sensors

MDPI

*Article*

# Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay

**Yeonghun Shin [1], Sungbum Kim [1], Wooyeon Jo [2] and Taeshik Shon [1,3,*]**

[1] Department of Artificial Intelligence Convergence Network, Ajou University, Suwon 16499, Korea
[2] Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23221, USA
[3] Department of Cybersecurity, Ajou University, Suwon 16499, Korea
* Correspondence: tsshon@ajou.ac.kr

**Abstract:** Vehicle systems have been one of the fastest-growing fields in recent years. Vehicles are extremely helpful for understanding driver behaviors and have received significant attention from a forensic perspective. Extensive forensic research was previously conducted on on-board vehicle systems, such as an event data recorders, located in the electronic control unit or manufacturer-based infotainment systems. However, unlike previous vehicles that used only manufacturer-based infotainment systems, most vehicles today are equipped with infotainment systems such as Android Auto and Apple CarPlay. These in-vehicle infotainment (IVI) systems connect to mobile devices such as smartphones and tablets. The vehicle can periodically communicate with a smartphone and thus a network outside the vehicle. Drivers can use more services in their vehicles than ever before. Accordingly, an increasing number of diverse data are being stored in vehicles, with mobile devices connected to both the vehicle and the cloud. Such data include information that can be of significant help to investigators in solving problems during forensic investigations. Therefore, forensics of IVI systems such as Android Auto and Apple CarPlay are becoming increasingly important. We analyzed various forensic studies conducted on Android Auto and Apple CarPlay. Most of the research was mainly focused on mobile devices connected through a wired USB connection. The use of wireless-based IVI systems has recently been increasing. However, the analysis of Android Auto and Apple CarPlay from this point of view is insufficient. Therefore, we proposed a forensic methodology that fully considers such limitations. A forensic analysis was conducted on various IVI systems. We also developed an IVI system forensics tool that works based on the proposed methodology.

**Keywords:** infotainment system; Android Auto; Apple CarPlay; vehicle forensics

check for updates

**Citation:** Shin, Y.; Kim, S.; Jo, W.; Shon, T. Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay. *Sensors* **2022**, *22*, 7196. https://doi.org/10.3390/s22197196

Academic Editor: Omprakash Kaiwartya

Received: 4 August 2022
Accepted: 17 September 2022
Published: 22 September 2022

## 1. Introduction

With the development of various vehicle technologies, in-vehicle infotainment (IVI) systems are rapidly changing. Current IVI systems support connectivity with mobile devices, such as smartphones and tablets, and provide various services to drivers. The structure of such systems is also changing. Previously, vehicles were installed with only manufacturer-based forms of IVI systems, such as Ford Sync. However, in addition to manufacturer-based IVI systems, Google's Android Auto and Apple CarPlay, first released in 2015 and 2014, respectively, are also being installed by default as of 2021. These systems work in connection with the driver's mobile devices. When an Android or iOS device is connected to the vehicle, Android Auto and Apple CarPlay provide a function mirroring the mobile device environment to the vehicle. This allows the driver to use apps installed in the mobile device environment on the in-vehicle display. Such IVI systems are installed in vehicles developed by most manufacturers.

The vehicle is now connected to the driver's mobile devices via the IVI system and communicates with an external network. This differs from the existing system, which only communicates various aspects within the vehicle [1]. IVIs such as Android Auto and CarPlay are connected to mobile devices and external networks, providing drivers with more information and services than ever before. However, the connection between the vehicle and mobile devices means that various information related to the driver or vehicle is transmitted between the two devices. Some of this information is stored on the IVI system or on a mobile device connected to the vehicle.

Recently produced vehicles support a wireless connection between the IVI system and a mobile device, in order to provide convenience for the driver. In the case of a wireless communication environment there is a high risk of being exposed to various vulnerabilities. For example, if a vehicle's wireless communication does not have a secure element such as authentication or encryption applied, an attacker can easily modify a message and it will be difficult for the devices to detect the modification [2]. Therefore, the importance of forensics in the wireless communication environment of vehicle infotainment systems is increasing. In addition, as IVI technology advances the scope of mobile devices forensics is expanding to include IVI, and like mobile devices, so vehicles are becoming an important source of digital evidence.

Forensic research on vehicles has been conducted from two perspectives: a vehicle on-board system, and an IVI system. Forensic research on the on-board system of a vehicle has mainly been focused on an event data recorder (EDR) existing in the form of a module inside the electronic control unit (ECU) [3–5]. Most research on IVI systems have been forensic studies on manufacturer-based IVI systems [6–11]. Some forensic studies in recent years have also been conducted on the most popular IVI systems, i.e., Android Auto and Apple CarPlay [12–15]. However, these forensic studies are limited to the internal storage of mobile devices connected to Android Auto or Apple CarPlay systems, and the wireless connections they have recently begun supporting were not considered.

As described above, Android Auto and Apple CarPlay systems work in conjunction with the driver's mobile device. The connected mobile devices communicate with the vehicle using the protocol provided by the manufacturer of each IVI system. When communication outside the vehicle is required, the network of the mobile device is used [16,17]. The modern vehicle infotainment system environment has at least one wireless connection, so appropriate acquisition methods and analysis techniques must be applied for each wireless connection [18]. Therefore, the forensic analysis of Android Auto and Apple CarPlay systems can be divided into four areas: wireless communication between the cloud and mobile devices; wireless communication between the vehicle and mobile devices; internal storage of the mobile device; and internal storage in the IVI system. However, only a forensic analysis of the internal storage of the mobile device is currently conducted, and a forensic analysis of the remaining three areas remains insufficient. As a result, a forensic case investigation may be unable to obtain important information for resolving a particular case. We therefore propose a forensic methodology for a total of four areas including the internal storage area of a mobile devices, as previously performed. In addition, various IVI systems including real vehicles are used to validate the proposed forensic methodology. Based on the forensic methodology, we developed a digital evidence acquisition tool that helps with the forensics of IVI systems. The main contributions of this study are as follows:

1. We proposed a methodology for conducting IVI forensics. The proposed methodology consists of four analysis areas: wireless communication between the cloud and mobile device, wireless communication between the IVI and mobile device, internal storage of the mobile device, and internal storage of the IVI system. Excluding internal storage of a mobile device, the other three areas of analysis are newly proposed;
2. Eight IVI systems from various vehicle vendors are used as the case studies. As a result of a forensic analysis, various digital forensic artifacts were obtained in each analysis area. The artifacts we acquired can be used as reference materials in digital forensic investigations of IVI systems;
3. We developed a tool to acquire digital forensic artifacts from an IVI system, which operates based on our proposed forensic methodology. The tool was developed using

a web-based application and automates the acquisition of digital forensic artifacts in four areas of forensics.

The rest of this paper is organized as follows: Section 2 reviews the existing research on vehicle systems; Section 3 describes the forensic methodology for IVI systems using Android Auto and Apple CarPlay; Section 4 presents case studies conducted on various IVI systems based on the proposed forensic methodology; Section 5 describes the limitations and implications of this study.; finally, Section 6 summarizes the study and discusses areas of future research.

## 2. Related Research

Forensic studies on vehicle data have been researched mainly from two perspectives: on-board and IVI systems. Forensic research of on-board systems has been conducted based on data acquired through the On-Board Diagnostic version II (OBD-II) protocol or data acquisition from storage devices such as hard disk drives (HDDs). Forensic research on IVI systems has been focused on data acquisition from a storage device such as the HDD of the IVI system, or mobile devices connected to the IVI system.

Previous studies of on-board systems have shown that vehicles store a variety of information, including the driver's habits, locations, and driving time. Colin et al. noted the cybersecurity vulnerabilities of existing vehicle technologies and the importance of forensic research [5].

According to a study by Sladović et al., the RAM of an on-board system stores information such as the acceleration and speed during vehicle operation, and the last 5 s are stored in the EDR when a vehicle crash occurs. In addition, OBD-II and ECU/EDR connection are methods used to acquire the stored data. Moreover, Bosch's Crash Data Retrieval or Berla's iVe tool can be used for acquiring data stored in an on-board system [3].

Mekki et al. noted that data stored in a vehicle play an important role from a forensic perspective. Therefore, they proposed a neural network model for identifying drivers based on data stored in the vehicle. The data used to train the proposed model are also obtained through the OBD-II protocol [4].

Various studies have been conducted using on-board vehicle systems, the results of which can be fully utilized as a basis for vehicle forensics. However, such studies have not considered the use of an IVI system.

An IVI system contains as much information as the on-board system. According to Henry, vehicle on-board systems can determine a point of impact, whereas IVI systems can show the longer-term driving habits of the vehicle's driver. Henry used Berla's iVe tool to analyze the Human–Machine Interface module of a 2015 Silverado pickup truck. Through this analysis, the author obtained various driver-related data, including a list of devices connected to the IVI system, phone calls, SMS messages, and certain GPS information [6].

In a study by Le-Khac et al., existing vehicle forensic studies were investigated, and case studies were conducted on multimedia devices of Volkswagen and BMW vehicles [10]. In a study by Lacroix et al., forensics of the first and second generations of Ford's IVI system, SYNC, were described. Artifacts such as a list of connected devices and the phone book were acquired [7].

In a study by Cohen, forensics were also conducted on the third generation of SYNC. In this case, artifacts such as Bluetooth connections and driving and location information were acquired from NAND flash and an HDD [8].

In a study by Moos et al., the applicability of commercial forensic tools was analyzed for an HDD acquired from a BMW IVI system [9].

Ebbers et al. described a forensic study of a manufacturer-based legacy IVI app. They connected with the vehicle through a mobile app provided by the manufacturer and collected personal information stored on a smartphone. Experiments were conducted on a total of 10 manufacturers and their vehicles, and various information such as the vehicle identification numbers, driver data, and recent locations were obtained by analyzing Android and iOS devices [11].

Although various studies have been researched on IVI systems, Android Auto and Apple CarPlay systems, which have recently been installed in most newer vehicles, have not been considered.

With the popularization of Android Auto and Apple CarPlay among IVI systems, the importance of forensics in this area has grown, and some forensic studies have been presented. In Hickman's Android Auto forensic study, data stored on a mobile device connected to Android Auto were acquired and analyzed. Using this method, the vehicle connection time, last location information, and Google Assistance records from Android Auto were acquired [13].

In a study by Edwards et al., a general mobile forensic technique was applied to mobile devices linked with Android Auto and Apple CarPlay, and artifacts such as the usage history and location information were acquired [12].

Following this study, Mahalik researched Android Auto connections through Bluetooth (BT) on an Android device. In addition, she analyzed various partitions in the mobile device to obtain records related to Android Auto and BT connections [15].

In another forensic study by Hickman, data stored on mobile devices connected to Apple CarPlay were acquired and analyzed, through which the vehicle linkage time and the last Siri usage record were acquired [14].

Various studies have been conducted on Android Auto and Apple CarPlay. Most such studies have applied mobile devices such as a smartphone and tablet. Modern IVI systems are connected to mobile devices, and thus forensics on mobile devices has gained importance. However, research in this area remains insufficient, and when conducting a forensic analysis of these IVI systems, consideration must be given to how they operate. The IVI system communicates with networks outside the vehicle by connecting to a mobile device. For wireless-based IVI systems, communication between each device is more exposed to the outside world. Communication between devices means that each device stores some of the communication data; however, not all communication data are usually stored on each device. Therefore, a forensic analysis of all communications in the IVI system must also be conducted. In addition, an analysis of the internal storage of IVI systems connected with Android Auto and Apple CarPlay remains insufficient.

## 3. Forensic Methodology for IVI Systems

We propose a forensic methodology for IVI systems using Android Auto and Apple CarPlay. Figure 1 represents the forensic methodology and IVI environment. The proposed forensic methodology reflects the characteristics of the current IVI environment, which consists of the in-vehicle IVI system, the driver's mobile device, and the cloud for providing IVI services. To use the IVI system, the driver must connect between the IVI system and the mobile device. There are two types of connection between these two devices: wired and wireless. A wired connection uses USB, and a wireless connection uses Wi-Fi and BT. For the communication method, different protocols are used depending on the manufacturer of the IVI. For Apple CarPlay, some communication methods are open to the public [19]. When the IVI system and mobile devices are connected, periodic communication between the two devices is conducted. This communication includes information related to the vehicle or driver, and some of this information is stored in the internal storage of the driver's mobile device or the IVI system. In addition, the IVI environment communicates with the cloud server outside the vehicle to provide application services such as navigation. This communication takes place on the mobile device. To the best of our knowledge, a vehicle cannot currently communicate with the cloud on its own.

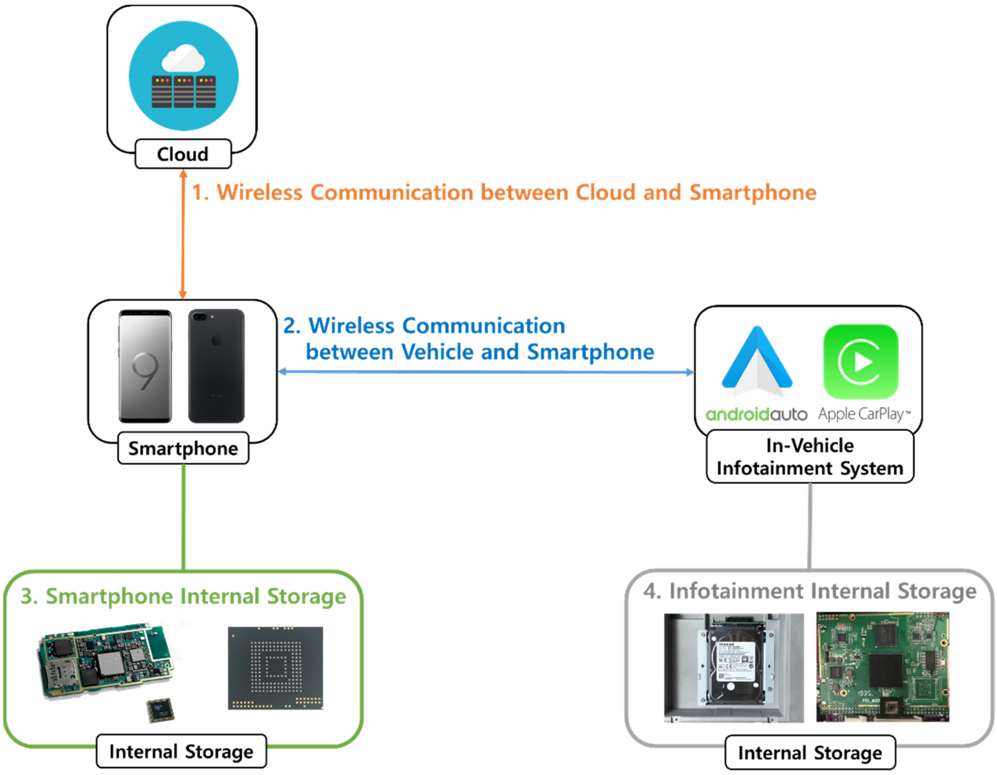

Cloud
1. Wireless Communication between Cloud and Smartphone
Smartphone
2. Wireless Communication between Vehicle and Smartphone
androidauto
Apple CarPlay
In-Vehicle Infotainment System
3. Smartphone Internal Storage
Internal Storage
4. Infotainment Internal Storage
Internal Storage

**Figure 1.** Forensic methodology for analysis of IVI system.

The above communication also includes personal information. For example, if the driver is using a navigation app, the communication is likely to include the current location or destination of the vehicle. Considering the characteristics of the IVI environment described above, we divided the forensic methodology into four areas of an IVI system are as follows:

1. Wireless communication between the cloud and mobile device;
2. Wireless communication between the IVI and mobile device;
3. Internal storage in the mobile device;
4. Internal storage in the IVI system.

### *3.1. Wireless Communication between the Cloud and Mobile Device*

IVI systems such as Android Auto or Apple CarPlay are connected to the mobile device, and the network availability of the mobile device is essential to remain online. When the vehicle and mobile device are connected, the IVI environment uses the network of the mobile device to communicate with a cloud server outside the vehicle. This communication, i.e., wireless communication between the cloud and mobile device, contains data directly related to the services used by the driver. Although unrelated to the communication between the vehicle and the mobile device, it has been proven that various artifacts can be obtained by analyzing the communication between the device and cloud [20].

Most of this communication is encrypted through the transport layer security (TLS). To analyze this, it is essential to apply a man-in-the-middle (MitM) by installing a certificate on the mobile device [21]. To analyze this communication and acquire important information, a certificate is installed on the mobile device in advance and proxy settings are configured. Web proxy tools such as Charles or Fiddler are used to acquire and analyze information on the communications.

### *3.2. Wireless Communication between the IVI and Mobile Device*

IVI systems such as Android Auto or Apple CarPlay are connected to a mobile device to periodically communicate with each other. As mentioned earlier, this communication includes information related to the vehicle or driver. From previous studies of mobile devices connected with Android Auto or Apple CarPlay, it is known that various information regarding the use of these IVI systems is stored in the mobile device. However, there is still insufficient research on acquiring and analyzing such information in the communication between two devices. An analysis of this aspect is also important from a forensic perspective because it can help in gathering a variety of information.

Wired and wireless methods are used for connecting Android Auto and Apple CarPlay systems to a mobile device, and this area of analysis focuses on the latter. In our experiments, Android Auto and Apple CarPlay use both BT and Wi-Fi for their wireless connections. Therefore, we collected and analyzed BT and Wi-Fi packets from Android and iOS devices. In addition, the packet analysis results using Android Auto and Apple CarPlay are compared with the analysis results of the connected legacy system without the application of the above IVI system. For acquisition and analysis on an Android device, Android's own featured BT Snoop and Wireshark tools are used. For iOS devices, Xcode's PacketLogger and Wireshark tools are applied.

### *3.3. Internal Storage in the Mobile Device*

Previous studies have demonstrated that mobile devices connected to IVI systems such as Android Auto and Apple CarPlay store various information related to the driver and vehicle. Therefore, we analyzed the newly added artifacts in slightly more detail using the newer versions of the IVI system applications installed on a mobile device.

In general, administrator privilege is basically required to obtain data stored in the internal storage of the mobile device [22]. Therefore, rooting of the Android devices and jailbreaking of the iOS devices were required. The internal storage was then dumped in the form of raw images, and general mobile forensic analysis techniques were applied. There is a possibility that some data will be deleted over time. Therefore, file recovery techniques must also be applied for each filesystem. Tools such as HxD, DB Browser for SQLite, FTK Imager, and the Sleuth Kit (TSK) are used for data collection and analysis.

### *3.4. Internal Storage in the IVI System*

Previous studies have demonstrated that the IVI system stores information related to a connected mobile device, the driver, or the vehicle. However, there remains a lack of forensic studies on the internal storage of IVI systems using Android Auto and Apple CarPlay. In this analysis area, the internal storage of the IVI system using Android Auto and Apple CarPlay is acquired and analyzed.

In general, the internal storage of IVI exists in the form of HDD or flash memory on a printed circuit board (PCB). If the internal storage of the IVI system uses an HDD, the data can be acquired by simply removing the drive from the vehicle. However, if the data are stored in flash memory, they must be accessed through an interface such as a Universal Asynchronous Receiver-Transmitter (UART) or Joint Test Action Group (JTAG). A chip-off may be applied as a final option if access is impossible owing to the security features of the IVI system manufacturer. As tools for data collection and analysis, HxD, DB Browser for SQLite, FTK Imager, and TSK are used for internal storage in the mobile device.

## **4. IVI Systems Forensic Use Cases**

This section describes case studies conducted on actual IVI systems based on the proposed forensic methodology. The IVI system used in the case study can be divided into vehicle systems and navigation systems. We selected 8 IVI systems considering this classification, whether they support Android Auto and Apple CarPlay, and whether they support wireless connectivity. Two of the eight IVI systems are drivable vehicles and head units acquired from vehicles; the other six are navigation systems that can be purchased online. Table 1 shows the IVI systems used in case studies and the connection possibilities on Android Auto or Apple CarPlay. Connectivity is expressed as Not Supported (not-supported connection), Wired (supported wired connection), and Wireless (supported wireless connection). For IVI systems marked as Wireless, a wired connection is also supported.

**Table 1.** IVI system used in case studies and connectivity of the IVI system.

| Manufacturer | IVI System | Android Auto | Apple CarPlay |
|---|---|---|---|
| BMW | NBT HU EVO | No Support | Wireless |
| BMW | X5 45e xLine | Wireless | Wireless |
| Chevrolet | TrailBlazer | Wireless | Wireless |
| Pioneer | AVH-Z5050BT | Wired | Wireless |
| Sony | XAV-AX5000 | Wired | Wired |
| TTEC | D5 | Wired | No Support |
| RASPBERRY-PI | Raspberry Pi 3B (Crankshaft) | Wired | No Support |
| Belsee | Best Aftermarket Auto | Wired | Wired |

Table 2 shows the mobile devices and tools used in the experiment. Smartphones were used as the mobile devices connected to the vehicle. A Samsung (Suwon, South Korea) Galaxy S9 with Android 10 and an Apple (Cupertino, CA, USA) iPhone 7 with iOS 13.3.1 were used. Figure 2 shows six of the eight test IVI environments configured by connecting an IVI system and a mobile device (from top left: TTEC (Englewood, CO, USA) D5, Raspberry Pi 3B, BMW (Munich, Germany) NBT HU EVO, Pioneer (Bunkyo City, Tokyo, Japan) AVH-Z5050BT, BMW X5 45e xLine, and Chevrolet (Detroit, MI, USA) TrailBlazer).

We tried to generate the same experiment data from the case studies of all IVI systems. After connecting the IVI system and the mobile device, we used the contact synchronization, phone calls, SMS messages, and use of the navigation application.

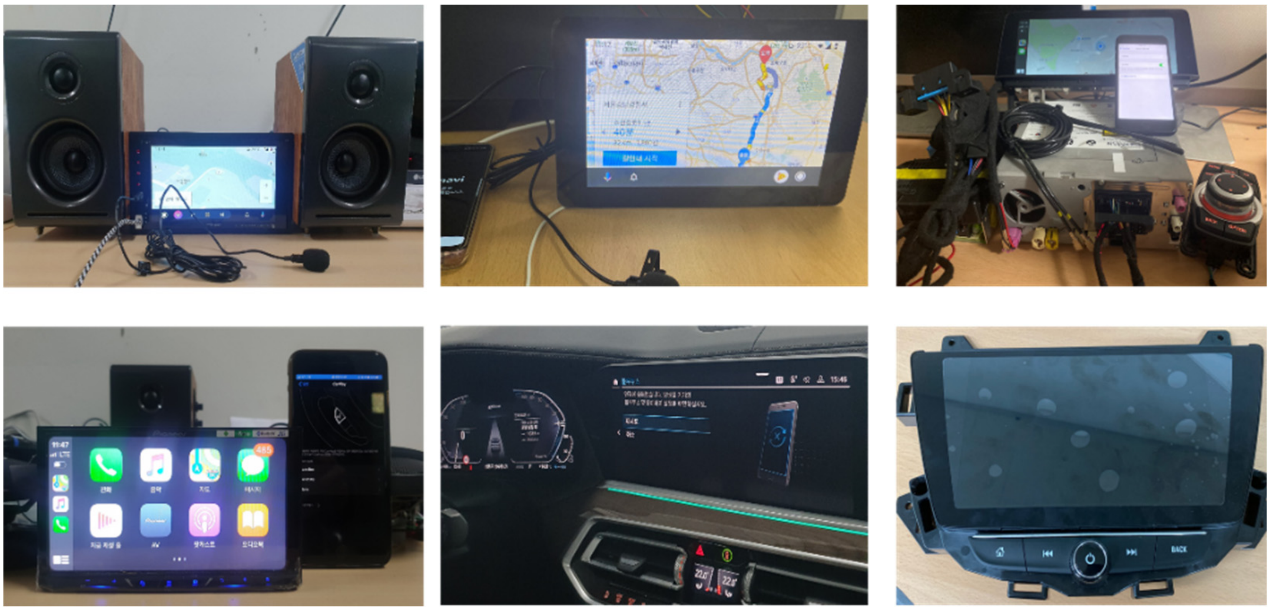


**Figure 2.** Test IVI environment for forensic analysis.

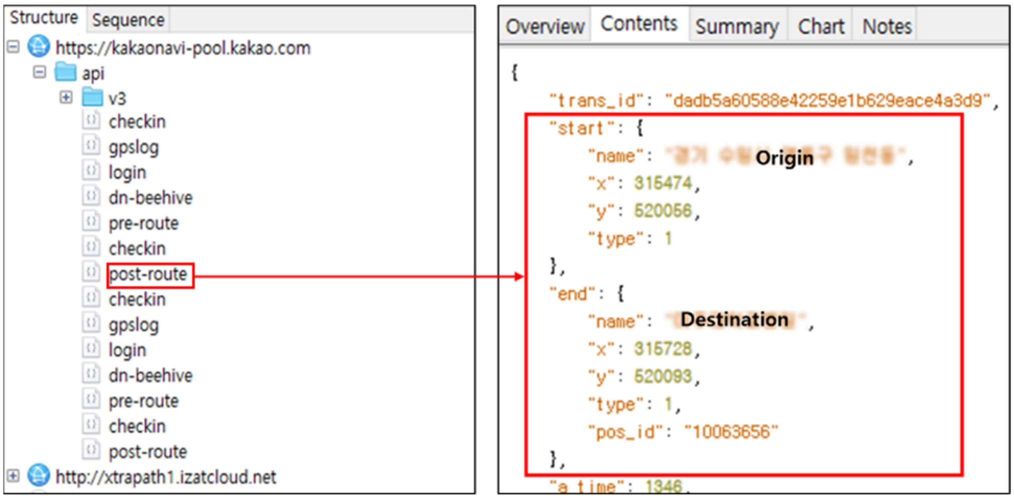
**Table 2.** Specification of mobile devices and software used in case studies.

| Manufacturer | Mobile Devices and Software | Version |
|---|---|---|
| Samsung | Galaxy S9+ | Android 10 |
| Apple | iPhone 7 | iOS 13.3.1 |
| Google | Android Auto [16] | 7.1.614573 |
| Apple | Apple CarPlay [17] | Depends on iOS version (13.3.1) |
| Crankshaft | Crankshaft [23] | csng-alpha 5.1 |
| The Wireshark team | Wireshark [24] | 3.4.0 |
| Apple | PacketLogger [25] | 7.0.0 |
| Sublime HQ Pty Ltd. | Sublime Text 3 [26] | 3.2.2 |
| sqlitebrowser | DB Browser for SQ Lite [27] | 3.10.1 |
| Karl von Randow | Charles Web Debugging Proxy [28] | 4.5.6 |

### 4.1. Wireless Communication between the Cloud and Mobile Device

The way a mobile device communicates with the cloud server differs depending on the connection method applied between the IVI system and the mobile device. When Android Auto and a mobile device have a wired connection, the mobile device communicates with the cloud server using Wi-Fi or Long-Term Evolution (LTE), and when connected wirelessly with the mobile device, the mobile device communicates with the cloud server using LTE. Regardless of whether Apple CarPlay and the mobile device are wired or wirelessly connected, the mobile device uses LTE to communicate with the cloud server. However, the MitM-based web proxy tool operates based on the Wi-Fi communication and does not support MitM for LTE communication. Therefore, this experiment can only be conducted using Android Auto. We collected and analyzed the Wi-Fi traffic of an Android device communicating with cloud servers. To apply MitM to Android smartphones, we referred to various previous studies [29–32]. A Raspberry Pi 3B with Craftshaft and TTEC's D5 IVI systems were used for this experiment.

We collected Wi-Fi traffic before the IVI system and the mobile devices were connected, after they were connected, and until the test data were generated. As a result of the analysis, no traffic types related to contact synchronization, SMS messages, or phone calls were identified. However, when the direction function of the navigation application was executed, we obtained traffic communication with the cloud server of the navigation application, as shown in Figure 3. This includes content that can determine the origin and destination of the driver. Some navigation application manufacturers may have stored this information [33–35].



```
⊟ https://kakaonavi-pool.kakao.com
    ⊟ api
        ⊞ v3
          checkin
          gpslog
          login
          dn-beehive
          pre-route
          checkin
          post-route
          checkin
          gpslog
          login
          dn-beehive
          pre-route
          checkin
          post-route
⊞ http://xtrapath1.izatcloud.net
```

```
{
    "trans_id": "dadb5a60588e42259e1b629eace4a3d9",
    "start": {
        "name": [redacted] Origin [redacted],
        "x": 315474,
        "y": 520056,
        "type": 1
    },
    "end": {
        "name": [redacted] Destination,
        "x": 315728,
        "y": 520093,
        "type": 1,
        "pos_id": "10063656"
    },
    "a_time": 1346,
```

**Figure 3.** Communication traffic of navigation application.

As a result of the analysis of wireless communication between the cloud and mobile device, four artifacts are acquired from the traffic of the navigation app: origin name, destination name, origin coordinate, and destination coordinates. Detailed artifacts are listed in Table 3. However, the artifacts we acquired are related to the third-party cloud, and not directly related to Android Auto.

**Table 3.** List of Artifacts in Wireless Communication between the Cloud and Mobile Device.

| IVI System | Artifact | Details |
|---|---|---|
| Android Auto | Origin | Woncheon-dong |
| | Destination | Ajou University Hospital |
| | Origin X, Y | 315,474, 520,056 |
| | Destination X, Y | 315,728, 520,093 |

### *4.2. Wireless Communication between the IVI and Mobile Device*

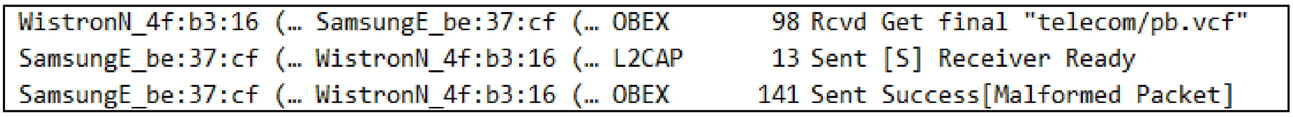
In this experiment, we conducted a collection and analysis of communication packets sent and received by Android Auto or Apple CarPlay with a mobile device. To collect communication packets between the IVI system and a mobile device, an experiment was conducted in a wirelessly connected environment. When Android Auto and Apple CarPlay connect wirelessly with a mobile device, they communicate using both BT and Wi-Fi channels. Therefore, we collected traffic from BT and Wi-Fi channels.

A BMW NBT HU EVO, a Pioneer AVH-Z5050BT, and a BMW X5 45e xLine were used in this experiment. BMW NBT HU EVO only supports Apple CarPlay wireless connection and does not support wireless connections to Android Auto. The Pioneer AVH-Z5050BT does not originally support a wireless connection to Apple CarPlay; however, a wireless connection is available using a CPC200-U2W PLUS adapter from CarLinkit Factory(. The BMW X5 45e xLine is the only one of the IVI systems we tested that supports wireless connectivity for both Android Auto and Apple CarPlay. To collect BT traffic of Android Auto, we used BT Snoop, a feature provided by Android OS. The Xcode PacketLogger tool was used to collect BT traffic from Apple CarPlay and a Wireshark tool was used to collect Wi-Fi traffic from both systems.

In addition, we applied BT connections between mobile devices and legacy systems that do not use Android Auto or Apple CarPlay and collected traffic from the BT channels. Both Android Auto and Apple CarPlay use BT and Wi-Fi for wireless connections. However, the connection of a legacy system also uses a BT channel. It is important to compare the traffic generated by the BT channel of Android Auto or Apple CarPlay with the traffic generated by the BT channel of a legacy system. Based on this comparison, we can determine whether the actual usage data of Android Auto and Apple CarPlay are also transmitted over the BT channel, or only through the Wi-Fi channel. Unlike Android Auto and Apple CarPlay, the legacy system does not mirror the navigation application of the mobile device, and thus only the functions of contact synchronization, SMS messages, and phone calls were used.

As a result of analyzing the BT traffic of Apple CarPlay, various artifacts and communication specifications were acquired. Artifacts that could be obtained on all devices were almost the same. It was confirmed that the BT communication of Apple CarPlay mainly uses an Audio/Video Remote Control Profile, host controller interface, and radio frequency communication (RFCOMM) protocols. It was also confirmed that some AT commands are used. As the result of a detailed analysis, details such as the BT address, BT name, pairing pin, encryption key, and related information of the vehicle and mobile device were acquired. In addition, the International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI) of the mobile device were acquired. Artifacts could also be acquired from Wi-Fi communication; however, the analysis was difficult in most cases because the traffic was encrypted.

As a result of analyzing the BT traffic of Android Auto, we obtained artifacts and communication specifications similar to those of Apple CarPlay. Android Auto also uses communication protocols over L2CAP channels such as RFCOMM and audio/video distribution transport protocol (AVDTP). Unlike Apple CarPlay, it uniquely uses the object exchange (OBEX) protocol for synchronizing the contacts. Figure 4 shows the process of requesting and receiving the contact file pb.vcf (phonebook.vcf) through the OBEX protocol. Using this packet, the contact stored in the mobile device can be obtained. In addition, artifacts such as the BT address and BT name were acquired. Unlike Apple CarPlay, the IMEI and IMSI of the mobile device cannot be obtained. In the case of Wi-Fi traffic, data are transmitted through [PSH, ACK] when the buffer is full. However, it appears to use encryption, and thus the content cannot be analyzed from every packet. Detailed artifacts are listed in Table 4.



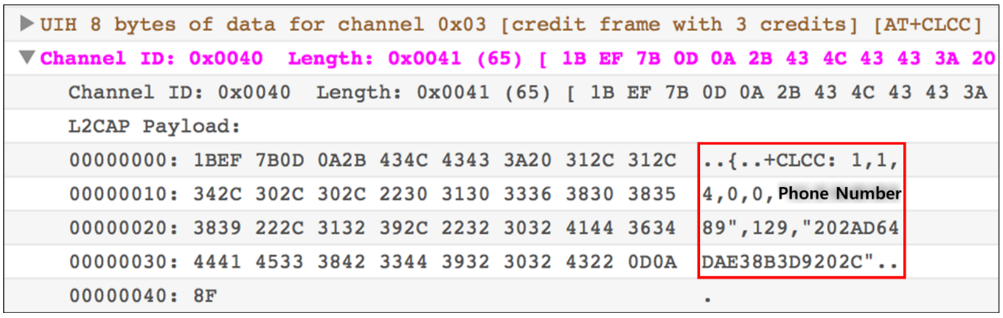
```
WistronN_4f:b3:16 (… SamsungE_be:37:cf (… OBEX       98 Rcvd Get final "telecom/pb.vcf"
SamsungE_be:37:cf (… WistronN_4f:b3:16 (… L2CAP      13 Sent [S] Receiver Ready
SamsungE_be:37:cf (… WistronN_4f:b3:16 (… OBEX      141 Sent Success[Malformed Packet]
```

**Figure 4.** Contact synchronization packets in Android Auto.

**Table 4.** List of Artifacts in Wireless Communication between the IVI and Mobile Device (Android Auto and Apple CarPlay).

| IVI System | Artifact | Details |
|---|---|---|
| Android Auto | Vehicle BT Address | 98:49:14:4F:B3:16 |
| | Vehicle BT Name | BMW 92906 |
| | Mobile Device Product Name | Galaxy S9+ |
| | Mobile Device BT Name | SM-G965N |
| | Mobile Device BT Address | 50:77:05:BE:37:CF |
| | Phone Book (Contact) | telcom/pb.vcf |
| Apple CarPlay | Vehicle BT Address | A0:56:B2:32:EB:23 |
| | Vehicle BT Name | BMW 88366 |
| | Vehicle Device ID | BC:30:7E:67:81:AB |
| | Vehicle Model Name | F25-NBTEvo-0716 |
| | Mobile Device BT Name | syh2347′s iPhone |
| | Mobile Device Product Name | iPhone9, 3 (iPhone7) |
| | Mobile Device BT Firmware | BCM4355C0_17.1.199.5230_Elsa_OS _USI_MCC_TRS_20190827.hcd |
| | Mobile Device OS Version | 13.3.1 (Build 17050) |
| | Mobile Device IMEI | 355321083330481 |
| | Mobile Device IMSI | 450080020035886 |
| | BT Pairing Pin | 665367 |
| | Link Layer Encryption Key | 2822d5031202e3de820476958beaab8d |
| | Link Layer Encryption State | 0x01 |

As a result of conducting an analysis on the legacy system, various artifacts and communication specifications were obtained. The same protocol is used for BT communication with both Android Auto and Apple CarPlay. However, more AT commands are used in the legacy system. As a result of the detailed analysis, in addition to the existing artifacts, details of the phone number of the call recipient and the phone number of the caller were also acquired. Figure 5 shows the acquired phone number. Comparing the artifacts acquired in the legacy system with the system using Android Auto and Apple CarPlay, it is assumed that they are transmitted over the Wi-Fi channel, excluding the initial pairing and contact synchronization. Detailed artifacts are listed in Table 5.



```
▶ UIH 8 bytes of data for channel 0x03 [credit frame with 3 credits] [AT+CLCC]
▼ Channel ID: 0x0040  Length: 0x0041 (65) [ 1B EF 7B 0D 0A 2B 43 4C 43 43 3A 20
    Channel ID: 0x0040  Length: 0x0041 (65) [ 1B EF 7B 0D 0A 2B 43 4C 43 43 3A
    L2CAP Payload:
    00000000: 1BEF 7B0D 0A2B 434C 4343 3A20 312C 312C  ..{..+CLCC: 1,1,
    00000010: 342C 302C 302C 2230 3130 3336 3830 3835  4,0,0,Phone Number
    00000020: 3839 222C 3132 392C 2232 3032 4144 3634  89",129,"202AD64
    00000030: 4441 4533 3842 3344 3932 3032 4322 0D0A  DAE38B3D9202C"..
    00000040: 8F                                       .
```

**Figure 5.** Phone number acquired in BT traffic (legacy system). From the red frame, the phone number and name saved in contacts are obtained.

**Table 5.** List of Artifacts in Wireless Communication between the IVI and Mobile Device (Legacy System).

| IVI System | Artifact | Details |
|---|---|---|
| Legacy System | Vehicle BT Address | A0:56:B2:32:EB:23 |
| | Vehicle BT Name | BMW 88366 |
| | Mobile Device Product Name | iPhone9, 3 (iPhone7) |
| | Mobile Device BT Firmware | BCM4355C0_17.1.199.5230_Elsa_OS_USI_MCC_TRS_20190827.hcd |
| | Mobile Device OS Version | 13.3.1 (Build 17050) |
| | Mobile Device IMEI | 355321083330481 |
| | Mobile Device IMSI | 450080020035886 |
| | Link Layer Encryption Key | C93982dd761c1d63dcc467a9f90ac287 |
| | Link Layer Encryption State | 0x01 |
| | Callee's Phone Number | 0107441xxxx |
| | Callee's Name | 20 2A AE 40 CC A0 C2 18 20 2C |
| | Caller's Phone Number | 0103680xxxx |
| | Caller's Name | 20 2A D6 4D AE 38 B3 D9 20 2C |

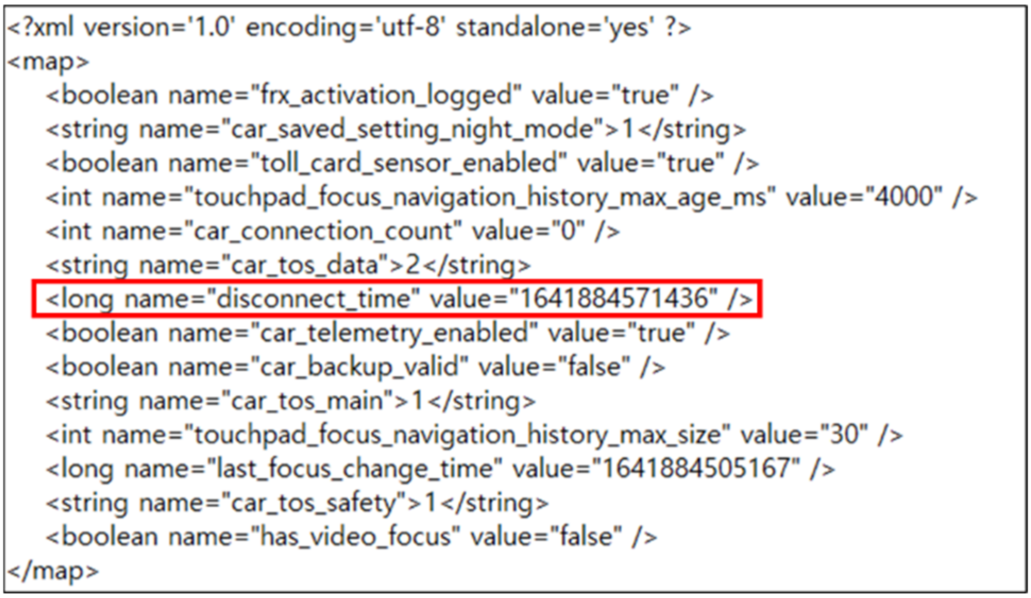
### 4.3. Internal Storage in the Mobile Device

Forensic research on mobile devices connected to Android Auto or Apple CarPlay has been actively conducted. According to known studies, the mobile device stores the connected vehicle information, IVI system usage history, and location information [12–15]. Therefore, when conducting the forensic analysis of mobile devices connected to a vehicle, we focused on finding newly added artifacts in the latest version of the IVI system. Mobile data acquisition and forensic analysis methods and forensic procedures were performed based on methods proposed in various studies conducted on Android OS and iOS [36–41]. Our analysis results can be used as a basis for future forensic investigations targeting Android Auto or Apple CarPlay systems.

BMW NBT HU EVO, BMW X5 45e xLine, Sony XAV-AX5000, and Pioneer AVH-Z5050BT were used in the experiments. When collecting data stored in the internal storage of a mobile device, the data were divided into cases of wired and wireless connections to the IVI system. For the Android Auto app, we used the latest version of Android 10, 7.1.614573 (as of December 2021, Mountain View, California, United States), on a Galaxy S9. For the Apple CarPlay app, the latest version of iOS, 13.3.1 (as of December 2021, Cupertino, California, United States), was used on an iPhone 7.

Analysis of data acquired from the internal storage of a mobile device connected with Android Auto confirmed that most of the artifacts acquired in the previous study were obtainable. However, we also discovered new artifacts added in the latest version of Android Auto. The newly added files are carservicedata.db and carservice.xml, which are placed inside the app directory of Android Auto.

Among them, carservicedata.db is a file that originally existed in the com.google.android.gms directory, according to a previous study [15]. This includes information such as the vehicle model, vehicle ID, and vehicle connection time. Because it stores information on connected vehicles, it appears to have been recently moved to the Android Auto package. The carservice.xml is a newly added file that stores various types of information. From a forensic perspective, however, the important information is the vehicle disconnection time (disconnect_time). Figure 6 shows the carservice.xml.



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="frx_activation_logged" value="true" />
    <string name="car_saved_setting_night_mode">1</string>
    <boolean name="toll_card_sensor_enabled" value="true" />
    <int name="touchpad_focus_navigation_history_max_age_ms" value="4000" />
    <int name="car_connection_count" value="0" />
    <string name="car_tos_data">2</string>
    <long name="disconnect_time" value="1641884571436" />
    <boolean name="car_telemetry_enabled" value="true" />
    <boolean name="car_backup_valid" value="false" />
    <string name="car_tos_main">1</string>
    <int name="touchpad_focus_navigation_history_max_size" value="30" />
    <long name="last_focus_change_time" value="1641884505167" />
    <string name="car_tos_safety">1</string>
    <boolean name="has_video_focus" value="false" />
</map>
```

**Figure 6.** The disconnect_time field inside the carservice.xml file. The red frame indicates the disconnection time (disconnect_time).

In addition, there is a file that already exists in the Android Auto package, although its contents have been changed. A new mirroring start time (pref_projected_activation_date) field has been added to the app_state_shared_preferences.xml file. An analysis of the data acquired from the internal storage of mobile devices connected to Apple CarPlay confirmed the results of previous studies. Detailed artifacts are listed in Table 6.

**Table 6.** List of Artifacts in Mobile Device Internal Storage.

| IVI System | Artifact | Details |
|---|---|---|
| Android Auto | Android Auto App List in Use | com.google.android.projection.<br>gearhead.common.HOTSEAT.xml (Package Name) |
| | BT MAC Address of Paired Vehicle | common_user_settings.xml<br>(MAC Address) |
| | Name of Paired Vehicle | common_user_settings.xml<br>(Bluetooth Name) |
| | Last Used Time | app_state_shared_preferences.xml (UNIX Timestamp) |
| | Projected Activation Time | app_state_shared_preferences.xml (UNIX Timestamp) |
| | Disconnection Time | carservice.xml (UNIX Timestamp) |
| | Wi-Fi Connection History | Timestamp (MM-DD HH:MM:SS) |
| | Google Assistance History [13] | binarypb File |
| Apple CarPlay | BT MAC Address of Paired Vehicle | com.apple.carplay.plist<br>(MAC Address) |
| | Name of Paired Vehicle | com.apple.carplay.plist<br>(Bluetooth Name) |
| | Last Used Time | com.apple.carplay.plist<br>(UNIX Timestamp) |
| | Last Siri Conversation | PreviousConversation.plist<br>(Text) |

### *4.4. Internal Storage in the IVI System*

In order to analyze the internal storage of the IVI system to obtain meaningful results from a forensic point of view, sufficient data must be stored in the target IVI system. Therefore, this experiment was conducted on the IVI system in which sufficient data was stored by applying the previous three case studies.

We conducted an analysis on six out of the eight IVI systems. Among the IVI systems we tested, a BMW X5 45e xLine was used for testing the wireless connectivity on Android Auto. Therefore, this IVI system was excluded from the experiment. We also excluded the crankshaft installed on the Raspberry Pi 3B device. Each IVI system was disassembled to check for the existence of an HDD, and if one was present, it was separated from the IVI system. We also analyzed the PCB to find a way to acquire data from flash memory. We minimized the damage when chip-off the flash memory from the PCB by referring to previous studies [42,43].

As a result, internal storage was obtained from a BMW NBT HU EVO and Belsee Best Aftermarket Auto. In the case of the BMW NBT HU EVO, an HDD is used. Belsee Best Aftermarket Auto has a flash memory capable of a chip-off. For other IVI systems, an analysis was conducted by considering UART and JTAG access; however, there were difficulties owing to the security features of the manufacturer. Figure 7 shows the HDD acquired from the BMW NBT HU EVO and the flash memory acquired from the Belsee Best Aftermarket Auto.

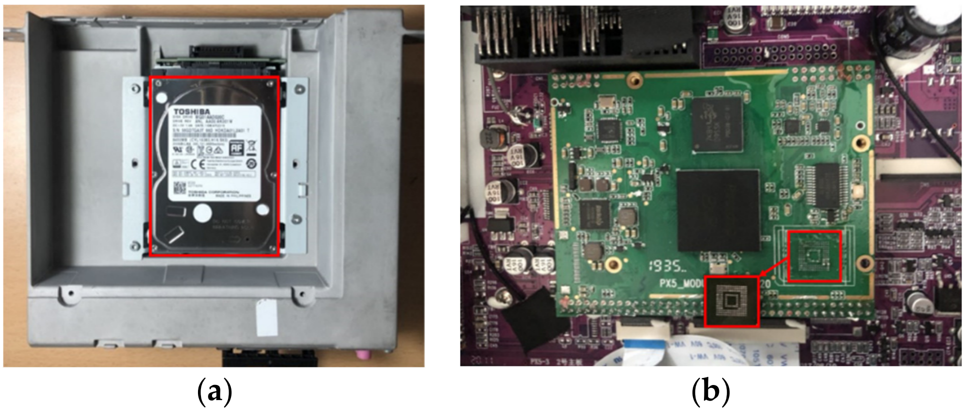


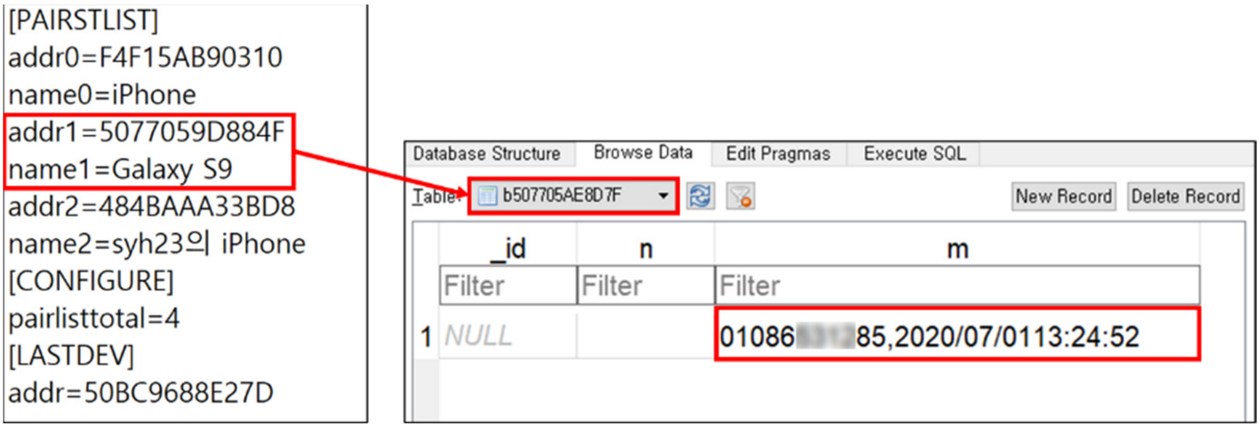
**Figure 7.** The red frames indicate the storage of the IVI system: (**a**) HDD acquired from BMW NBT HU EVO, (**b**) NAND flash acquired from Belsee Best Aftermarket Auto.

We analyzed the acquired BMW HDD and the Belsee flash memory. Table 7 lists the specifications for both types of internal storage. To acquire the data from the HDD of the BMW, we mounted the drive to a PC. However, it was confirmed that the HDD of the BMW system was ATA locked. To solve this problem, we refer to various studies related to BMW HDD and ATA and articles for unlocking the ATA Lock of BMW HDD [9,44,45]. However, in the case of the BMW NBT HU EVO system used in the experiment, with a higher level of security than before, analysis could no longer be performed.

**Table 7.** Internal storage specifications for BMW NBT HU EVO and Belsee Best Aftermarket Auto.

| Specification | BMW NBT HU EVO | Belsee Best Aftermarket Auto |
|---|---|---|
| Type | Hard Disk Drive | NAND Flash |
| Capacity | 200 GB | 64 GB |
| Filesystem | QNX4, QNX6 | Ext4, F2FS |
| OS | QNX | Android |

We conducted an Android-based forensic analysis on the internal storage acquired from the Belsee IVI system. A forensic analysis of the Ext filesystem was conducted based on our existing studies [46,47], and a forensic analysis of the F2FS filesystem was conducted using a TSK-based tool developed by our team. As the analysis results indicate, the vehicle connection and usage information were acquired from the internal storage. In addition, we confirmed that the drive contained artifacts that are commonly acquired on an Android device. Among them, only artifacts related to the Belsee IVI system and directly related to the mobile device were considered. Figure 8 provides a list of mobile devices connected to the Belsee IVI system. The left side of Figure 8 shows the file recording of the BT address and the BT name of the connected mobile devices (bt_conf.ini); the right side shows the database file with the BT address values in a table form (DateBase1.db). In this database file, the phone number and connection time of the mobile device connected to the vehicle are recorded. By correlating these two files, you can obtain BT-related information and phone number of the connected mobile device. In addition, we acquired artifacts on the locations where the vehicle was connected. Detailed artifacts are listed in Table 8.



```
[PAIRSTLIST]
addr0=F4F15AB90310
name0=iPhone
addr1=5077059D884F
name1=Galaxy S9
addr2=484BAAA33BD8
name2=syh23의 iPhone
[CONFIGURE]
pairlisttotal=4
[LASTDEV]
addr=50BC9688E27D
```

| | _id | n | m |
|---|---|---|---|
| | Filter | Filter | Filter |
| 1 | NULL | | 01086[redacted]85,2020/07/0113:24:52 |

**Figure 8.** BT paired device list (bt_conf.ini) and phone number acquired from Belsee Best Aftermarket Auto (DateBase1.db).

**Table 8.** List of Artifacts in IVI System Internal Storage.

| IVI System | Artifact | Details |
|---|---|---|
| Belsee Best Aftermarket Auto (Android Auto) | BT Paired Device List | bt_conf.ini (Bluetooth Name) |
| | Phone Number of BT Paired Device | DateBase1.db (Phone Number) |
| | Pairing Time of BT Paired Device | ivt.log (Unix Timestamp) |
| | BT Communication Log<br>Vehicle Location | SETTINGS.xml (Latitude, Longitude) |

### *4.5. Cross-Validation of In-Vehicle Infotainment System Artifact*

We conducted experiments on four methods for collecting forensic artifacts from the In-Vehicle Infotainment experimental environment and real vehicles. Based on this, we collected various forensic artifacts. Collected artifacts can be correlated to assist in forensic investigations.

In actual forensic investigations, Sections 4.1 and 4.2 tend to be real-time, so they are not generally suitable for post-forensic investigations. If it is not a planned investigation of a specific person, this corresponds to the prior knowledge that investigators should know before conducting a forensic investigation into the In-Vehicle Infotainment System. Therefore, in the post-forensic investigation, cross-validation can be performed for Section 4.3 (Internal Storage in the Mobile Device) and Section 4.4 (Internal Storage in the IVI System).

Before discussing methods for performing cross-validation on collected forensic artifacts, these are just a few of the many examples that can be used for forensic investigations. The forensic artifacts collected using the method proposed in this paper can be utilized in a variety of other ways besides the few examples we mention. We have summarized three methods for performing cross-validation on forensic artifacts collected based on the proposed method:

1. Forensic investigators can examine the driver's smartphone to determine which apps the driver used in Android Auto or Apple CarPlay. Based on this, when performing analysis on infotainment internal storage, it is possible to reduce the time required for forensic investigation by determining the main analysis target in advance;
2. Forensic investigators can examine the driver's smartphone to determine vehicle information related to usage time. Information that can be identified includes when the driver last used Android Auto or Apple CarPlay, and the connected vehicle's Bluetooth Name and MAC Address. Afterwards, forensic investigators can perform an analysis on infotainment internal storage to obtain a Bluetooth Log. Based on this, the forensic investigator can determine the vehicle's Bluetooth Name and MAC Address, as well as information about the smartphone connected to the vehicle. It is possible to specify a suspect by combining artifacts collected from these two sources. This can also be done in reverse order;
3. If a planned investigation is carried out on a specific person, sniffing for wireless communication between vehicle and smartphone such as Bluetooth and LTE may be performed. In this case, the Bluetooth Name and MAC address of the vehicle and smartphone can be identified through the wireless communication section packet. In addition, it is possible to obtain the driver's call record and a unique identification number such as the IMEI of the smartphone. This information can help specify the driver's smartphone in a post-forensic investigation and provide a non-repudiation. Also, when a forensic investigator performs an analysis on the Smartphone internal storage, only the last connected time can be obtained. However, based on the packet information collected in advance, the forensic investigator can timeline the time information when the smartphone is connected to the Infotainment System.

### *4.6. Significant Artifacts from IVI System Analysis*

We performed case studies for the actual vehicle environment. Most of the forensic studies on IVI systems that have been conducted are indirect forensic artifact collection studies limited to mobile devices. Accordingly, we conducted a forensic analysis of the internal storage of smartphones along with three new forensic analysis sections. As a result, we were able to acquire a variety of artifacts, including those acquired by existing studies. The acquired artifacts are summarized in Tables 3–6 and 8.

As a result of the analysis of Wireless communication between the cloud and mobile device, four artifacts related to the origin and destination were derived from the traffic of the navigation app. The derived artifacts are summarized in Table 3. In addition, it was confirmed that the artifacts derived from the Android Auto environment and Crankshaft are the same.

As a result of our analysis of Wireless communication between the IVI and mobile devices, we obtained over 10 artifacts related to vehicles and smartphones. The acquired artifacts are summarized in Tables 4 and 5. The acquired artifacts include vehicle information as well as information that is directly related to the connected smartphone. The derived artifacts have great significance in themselves, but they can also be used for cross-validation with other analysis sections. This can increase the reliability of the overall analysis results.

As a result of the analysis of Internal storage in the mobile device, five artifacts were derived from Samsung Galaxy S9+ devices, and four artifacts were derived from Apple iPhone 7 devices. We derived only artifacts that are directly related to the use of IVI systems, excluding information stored due to the use of a typical smartphone. The artifacts are summarized in Table 6. One of the artifacts acquired from Android Auto was a new artifact. This artifact serves as a reference for selecting an app to perform forensic analysis. In addition, we have shown that the acquired artifacts can be used to conduct organic analysis to determine the relevance of messaging and call records to vehicle use. Furthermore, based on our research, we confirmed that some artifacts that can be obtained may differ depending on the OS version. Android Auto does not exhibit much difference, whereas for Apple CarPlay, fewer artifacts can be acquired on the latest OS. In addition, the derived artifacts can be used for cross-validation with other analysis results.

Analysis of the Internal storage in the IVI system revealed four artifacts from Belsee Best Aftermarket Auto. These are summarized in Table 8. Because it included the BT Name and BT Address of the smartphone connected to the vehicle, it was possible to perform cross-validation with artifacts derived from the analysis of the wireless communication between the vehicle and smartphone and the internal storage of the smartphone. In addition, we derived the vehicle usage time and location information artifacts that are difficult to obtain from a smartphone. As a result of the analysis of the BMW NBT HU EVO, the vehicle internal data could not be acquired due to the reinforced ATA lock set on the HDD. We were only able to derive the type of OS and filesystem used by the BMW NBT HU EVO.

### *4.7. Forensic Analysis Tool for IVI System*

We developed a forensic tool that operates based on the four areas of the proposed forensic methodology. Therefore, our forensic tools provide a total of four functions:

First, the analysis of traffic between mobile devices and the cloud is automated. Packets from mobile devices and the cloud are ingested through the Charles Proxy tool. The tool analyzes the collected packets to obtain information such as the origin and destination of the navigation app.

Second, it automates the analysis of BT packets between the mobile device and the vehicle. When a BT packet between a mobile device and a vehicle is input into the tool, the tool parses the packet file to obtain the artifacts derived through the analysis.

Third, it automates the analysis of the internal storage of the mobile device. Raw images obtained from the internal storage in the mobile device are imported into the tool, and the tool acquires the derived artifacts. In addition, it can organize the acquired artifacts based on the timeline.

Fourth, it automates the analysis of the internal storage of the IVI system. In this case, because the analysis was conducted only on Belsee Best Aftermarket Auto devices, it only works on an Android-based IVI. When the tool applies a raw image from the internal storage of the IVI, the tool acquires the derived artifacts. In addition, it can also organize the acquired artifacts based on the timeline.

Figure 9 shows a flowchart of analyzing BT packets between a mobile device and a vehicle. The artifact acquisition and analysis automation tool works with the following procedures:

1. Select analysis target (Internal Storage of Smartphone(2) or BT packet(3));
2. Analysis of Smartphone's Internal Storage
   - 2.1 After connecting the smartphone, select the operating system to be analyzed
   - 2.2 The analytics tool performs the process of collecting data from a specific location on the smartphone's internal storage
   - 2.3 Analyze the collected data to derive forensic artifacts and output them as results;
3. Analysis of BT packet
   - 3.1 After entering the packet file, select the IVI system to be analyzed
   - 3.2 Parsing and analyzing the contents of the packet file to derive forensic artifacts and output them as results.

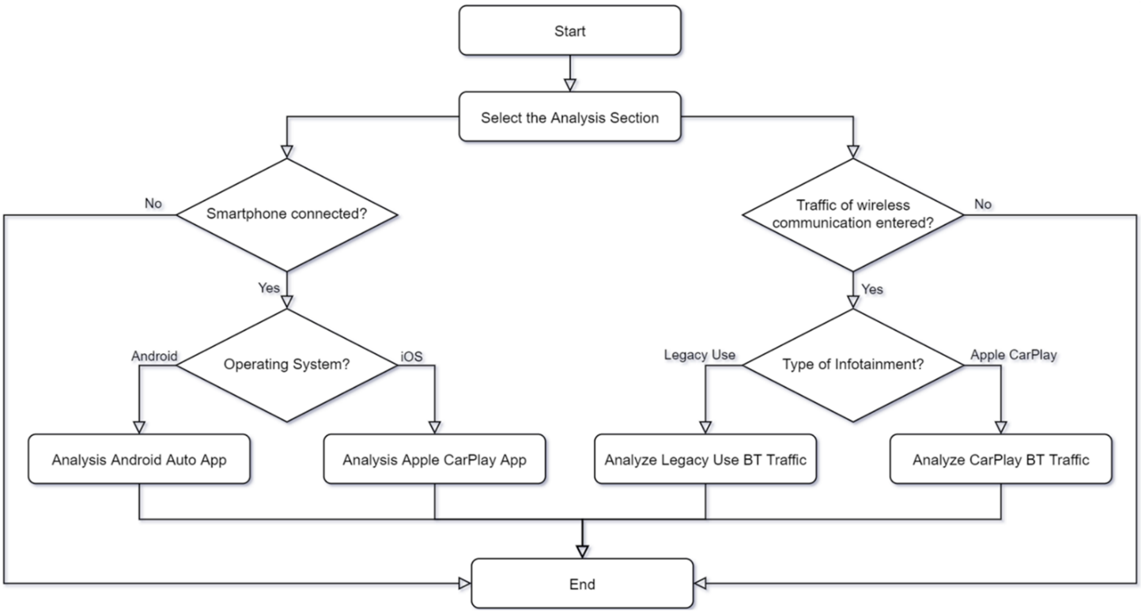
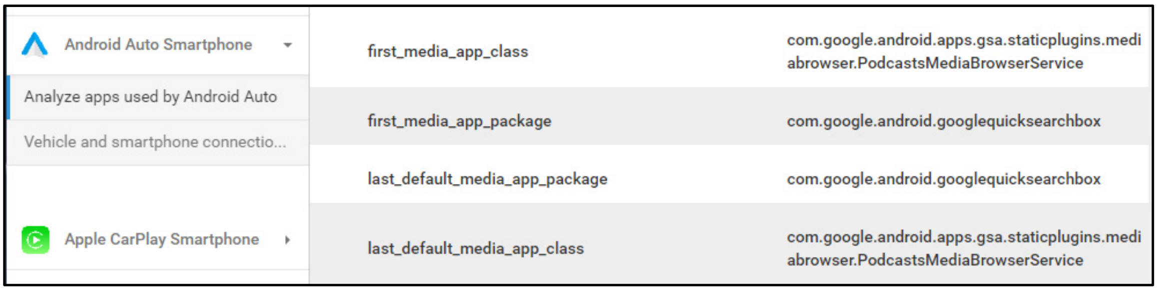

Start
Select the Analysis Section
Smartphone connected?
No
Yes
Operating System?
Android
iOS
Analysis Android Auto App
Analysis Apple CarPlay App
Traffic of wireless communication entered?
No
Yes
Type of Infotainment?
Legacy Use
Apple CarPlay
Analyze Legacy Use BT Traffic
Analyze CarPlay BT Traffic
End

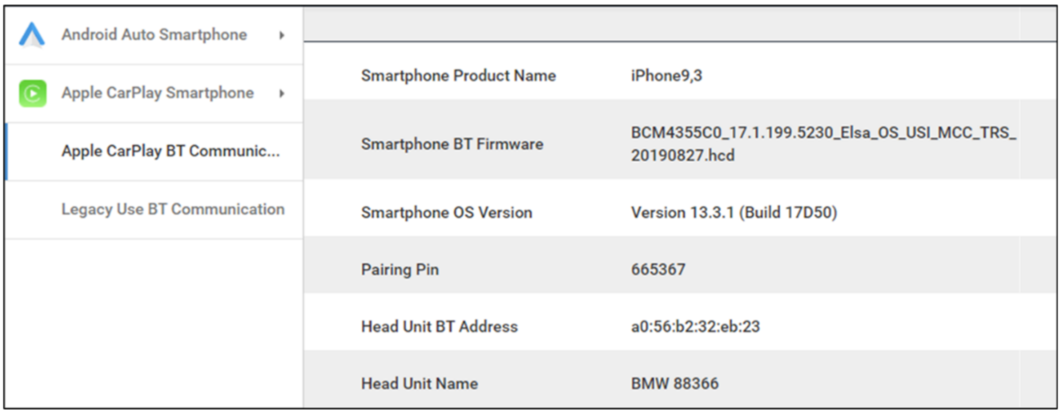
**Figure 9.** Flowchart for analyzing BT packets between a mobile device and a vehicle.

Figure 10 shows the results of the tool developed for analyzing the Internal Storage of an android smartphone. The figure shows the default app setting of Android Auto and the last used app output as a result of analyzing the internal storage of the Android smartphone. Figure 11 shows the results of the tool developed for analyzing the BT packets between the mobile device and the vehicle. The figure shows that the developed tool analyzes the BT packet and outputs information about the connected smartphone, pairing pin, and information on the IVI system.


Android Auto Smartphone
Analyze apps used by Android Auto
Vehicle and smartphone connectio...
Apple CarPlay Smartphone

| | |
|---|---|
| first_media_app_class | com.google.android.apps.gsa.staticplugins.mediabrowser.PodcastsMediaBrowserService |
| first_media_app_package | com.google.android.googlequicksearchbox |
| last_default_media_app_package | com.google.android.googlequicksearchbox |
| last_default_media_app_class | com.google.android.apps.gsa.staticplugins.mediabrowser.PodcastsMediaBrowserService |

**Figure 10.** Results of analyzing the Internal Storage of Android Smartphone.



| | |
|---|---|
| Smartphone Product Name | iPhone9,3 |
| Smartphone BT Firmware | BCM4355C0_17.1.199.5230_Elsa_OS_USI_MCC_TRS_20190827.hcd |
| Smartphone OS Version | Version 13.3.1 (Build 17D50) |
| Pairing Pin | 665367 |
| Head Unit BT Address | a0:56:b2:32:eb:23 |
| Head Unit Name | BMW 88366 |

**Figure 11.** Results of analyzing the BT packet between the mobile device and vehicle.

## 5. Discussion

Although forensic studies of the Android Auto and Apple CarPlay IVI systems have been conducted, the operation method of the IVI system was not taken into account in the forensic analysis. For this reason, there are limitations in the field of IVI system forensics that have made it difficult to collect forensic artifacts in some areas of analysis. To overcome these limitations, we proposed a forensic methodology that considers the operation of an IVI system and analyzed several different systems. Our findings show that a forensic analysis of wireless communication in an IVI system is meaningful. In addition, we found important information that is meaningful from a forensic perspective in the storage of a mobile device and the storage of an IVI system. We have overcome the limitations of IVI system forensics to a certain extent by applying the proposed forensic technique.

There are certain limitations to our case studies. The analysis of the wireless communication between the cloud and mobile device could only be conducted using Android Auto, because Apple CarPlay applies LTE for communication between the cloud and mobile devices. In the analysis of the wireless communication between the IVI and a mobile device, we compared the analysis results of the legacy system using Android Auto and Apple CarPlay. The results show that most of the actual usage data for Android Auto or Apple CarPlay were transmitted over the Wi-Fi channel. However, we could not analyze the Wi-Fi channel owing to encryption or the communication standards of the manufacturer. Nevertheless, forensic analysis results show the need for a wireless communication analysis in IVI systems. A detailed analysis of the internal storage in the IVI system could not proceed owing to encryption of the HDD of the BMW NBT HU EVO.

Despite the above limitations in our case studies, we obtained sufficiently diverse forensic artifacts in the IVI environment. In particular, newly added artifacts were discovered in the analysis of the internal storage of the mobile device connected with Android Auto. These artifacts can be used as important evidence in conducting a forensic investigation because they contain timestamps that are connected to or disconnected from the vehicle. In addition, we analyzed the internal storage used in the IVI system based on the Android platform. Because the share of Android Automotive OS has been gradually increasing in recent years, the analysis results are also sufficiently meaningful.

## 6. Conclusions

Forensic studies of Android Auto and Apple CarPlay systems have only been conducted on the internal storage of mobile devices. However, there are also IVI systems that make up the IVI system environment. Therefore, analysis must also be performed on the data stored inside the IVI system, and since the IVI system and the mobile device are connected, the resulting communication section is also subject to analysis. Therefore, we have proposed a forensic methodology and conducted various case studies to address the shortcomings in the field of IVI system forensics research. The analysis results showed that the proposed methodology can solve the above constraint. In addition, the forensic artifacts acquired in each analysis area show that the forensic artifacts obtainable in IVI systems using Android Auto and Apple CarPlay are not limited to the internal storage in a mobile device. As such, a digital forensic examination of various elements constituting the IVI system is a useful addition to vehicle forensics. An increasing number of people are using Android Auto and Apple CarPlay, and more vehicles and manufacturers are sup-porting these systems. The proposed forensic methodology and the acquired artifacts can be applied as an important basis for future vehicle crime investigations.

As IVI technology advances, mobile devices and IVI systems are increasingly making use of driver-related information. In the near future, IVI systems will become an important source of evidence in digital forensic investigations, just like today's smartphones. In our study, although the analysis of various sections constituting the IVI system environment was performed, there are still shortcomings. By performing decompilation analysis on IVI applications with future work, communication structure analysis studies on Wi-Fi communication channels of IVI systems can be performed. This allows you to perform a complete analysis of the communication between the IVI system and your mobile device. In addition, most of the IVI systems used for analysis in our study were chip-off resistant systems. Therefore, it is possible to conduct research on data acquisition methods using hardware debugging interfaces such as UART and JTAG for IVI systems that cannot be chip-off with future work.

**Author Contributions:** Conceptualization, Y.S. and T.S.; methodology, Y.S., S.K., W.J. and T.S.; validation, Y.S. and S.K.; formal analysis, Y.S., S.K. and W.J.; investigation, Y.S.; writing—original draft preparation, Y.S.; writing—review and editing, Y.S., S.K., W.J. and T.S.; project administration, Y.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by Institute of Information and Communications Technology Planning and Evaluation(IITP) grant funded by the Korean government (MIST) (No.2022-0-01022, Development of Collection and Integrated Analysis Methods of Automotive Inter/Intra System Artifacts through Construction of Event-based experimental system). The research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2018R1D1A1B07043349).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Jo, W.; Kim, S.; Kim, H.; Shin, Y.; Shon, T. Automatic whitelist generation system for ethernet based in-vehicle network. *Comput. Ind.* **2022**, *142*, 103735. [CrossRef]
2. Kim, S.; Jo, W.; Shon, T. APAD: Autoencoder-based payload anomaly detection for industrial IoE. *Applied Soft Computing* **2020**, *88*, 106017. [CrossRef]
3. Sladović, D.; Topolčić, D.; Hausknecht, K.; Sirovatka, G. Investigating modern cars. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019. [CrossRef]
4. El Mekki, A.; Bouhoute, A.; Berrada, I. Improving driver identification for the next-generation of in-vehicle software systems. *IEEE Trans. Veh. Technol.* **2019**, *68*, 7406–7415. [CrossRef]
5. Urquhart, C.; Bellekens, X.; Tachtatzis, C.; Atkinson, R.; Hindy, H.; Seeam, A. Cybersecurity internals of a skoda octavia vRS: A hands on approach. *IEEE Access* **2019**, *7*, 146057–146069. [CrossRef]
6. Henry, P. Digital Forensics—Automotive Infotainment and Telematics Systems. Available online: https://www.sans.org/blog/digital-forensics-automotive-infotainment-and-telematics-systems/ (accessed on 1 July 2022).
7. Lacroix, J.; El-Khatib, K.; Akalu, R. Vehicular digital forensics: What does my vehicle know about me? In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Valletta, Malta, 13–17 November 2016; pp. 59–66. [CrossRef]
8. Cohen, T. "Look at What My Car Can Do." DEFCON 19. Available online: https://www.youtube.com/watch?v=Jun0cD6x08U (accessed on 1 July 2022).
9. Moos, J.; Davies, G.; Lewis, E.; Williams, N.; Gichohi, B.; Lane, R.; Bellany, A. Digital forensics for automobile systems: The challenges and a call to arms. *Int. J. Forensic Sci.* **2016**, *1*, 1–13.
10. Le-Khac, N.A.; Jacobs, D.; Nijhoff, J.; Bertens, K.; Choo, K.K.R. Smart vehicle forensics: Challenges and case study. *Future Gener. Comput. Syst.* **2020**, *109*, 500–510. [CrossRef]
11. Ebbers, S.; Ising, F.; Saatjohann, C.; Schinzel, S. Grand Theft App: Digital Forensics of Vehicle Assistant Apps. *arXiv* **2021**, arXiv:2106.04974. [CrossRef]
12. Edwards, S.; Mahalik, H. They See Us Rollin'; They Hatin': Forensics of iOS CarPlay and Android Auto. SANS DFIR. 2019. Available online: https://www.youtube.com/watch?v=IGhXsfZXL6g (accessed on 1 July 2022).
13. Hickman, J. Android Auto & Google Assistant. DFRWS USA. 2019. Available online: https://dfrws.org/presentation/android-auto-google-assistant-how-google-encourages-hands-free-motoring-2/ (accessed on 11 July 2022).
14. Hickman, J. Ridin' with Apple CarPlay, the Binary Hick—Thoughts from a Digital Forensic Practitioner. 2019. Available online: https://thebinaryhick.blog/2019/05/08/ridin-with-apple-carplay/ (accessed on 1 July 2022).
15. Mahalik, H. How Android Bluetooth Connections Can Determine If the Hands of a Driver Were on the Wheel during an Accident. 2020. Available online: https://cellebrite.com/en/how-android-bluetooth-connections-can-determine-if-the-hands-of-a-driver-were-on-the-wheel-during-an-accident/ (accessed on 1 July 2022).
16. Google. Android Auto. Available online: https://www.android.com/auto/ (accessed on 1 July 2022).

17. Apple. Apple CarPlay. Available online: https://www.apple.com/ios/carplay/ (accessed on 1 July 2022).
18. Kwon, S.; Yoo, H.; Shon, T. IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. *IEEE Access* **2020**, *8*, 77572–77586. [CrossRef]
19. Schubert, E. Developing CarPlay Systems, Part 1. Apple Worldwide Developers Conference. 2016. Available online: https://developer.apple.com/videos/play/wwdc2016/722/ (accessed on 1 July 2022).
20. Jo, W.; Shin, Y.; Kim, H.; Yoo, D.; Kim, D.; Kang, C.; Jin, J.; Oh, J.; Na, B.; Shon, T. Digital forensic practices and methodologies for AI speaker ecosystems. *Digit. Investig.* **2019**, *29*, S80–S93. [CrossRef]
21. Shin, Y.; Kim, H.; Kim, S.; Yoo, D.; Jo, W.; Shon, T. Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. *Digit. Investig.* **2020**, *33*, 301010. [CrossRef]
22. Sathe, S.C.; Dongre, N.M. Data acquisition techniques in mobile forensics. In Proceedings of the 2nd International Conference on Inventive Systems and Control, Coimbatore, India, 19–20 January 2018; IEEE: Piscataway, NJ, USA, 2018. [CrossRef]
23. Crankshaft. Available online: https://getcrankshaft.com/ (accessed on 12 September 2022).
24. The Wireshark Team. Wireshark. Available online: https://www.wireshark.org/ (accessed on 12 September 2022).
25. Bluetooth. A New Way to Debug iOS Bluetooth Applications. Available online: https://developer.apple.com/download/more/?=xcode (accessed on 12 September 2022).
26. Sublime, H.Q. Sublime Text. Available online: https://www.sublimetext.com/ (accessed on 12 September 2022).
27. sqlitebrowser. DB Browser for SQLite. Available online: https://sqlitebrowser.org/ (accessed on 12 September 2022).
28. von Randow, K. Charles. Available online: https://www.charlesproxy.com/ (accessed on 12 September 2022).
29. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
30. Callegati, F.; Cerroni, W.; Ramilli, M. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy* **2009**, *7*, 78–81. [CrossRef]
31. Fahl, S.; Harbach, M.; Muders, T.; Baumgärtner, L.; Freisleben, B.; Smith, M. Why Eve and Mallory love Android: An analysis of Android SSL (in) security. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh North, CA, USA, 16–18 October 2012. [CrossRef]
32. Onwuzurike, L.; De Cristofaro, E. Danger is my middle name: Experimenting with SSL vulnerabilities in Android apps. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, 22–26 June 2015. [CrossRef]
33. Kakao Mobility. Location-Based Service Terms and Conditions. Available online: https://policy.kakaomobility.com/viewer/?pageCode=LOCATION&languageCode=en (accessed on 12 September 2022).
34. Kakao Mobility. Kakao T Terms of Service. Available online: https://policy.kakaomobility.com/viewer/?pageCode=TERMS (accessed on 12 September 2022).
35. Kakao Mobility Privacy (Location Information) Policy for Partners. Available online: https://policy.kakaomobility.com/viewer/?pageCode=PRIVACY_POLICY&languageCode=en (accessed on 12 September 2022).
36. Al-Sabaawi, A.; Foo, E. A comparison study of android mobile forensics for retrieving files system. *Int. J. Comput. Sci. Secur. (IJCSS)* **2019**, *13*, 148–166.
37. Roy, N.R.; Khanna, A.K.; Aneja, L. Android phone forensic: Tools and techniques. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 29–30 April 2016; IEEE: Pisca-taway, NJ, USA, 2016. [CrossRef]
38. Al-Dhaqm, A.; Abd Razak, S.; Ikuesan, R.A.; Kebande, V.R.; Siddique, K. A review of mobile forensic investigation process models. *IEEE Access* **2020**, *8*, 173359–173375. [CrossRef]
39. Bays, J.; Karabiyik, U. Forensic analysis of third party location applications in android and ios. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019.
40. Alghafli, K.A.; Jones, A.; Martin, T.A. Forensics data acquisition methods for mobile phones. In Proceedings of the 2012 International Conference for Internet Technology and Secured Transactions, London, UK, 10–12 December 2012; IEEE: Pisca-taway, NJ, USA, 2012.
41. Morrissey, S.; Campbell, T. *iOS Forensic Analysis: For iPhone, iPad, and iPod Touch*; Apress: New York, NY, USA, 2011.
42. Fukami, A.; Ghose, S.; Luo, Y.; Cai, Y.; Mutlu, O. Improving the reliability of chip-off forensic analysis of NAND flash memory devices. *Digit. Investig.* **2017**, *20*, S1–S11. [CrossRef]
43. van Zandwijk, J.P.; Fukami, A. NAND flash memory forensic analysis and the growing challenge of bit errors. *IEEE Secur. Priv.* **2017**, *15*, 82–87. [CrossRef]
44. u/Krzys_CCE. ATA Password on a Hard Drive. Available online: https://www.reddit.com/r/datarecovery/comments/hg4njd/ata_password_on_a_hard_drive/ (accessed on 12 September 2022).
45. Coughlin, T. The Memory of Cars [The Art of Storage. *IEEE Consum. Electron. Mag.* **2016**, *5*, 121–125. [CrossRef]
46. Lee, S.; Jo, W.; Eo, S.; Shon, T. ExtSFR: Scalable file recovery framework based on an Ext file system. *Multimed. Tools Appl.* **2020**, *79*, 16093–16111. [CrossRef]
47. Lee, S.; Shon, T. Improved deleted file recovery technique for Ext2/3 filesystem. *J. Supercomput.* **2014**, *70*, 20–30. [CrossRef]