acquisition**

For this project, a general method for the syncing and acquisition processes was developed and followed using the SWGDE “Best Practices for Vehicle Infotainment and Telematics Systems” [19] as general guidelines, in conjunction with the iVe user manual provided with the iVe software. This protocol was to be followed during all processes over the course of the project. The overarching pattern of the processes used in the research protocol is outlined below. The acquisition procedure details specific to each system are not described in this article as they are specific to the iVe software and only accessible with the software license.

Below, Table 2 indicates each phase of the research protocol and its objective while Figure 1 provides a visual depiction of the phase order and what occurs during each phase.

**Table 2.** *Each acquisition phase of the research protocol and its corresponding objective.*

Acquisition	Objective
Baseline	Determine what data is on the system
Unpair/“Un-sync”	Determine if/what data is made unrecoverable upon phone removal through on-screen interface
“Remove Personal Data”	Determine if/what data is made unrecoverable upon use of “Remove Personal Data” function



**Figure 1.** Visual depiction of phase order and what occurs in each phase.

Prior to any syncing taking place, a “baseline” acquisition of the infotainment system was performed to account for anything present on the system prior to our accessing the system. Following the baseline acquisition, any previously paired devices were removed from the system using the on-screen interface and another acquisition performed. Looking at this image, in conjunction with the baseline images, deduction of the user data left behind on the system upon device unpairing should be possible. It should be noted that in systems that contained a “Remove Personal Data” option, the option was selected and data was acquired again.

All of the acquisitions done on the two systems were performed using a Dell Latitude E6500 Laptop with 4 GB of RAM running Windows 8.1 Enterprise (64-bit). The version of iVe

used was 1.8.4. Additionally, all acquisitions were stored on a Western Digital My Passport Ultra 1 TB external hard drive.

## System Specific Information

### *2013 Dodge Dart*

The 2013 Dodge Dart Limited contained a Uconnect 8.4 infotainment system, referred to as “the system” in this section. Prior to any data acquisition, a visual examination was performed. Following this, a baseline image was acquired. This was done by placing the system in “dealer mode” and transferring the user data to a PNY 64 GB USB 3.0 flash drive. This resulted in a userdata.pas file, or a Uconnect Panasonic Binary file, which was imported into the iVe tool and processed. Importing this data into iVe was classified as a logical, “import” acquisition type. Once imported and processed, a case was created for the acquisition so that analysis could be performed. Hashing and indexing were allowed to finish prior to analysis.



**Figure 2.** Uconnect 8.4 infotainment system of a 2013 Dodge Dart Limited.

### *2013 Toyota Highlander Limited*

The 2013 Toyota Highlander Limited infotainment system had a Toyota extension box, which will be referred to as “the system” in this section. Again, prior to any data acquisition, a visual examination was performed. This was followed by the acquisition of a system baseline acquisition using the iVe USB acquisition kit. Once the data was collected, a case was created for the acquired data so that it could be analyzed, and hashing and indexing were allowed to complete prior to analysis of the data; this was done for each acquisition. Next, all paired devices were unpaired one-by-one from the system. Following the removal of all paired



**Figure 3.** 2013 Toyota Highlander Limited infotainment system with Toyota Extension Box.



devices, data was acquired again. It was noted that the Toyota system had an option labeled “delete personal data”; this option was not noted on the previous Uconnect system. The “delete personal data” button was selected and a final data acquisition was performed.

## **Results & Discussion**

### **2013 Dodge Dart Limited**

It was noted upon visual examination that there were three previously paired devices visibly listed on the system screen. Other than device names, there was no further user information available on the infotainment system screen. Upon analysis of the baseline acquisition and viewing of the generated report, it was seen that there were no attached devices, text messages (SMS), call log entries, or contacts identified and acquired by the iVe software. The only relevant information obtained from the Uconnect 8.4 system was a list of addresses from locations listed in the system. These addresses were also listed with their corresponding geolocation data (latitude and longitude).

### **2013 Toyota Highlander Limited**

Upon visual examination of the infotainment system, it was noted that there were three foreign (or non-test) devices listed on the screen as paired with the system. Aside from the names of the devices, there was no user information available from the infotainment system screen. Upon analysis of the acquired baseline data, there were 13 devices listed, 3 of which were those that had been noted on the system’s screen. For each of those 3 devices, there were hundreds of contacts and call logs obtained by iVe. It was noted that call logs as far back as three years (2013) could be seen in the recovered data. One of the devices was only listed with its corresponding phone version, but the other two were listed with their International Mobile Station Equipment Identities (IMEIs) and one even listed the user’s unique number Apple ID. IMEIs are important to note as they are unique numbers that identify mobile and satellite phones, giving an indication of who may own the device. For the other 10 devices, information about 22 media files was found, as well as more contacts and call logs under a device labeled “UNKNOWN.” Information about the 22 media files was from 2 different devices (11 from each device) and they were all listed as audio files. The types of artifacts found on the system and the total number of items for each type can be found below in Table 3. All of the data acquired from the test vehicles was deleted after examination and

analysis. This was done in order to maintain the privacy of the individuals whose data was synced with these systems.

**Table 3.** Type and total number of artifacts found on the background system image.

Artifact Type	Number of Records
Devices	13
Contacts	1,347
Calls Logged	603
Media	22
Locations & Addresses	18

It should be noted that 6 of the 13 devices observed from the acquired baseline data appeared to be installed by the iVe software. It was concluded that no write blocker was incorporated into the iVe hardware that was used for acquisition since writes were made to the system and no user artifacts were found to be associated with these 6 devices. This can be of concern in the forensics community because, without write blockers, writes to the system can be made, which can be considered as altering the evidence. This can be problematic in a courtroom setting as it raises the question “If the system was knowingly altered, could the incriminating evidence have not also been placed on the system?” Fortunately, almost all of the data acquired from the infotainment systems is time/date-stamped. This allows the analyst to see what the acquisition process affected and which artifacts were added by the software. In addition, detailed notes kept by the analyst can assist in identifying what data the processes affected.

Even though writes were made to the system during acquisition, this does not discount the forensic value of this type of digital evidence. This is demonstrated by the fact that mobile phone evidence is frequently used in court and writes are made to the phone systems during some mobile phone extractions and examinations. By keeping meticulous notes and documenting exactly what was done, evidence integrity may be maintained. So while the lack of write blocking is a definite downside to digital evidence obtained by iVe in this manner, it does not *appear* to diminish its value when explained properly; this cannot be said with any degree of certainty though, as more research is required. In this case, no signs of compromised data were detected but future work

would be required to help determine whether the lack of write blocking compromised the forensic value or soundness of the evidence.

Following the analysis of the baseline acquisition data, the data acquired after the on-screen removal of the three devices originally listed on-screen was analyzed. There were still 13 devices noted in the data collected although devices were no longer listed on the screen of the infotainment system. Again, 6 of the 13 devices were noted to have been placed there by the use of the acquisition software. Media file information for all 22 media files was retained on the system, as were the 18 locations and addresses, as well as their associated latitude and longitude. Additionally, the two devices that had originally listed their IMEIs no longer displayed their IMEIs, though the unique number Apple ID was still present. There were still contacts and call logs listed, but the number present was smaller than what was noted in the previous data set and the items were no longer listed according to their associated device. In terms of numbers, the total number of contacts dropped from the previously noted 1,347 to 819, while the total number of calls logged stayed consistent at 603. This means that the contacts and call logs were not removed or deleted from the system after the device was unpaired or “un-synced” from the system and that instead they were all marked as being from an “UNKNOWN” device. This is good news because it means that this type of user information cannot be easily removed from the system by the user. All of these artifacts left behind have the ability to prove extremely valuable to investigators as they search for suspects or witnesses and can also help them corroborate or disprove someone’s alibi. While the media/audio file information found on this system may not seem relevant in this case, their presence may point to the ability of analysts to recover information regarding other media files such as videos or pictures, which could prove relevant in some types of cases.

The last data acquisition on the system was performed after the “Remove Personal Data” option was selected on the system. Upon analysis of this data, it was determined that the only data type made unrecoverable when the “Remove Personal Data” option is used is the locations and addresses stored on the system. This means that by removing a device from the system **and** selecting the “remove personal data” option, only the user’s locations or addresses entered into navigation are made unrecoverable, along with phone IMEI. Other than that, the rest of the data appears to remain recoverable. Table 4 below shows this in simplified form and compares the noted artifacts from before and after selection of the “remove personal data” option.

**Table 4.** *Comparison of recovered artifacts on the Toyota Extension Box before and after “Remove Personal Data”*

	Before “Remove Personal Data”	After “Remove Personal Data”
<b>Artifacts Found</b>	Devices (IMEI, Phone version, Unique number Apple ID, Last sync)	Devices (Phone version, Unique number Apple ID, Last sync)
	Contacts (Name, Phone Number, Email)	Contacts (Name, Phone Number, email)
	Call logs	Call logs
	Media (Audio Files)	Media (Audio files)
	Locations & Addresses (latitude and longitude)	
<b>Total Number of Records</b>	13 Devices (0 noted on-screen)	13 Devices (0 noted on-screen)
	819 Contacts	819 Contacts
	603 Calls logged	603 Calls logged
	22 Media files	22 Media Files
	18 Locations	

It is possible that when the “Remove Personal Data” option was used, the locations and addresses artifacts were not removed but rather placed in unallocated space. This means the artifacts would still be on the system but there is nothing in the file system that points to that data location. It may be that the iVe software cannot find the “removed” data when a logical acquisition is performed since a logical acquisition only recovers data that is part of the file system, akin to what happens when someone “deletes” files and information on computer hard drives. In terms of a computer hard drive, a physical acquisition of the data may recover “deleted” data but a logical acquisition cannot; this may also hold true in the case of vehicle forensics.

### Comparison

In looking at artifacts recovered from each system, it is clear that more forensically relevant data was obtained from the Toyota Extension Box than from the Uconnect system. The Toyota system provided devices, contacts, call logs, audio files, *and* locations, while the Uconnect system provides only locations. Table 5 below provides a side-by-side comparison of the artifacts recovered from each of the two systems, as well as the total number of each recovered type.

**Table 5.** Comparison of artifacts found stored on infotainment systems prior to personal data removal.

<b>System</b>	<b>2013 Dodge® Dart Limited Uconnect® 8.4 system</b>	<b>2013 Toyota™ Highlander Limited Toyota™ Extension Box system</b>
<b>Artifacts Found</b>	On-screen Devices	Devices
		Contacts (Name, Phone Number, Email)
	Locations & Addresses/Routes (With latitude and longitude)	Call logs
		Media (Audio Files)
<b>Total Number of Records</b>	3 On-screen devices	13 Devices (3 noted on-screen)
	53 Locations	1,347 Contacts
		603 Calls logged
	50 Addresses/Routes	22 Media files
		18 Locations

As indicated, the Toyota system clearly provides more types of artifacts in comparison to the Uconnect system of the Dodge. But keep in mind that when the user has completed as much personal data removal as they possibly can on both systems, there will be locations and addresses left on the Dodge Uconnect system, while there will be user information such as call logs, contacts, and media files left on the Toyota Extension Box system. From this it can be concluded that the Toyota system provides more *user-specific* artifacts than the Dodge system. And while on the surface it may look like the Toyota system provides more digital evidence in general, when it really comes down to it both systems provide artifacts that could be valuable in a forensic investigation.

While both systems contain relevant digital evidence in varying quantities, the data acquisition time on each system varies drastically. As mentioned in the materials and methods section, the Dodge Uconnect system data acquisition was an import acquisition – where the user data was first transferred to a USB device before being imported into iVe for case creation, processing, and analysis. This process resulted in a 1.43 MB file, which required 15 seconds to transfer and 4 seconds to import. For the Toyota system though, a logical data acquisition was

performed. Each acquisition yielded a file 2.18-2.25 MB in size and took anywhere from approximately 13 to 16 minutes to complete. This acquisition time differential is reasonable though since the acquisitions performed on the Toyota system were full file system extractions, while those on the Dodge system were user data only. Additionally, the sheer number of artifacts obtained from the Toyota system is much greater than that obtained from the Dodge system and likely takes longer to acquire; this is supported by the notable difference in acquisition file sizes.

## Conclusions

Based on the projected proliferation of connected cars and the type of data they contain, there is a clear need for vehicle forensics. Projections from the automotive industry indicate that the number of connected cars sold is expected to rise significantly over the next two years. Statista estimates that 98% of new cars sold in 2020 will be able to connect to the internet. That same study predicts that number will rise to 100% by the year 2025 [20].

This research aimed to address four things: which user artifacts can be found on vehicle infotainment systems; which of those artifacts could be useful to law enforcement; whether any of those artifacts remain on the system once the devices are removed through the on-screen interface; and whether different infotainment systems allow for recovery of different artifacts. This study showed that devices, contacts, call logs, and media files, as well as locations and addresses could be obtained from the two different infotainment systems inspected. And all of the types of artifacts recovered during this study could prove valuable to investigators and law enforcement officers. As it was a goal of this research to demonstrate to the law enforcement and forensic science communities the need for vehicle forensics and the potential evidence that it can recover, this is an important conclusion. Additionally, it was seen that even after the user attempts to “clean” the infotainment system and remove all personal data, artifacts remained that could aid in the identification of an individual. Finally, in comparing the artifacts that were recovered from the two systems used in this study, it was established that different systems allow different artifacts to be recovered.

One concern to note is that because only certain iVe acquisition kits come with a write blocker – meaning that only certain types of acquisitions permit the blocking of writes – none of the acquisitions performed in this study used a write blocker, as it was not permitted by the extraction kits. This is clear, as the iVe software introduced 6 of the 13 devices listed on the Toyota

system during acquisition. This is of concern in the forensics community because without write blockers writes to the system can be made, thus altering the evidence. Fortunately, almost all of the data acquired from the infotainment systems is time/date-stamped, which allows the analyst to see what the acquisition process affected and which artifacts were added by the software. Even though writes were made to the system, this does not discount ability of this type of digital evidence being used in court. In light of this though, the acquisitions in this study bear repeating while using a write-blocking software in order to observe whether this has any effect on the data obtained.

With vehicle forensics being such a new and cutting-edge field, it has yet to reach its full potential. But with the number of connected cars only increasing, the amount of digital evidence that could be contained by vehicles will increase accordingly. With more research, vehicle forensics has the ability to play a major role in the future of digital forensics and could become one of the most useful mechanisms for the collection of digital evidence.

## **Acknowledgements**

The authors thank Brian McManus of the National White Collar Crime Center for his review, as well as the faculty and staff of Marshall University Forensic Science Graduate and Undergraduate Programs, especially Dr. Terry Fenger and Ian Levstein, for their time, review, and advice.

## References

- [1] Carrier B. Defining digital forensic examination and analysis tools. *International Journal of Digital Evidence* 2002 Aug.
- [2] <http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx>
- [3] TIBCO Software. *The connected car: finding the intersection of opportunity and consumer demand*. Palo Alto (CA): 2016.
- [4] Coronetto AD, LaMere B, McGee C. *Vehicle system forensics: introducing your new star witness*. *US Law* 2015 Fall/Winter.
- [5] Moos J, Davies G, Lewis E, Williams N, Gichohi B, et al. *Digital forensics for automobile systems: the challenges and a call to arms*. *International Journal of Forensic Sciences* 2016 June.
- [6] GSMA and ATKearney. *The mobile economy 2013*. London (UK): 2013.
- [7] Nilsson DK, Larson UE. *Combining physical and digital evidence in vehicle environments*. *IEEE Third International Workshop on Systematic Approaches to Digital Forensic Engineering* 2008.
- [8] Kwederis J, Boehmer G. *Cyber risks ahead for connected cars*. *Risk and Compliance Journal* 2015 May.
- [9] Capgemini. *Cybersecurity for the connected vehicle*. Paris (FR): 2015.
- [10] Greenberg A. *Hackers remotely kill a Jeep on the highway – with me in it*. *Wired* 2015 July 21.
- [11] <http://www.garykessler.net/mobileforensics.html>
- [12] <https://investigation.com/services/digital-forensics/cell-phone-forensics/>
- [13] Moran B. *A (new) way to consider getting data from mobile phones*. *BriMor Labs* 2015 Feb 11.
- [14] [https://berla.co/downloads/ive\\_datasheet.pdf](https://berla.co/downloads/ive_datasheet.pdf)
- [15] Berla Corporation. *iVe user manual*. Annapolis (MD): 2016.
- [16] *Consumer Reports*. *Navigating the electronics maze*. *Cars* 2014 Oct.
- [17] <http://gpsforensics.org/articles/tomtom/basis.html>
- [18] <https://berla.co/products/ive/>
- [19] *Scientific Working Group on Digital Evidence*. *SWDGE best practices for vehicle infotainment and telematics systems, version 2.0*. 2016 June 23.



[20] Accenture. (n.d.). Share of new cars sold that are connected to the Internet worldwide from 2015 to 2025. In *Statista - The Statistics Portal*. Retrieved June 1, 2018, from <https://www.statista.com/statistics/275849/number-of-vehicles-connected-to-the-internet/>.