Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective

Jesse Lacroix

University of Ontario Institute of Technology

MSc Computer Science Thesis

Author Note

This thesis reports the general findings of what is stored long-term on a vehicle's infotainment system and a reflection on how the data could be used. All funding provided by the Natural Sciences and Engineering Research Council (NSERC). Correspondence address: 8-3374 Muskoka Street, Washago, ON, L0K 2B0. Important note: I have been employed as a Digital Forensic Analyst/Investigator for the Ontario Provincial Police since June 2016.

Abstract

In today's transportation system, countless numbers of vehicles are on the road and later generations have become mobile computers. Vehicles now have embedded infotainment systems that enable user-friendliness and practicability with functions such as a built-in global positioning system, media playback device and application interface. Smartphones and laptops can connect to them through Bluetooth and WiFi for all sorts of utilities. This enables data flow between a user's device and the infotainment system and because of this interaction, data remnants are kept on these embedded devices. It is important to determine what type of data is stored long term since this information reflects a user's activity and potential personal information. In terms of forensics, this data could be used to solve criminal activities if a vehicle was suspected of being an accessory to a crime; raising general awareness about this topic is important due to the potential sensitive information circulated. This main objective of this thesis is to demonstrate what types of information are stored on infotainment systems, how it can be acquired and the implications and contributions of the collected data in relation to the overall field of digital forensics.

Keywords: digital forensics, internal vehicle components, embedded devices, infotainment systems, vehicular forensics

Overall Contribution

This collaborated effort and thesis was made with the ultimate goal of identifying what types of information and data are stored on vehicular infotainment systems for its extended use, may it be for legal or personal use; we hope to positively contribute to the overall field of digital forensics, to law enforcement and raising general awareness about the data that is circulated and kept on these platforms. We also hope this work and thesis can be used as a baseline or reference for future research efforts in regards to vehicular and mobile digital forensics as well as the internal electronic components of vehicles and interactions with infotainment systems. The goal is to educate and showcase all relevant acquired data, its application and a framework to follow when interacting with such systems as well as validating that such data exists and can be put to use in the overall field of digital forensic.

Acknowledgments

I would like to take the time to thank the Ontario Provincial Police's Technological Crime Unit (OPP TCU) and Special Constable Jeremy Dupuis, the Office of the Privacy Commissioner of Canada (OPC), John Fledderus from Whitby OWASCO's Audi/Volkswagen dealership, Dr. Rajen Akalu of the University of Ontario Institute of Technology (UOIT) and Jason Whelan, a former student of the University of Ontario Institute of Technology, for their assistance with this project in giving us help and access to many resources including forensic images for analysis, software and hardware for acquisition processes as well as funding. I would especially like to thank my supervisor from the University of Ontario Institute of Technology, Dr. Khalil El-Khatib, for his continued patience, guidance and resources that enabled me to do this project to the best of my abilities.

Contents

List of Figures

List of Tables

Chapter I – Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective

The evolution of technology has allowed for the implementation of embedded systems in every aspect of our lives. This has made a huge impact on the development of vehicles and embedded technologies enabling many more utilities. Typical modern vehicles are now composed of Electronic Control Units (ECUSs) which basically actuate a motor for a vehicle functionality to complete based on messages received. Sensors that are embedded on the vehicles can also trigger the ECUs themselves for safety and efficiency reasons without the driver being aware, which can end up stopping non-desirable scenarios. All in all, vehicles are starting to resemble computer/computer networks, which will be discussed later in this thesis in a comprehensive form for better understanding. This leads to the connected devices that make up the vehicles and allow all their functionalities. Take for example the infotainment system, a growing aspect of a vehicle's components as in the past, it mainly constituted of a media device for radio and audio playback. These devices are now outfitted with a built-in Global Positioning System (GPS), Bluetooth and WiFi connectivity for mobile devices such as smartphone and laptops and an application interface on top of the traditional media utilities. These devices can even monitor information relating to the vehicle itself (e.g., motor status, tire pressure, braking status, etc.).

Infotainment systems tend be manufactured by the original vehicle maker therefore can be closed source although most are simply rebranded devices bought from a technology supplier. This means that no standard has been established towards the development of the infotainment systems. Luckily, Google has teamed up with technological and vehicle manufacturer giants to establish the Open Automotive Alliance (https://www.openautoalliance.net/) which has an aim

for developing a common platform across infotainment systems and the Android platform. This has allowed the alliance to develop *Android Auto*, an application which interfaces a user's Android phone to the "Android Auto ready" infotainment system directly. Apple has also achieved the same type of application with *Apple CarPlay*, which allows iPhones to directly interface with the appropriate "Apple CarPlay ready" infotainment systems. This is important to note as we are seeing a trend of popular devices easily and seamlessly connecting to infotainment systems. Although these applications are recently made available to users and functional in infotainment systems, they will not further be covered in the scope of this thesis. This is to simply state the increased amount of information flows between these systems and that they allow for direct interfacing between an Android or Apple device and the connected infotainment system.

The widespread of infotainment systems leads to an important question: What is being stored long-term on these infotainment systems, considering how much interaction they have with end users' personal devices? When a user connects to these platforms, some functionalities require the user's permission for access to certain aspects of the user's personal device for some functionalities of the infotainment system to work (e.g., making phone calls with voice command using Ford's SYNC platform, answering/making phone calls, sending/reading text messages, etc.). With this in mind, there is an automatic assumption that data remnants are present on the infotainment device but it is important to determine exactly what. When interacting and storing information on a personal computer, the user will be aware of what he/she is keeping on the device (excluding maybe cookies and session information when browsing online and temporary folders). When users interact with an infotainment system after connecting it to their personal mobile device, they may not be aware that data is being stored as information is being relayed to

the vehicle infotainment platform automatically. Users would not know what is being stored and it could be personal and sensitive information they would rather not have stored on their vehicle. With the vehicle infotainment aftermarket being just as huge as the main manufacturer one, this information could potentially end up in the wrong hands. From a forensics point of view, this could help solve crimes when a vehicle is suspected of being somewhat involved in a crime (e.g., a vehicle gets stolen then recovered without the culprit therefore one could use the infotainment and GPS data to determine what the culprit did and where he/she went while possessing the vehicle). The information could also potentially help determine the cause of an accident on top of all the other sensor data collected. The uses of this data, once put into perspective, could shine some light on what its practical uses could be and if some of it is necessary at all.

This finally establishes the hypothesis of this research: *What data is stored on in-vehicle infotainment systems and can we determine anything about the users based off this acquired information?* This thesis will consist of the following chapters: Chapter II will give an overview of Vehicular Ad Hoc Networks (VANETs), vehicle internal network buses and components and how they communicate as well as overall security vulnerabilities involving both VANETs and internal communication components since infotainment systems are part of the in-vehicle network buses; Chapter III will discuss generic forensic concepts and its current state, the state of mobile device forensics due to their close interactions with infotainment systems, Android forensics as most popular aftermarket infotainment systems are Android based platforms and finally it will present the current state of vehicular forensics in general, not necessarily relating to infotainment systems; Chapter IV will present the acquisition methods for our infotainment systems and the results obtained from the acquisitions of infotainment systems; Chapter V will

discuss the overall implications of the results acquired by this research and how it applies to digital forensics; Chapter VI will provide a conclusion summarizing the research.

Chapter II – VANETs and Vehicle Internal Network Buses/Components

Modern vehicles have made leaps and bounds in terms of technological advancements and housing of components. Embedded systems are adding more functionality to vehicles making them more efficient, practical and safe in terms of their intended design. Inter-vehicle communication networks, also known as Vehicular Ad Hoc Networks (VANETs), are being researched and developed to modernize the transportation system in hopes of making it more efficient, safer and allowing vehicles to communicate with one another. Modularity is also kept in mind as the transportation system is prone to advancements on its side as well due to vehicular advancements. This chapter gives an overview of VANETs, internal network components of vehicles as well as their place in the transportation system. The security state is also mentioned due to the interoperability of internal vehicle components as it is important to understand to the basis of vehicle vulnerabilities (and associated systems) as one system can compromise the other.

2.1 State of Transportation System

The VANET infrastructure has been in development and an active research topic for years now. It has seen considerable progress for its proper implementation and standardization with collaborations from around the world. This infrastructure leads to the implementation of the Intelligent Transportation System (ITS), which is a collection of applications and services meant for a more efficient, safer and user-friendly transportation system. In VANETs, vehicles will be able to communicate with other vehicles directly through peer-to-peer means called Vehicle-to-Vehicle communications (V2V) and to static infrastructure through Vehicle-to-Infrastructure and Infrastructure-to-Vehicle communications (V2I and I2V).

Modern vehicles are now embedded with Electronic Control Units (ECUs) and On-Board Units (OBUs) to send and receive information to other vehicles or Road Side Units (RSUs). RSUs and vehicles are used to send critical information to other peers and to communicate to other parts and types of network infrastructures such as the Internet. RSUs are important in the operation of VANETs because they are used as relays to send information to all vehicles (for e.g., safety-related messages such as an accident occurring within a specific region and authentication messages for system validation). Vehicle tracking, vehicle speed, Basic Safety Messages (BSMs) and other related information can all be exchanged between the vehicles themselves directly to ensure efficient and safe operation of the vehicles in their respective environments. What is important about VANETs is that they incorporate other means of communications to facilitate their operation. Examples of these as shown by Checkoway et al. [10] are: Bluetooth; broadcast channels, such as radio and GPS channels); addressable channel, such as OnStar [10]; and cellular channels, including 3G/4G LTE and basic voice channels for cellular communications. Combining all of these technologies together offers much more robustness to VANETs; however, on a security aspect, it offers more attack surfaces and potential for more vulnerabilities to be discovered and have these technologies leveraged against the vehicle and its users.

The IEEE 1609 standard shown by the IEEE Standards Association [29], also known as the Wireless Access in Vehicular Environments (WAVE), is a service recognized by the ITS. It is employed in the United States and similar infrastructures employed around the world for VANETs so that vehicles and respective infrastructure can communicate. This standard can also be associated to the Dedicated Short Range Communications (DSRC) protocol for radio

spectrum allocation used by WAVE technologies. WAVE embodies many standards for its secure and efficient communications. They are as followed:

- IEEE Std 802.11 (2012)—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications for metropolitan and local networks as well as data exchange between systems
- IEEE Std 1609.2 (2013)—WAVE Security Services for applications and Management Messages; makes use of Elliptic Curve Cryptographic (ECC) as an encryption standard
- IEEE Std 1609.3 (2010)—WAVE Networking Services
- IEEE Std 1609.4 (2010)—WAVE Multi-Channel Operations
- IEEE Std 1609.11 (2010)—WAVE ITS over-the-air payment data exchange protocol
- IEEE Std 1609.12—WAVE Identifier Allocations

The European Telecommunications Standards Institute (ETSI) has developed its set of standards for VANET communication and information exchange for the ITS based off IEEE 802.11 technologies shown by Rizzo and Brookson [65]. ETSI ITS standards will take in consideration the IEEE 1609.2 data sets, but it will adopt them to fit explicit protocols developed for ETSI standards and will collaborate closely with the IEEE community. Here are some of the current ETSI ITS security standards:

- ETSI TS 102 867—ITS Security Service IEEE 1609.2 stage 3 mapping
- ETSI TS 102 940—ITS Security Service for communications security architecture and management
- ETSI TS 102 941—ITS Security Service for Trust and Privacy Management

- ETSI TS 102 942—ITS Security Service for Access Control
- ETSI TS 102 943—ITS Security Service for Confidentiality Services
- ETSI TS 103 097—ITS Security Service for headers and certificate formats

Vehicle components allow for a vehicle to generate, log and exchange data about its surrounding and users in real time. The data logged hypothetically gives a third party the ability to analyze this data if it manages to access it. According to Illera and Vidal [30], data dumps of vehicle crashes are stored into a vehicle's Electronic Control Unit (ECU). These data dumps, if retrieved, could grant law enforcement agencies the ability to reconstruct accidents and determine the cause of an accident. Data about a driver could also be collected if he or she was suspected of criminal activities. Infotainment systems inside modern vehicles could determine a lot about the end user through his trends and activities, not to mention the localization data produced by embedded GPS systems.

The data logged and circulating inside these vehicles directly relate to the driver's habit since it reflects the users actions. Insurance companies, such as the Canadian firm Desjardins, make use of hardware modules to monitor these habits. Their service Ajusto, reported by CTV Ottawa [15], is a plug-in-play car attachment used by Desjardins which monitors user activity. Wall [74] reported that user activity and driving habits are measured through the use of the same "black box" units and related applications installed in smartphones. This allows good and safe drivers to pay less insurance fees since their recorded habits reflect lower chances of causing an accident and breaking the law. After contacting a Desjardins technical support representative, it was confirmed that the data is kept on the Ajusto box locally until transmitted. The transmission is done twice a day if still connected to its respective cellular network on Canadian soil. If the vehicle is outside Canada, the data is stored locally onto the Ajusto device until it connects back

to the Canadian network. Based off this information, the possibility of extracting the information kept on these specific devices becomes more apparent and plausible as two large time windows are made available or the time window become indefinite if the vehicle is outside of its intended country of operation. The ability to verify exactly what type of information is kept onto devices such as Ajusto could potentially be used to determine information of the vehicle driver. Additionally, what needs to be verified is if any of that or related information is kept in other components of the vehicle, more specifically, the infotainment system. This information can be potentially extracted and analyzed by third parties.

2.2 Internal Communication Buses

Modern vehicles now make use of many computer buses within their internal components to send and receive operational messages. ECUs process this data then actuate mechanisms to accomplish tasks requested by the vehicle's user. Vehicles are starting to resemble actual computer networks and each component can be viewed as a node for passing or processing information. Some of these components and buses are segregated from one another for compartmentalization; however, they are all able to communicate with one another to fulfill the vehicle user's demands using the Control Area Network (CAN) bus. As per Everett and McCoy [17], there are multiple modules/units and respective buses and they are each responsible for specific traffic flow inside the vehicle. The following list is the core networking buses within a vehicle for data exchange:

- CAN (Controller Area Network) – Core bus that links all buses together for data exchange and provides an interface for on-board diagnostics

- LIN (Local Interconnect Network) – Sub-network used for low-speed and bandwidth applications. For e.g., doors and sliding windows up and down
- FlexRay – Sub-network used for safety critical and high-speed messages. For e.g., vehicle stability control and embedded sensors
- MOST (Media Oriented System Transport) – Sub-network used for high-speed and bandwidth multimedia related applications. For e.g., music/video streaming and vehicle cameras

The following list describes the core modules attached to the aforementioned buses. In general, they are found in modern vehicles and associated internal networks as shown by Everett and McCoy [17]:

- Junction Box – provides typical functions for the vehicle's circuits but in this case, connects the OBD II (On-Board Diagnostics) port to the CAN bus
- Engine Control Unit – Controls actuators for the engine to ensure optimal performance and does so by reading acquired data from multiple sensors through CAN bus
- Multimedia Head Unit – infotainment system in this case, communicates to dash and multimedia displays through MOST bus and can receive data from CAN bus as well
- Stability Control Unit – uses FlexRay sub-network to engage stability control ECUs and actuators and relay/receive information to CAN bus
- Tire Pressure Control Unit – directly affiliated with Tire Pressure Monitoring System (TPMS) for relaying information about each tire through the CAN bus

- HSM (Hardware Security Module) – Stores and secures sensitive data (for e.g., private keys)
- Telematics Control Unit – controls embedded systems (for e.g. GPS unit, 3G/LTE, WiFi communication interfaces) within the vehicle through the CAN bus
- Body Control Unit – uses the LIN bus for engaging door locks, window/side mirror positioning, seat positioning, etc. and relays/receives information through the CAN bus

As mentioned above, the CAN network is responsible for forwarding all traffic that needs to be relayed between each sub-network. It is absolutely vital to the vehicle's operation since it forwards all queries and responses. Error messages also circulate on this network for diagnostic messages. End users are then notified through the vehicle's dash display about a present issue. Access to a CAN bus could lead to great live vehicular forensics if enough data is collected and analyzed correctly. Once connected to the CAN, it could grant potential access to separate modules within the vehicles and their respective ECUs. This could then lead to further vehicular forensic opportunities through non-volatile memory. The network/bus used for infotainment/multi-media traffic is the MOST bus. The MOST bus makes use of optical fiber cables and can now reach speeds of up to 150 Mbps. The speeds achieved by this sub-network hint that a lot of information circulates on this bus type. As mentioned above, access to the CAN bus could potentially lead to further research whether information stored within other buses can be accessed and downloaded (for e.g. the MOST bus being accessed through the CAN and potential for downloading stored data on an infotainment system). Figure 1, shown below, displays a diagram of all buses and modules discussed by Everett and McCoy [17].

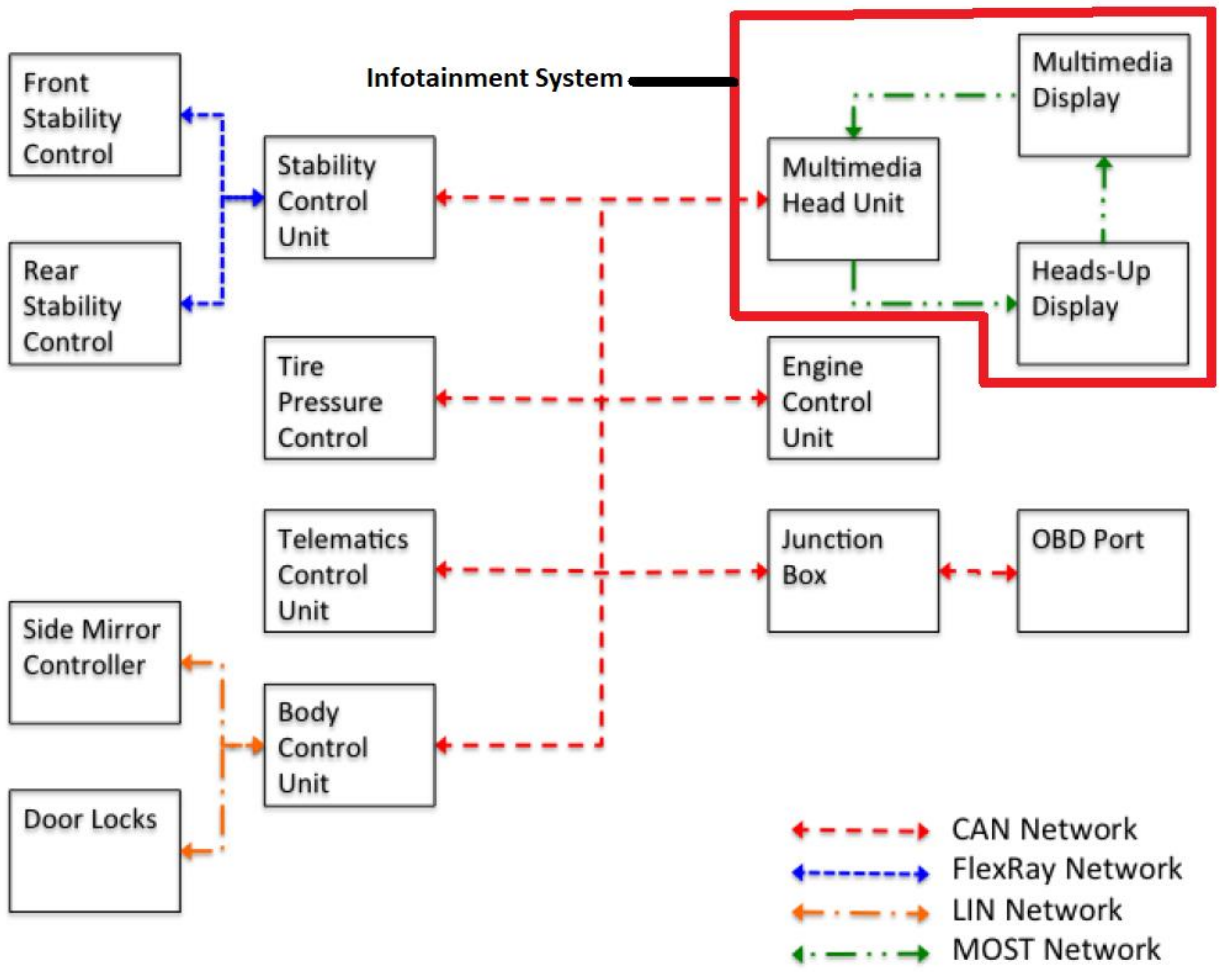


Figure 1. Vehicle Network Components and Buses [17] (original picture edited)

2.3 VANET Security Challenges

VANET security shows that there are many mechanisms being developed to ensure that all security concepts are enforced and maintain a standard of efficiency for the operation of vehicular networks. The mechanisms being developed do have specific reasons and are made to fend off many types of attacks that are present and could potentially target a VANET. It is important to be aware of these types of attacks since internal vehicle network buses and communication components are closely intertwined and the potential for global access of the

vehicle is plausible if VANETs or the vehicles themselves are exploited. Work shown by Rawat, Sharma and Sushil [63] demonstrates these types of attacks. Here is a list of network attacks that affect network communications when it comes to V2V and V2I communications:

- Denial-of-Service (DoS) attacks – as mentioned above, these attacks can target any specific object within the network in hopes of disrupting network service and functionality so that all operations are delayed or rendered useless with the use of excessive traffic and/or over-utilizing key resources in the infrastructure
- Sybil attacks – also elaborated by Yu, Xu and Xiao [79], Sybil attacks are done when a malicious users impersonates multiple identities hoping to fool legitimate users in taking different routes due to traffic congestion protocols
- Message suppression-iteration/falsification – a malicious user manages to drop legitimate traffic in the network in attempts of falsifying road conditions. Alteration is when legitimate messages are altered to fool legitimate users with incorrect data. Falsification is when an attacker broadcasts false information to influence the traffic to his liking or cause havoc
- Replay attack – legitimate messages are captures and used later in legitimate circumstances for illegitimate means
- GPS spoofing – an attacker falsifies GPS information to fool other vehicles into thinking they are at a different location with his/her own GPS simulator
- Tunneling attack – two physically separated parts of a VANET are connected through a tunnel thinking they are neighbours so an attacker could analyze the traffic of perform selective forwarding attacks

- Timing attack – time slots are altered so that safety critical message are delayed and received after their useful lifetime is outlived
- Man-in-the-middle attack – the attacker is between a legitimate communication session and intercepts traffic to see the content but forwards it to the right end destinations to remain invisible
- Home attacks – malicious user attempts to take control of the vehicle's internal components with the use of the Internet
- ID disclosure – a target's location is disclosed and made publicly available so that anyone can view the location of the vehicle
- Brute-force attack – an illegitimate user attempts to break cryptographic keys used in secure communication sessions

All these types of attacks have the potential of affecting VANETs and end users. That is why security standards are being developed so that all fronts are reinforced and that these attacks greatly reduced, if not rendered completely ineffective. These attacks, if well-coordinated, could also lead to the compromise of internal components if vehicles are lured to specific locations which allow an organized attacker to perform more sophisticated types of attacks.

A different attack has been introduced that basically fully compromises a node in the Vehicular Ad Hoc Network. The work presented by Lin et al. [37] demonstrates that a malicious user attempts to physically capture nodes inside the network. Once physical access is acquired, the adversary implements malware as well as attempts to reveal secret keys so that all communications with compromised nodes are known and traffic is exposed. Privacy concerns also arise as location could then be disclosed, not to mention other attacks could be launched including Denial-of-Service, spamming, Sybil attacks, etc. A compromised node could then

affect further nodes attached to it so it can spread into the network and increase its potential regional reach, if not global, up until the entire network is compromised. The only downfall to this attack is that physical access is required so some parts of the infrastructure are not reachable (e.g., highway RSUs) and/or publicly exposed; however, if managed correctly and not caught in the act, RSUs that are not easily physically accessible could fall prey to one that is and be compromised. This type of attack is dangerous as it enables a platform to launch all mentioned above attacks through a seemingly legitimate node of the infrastructure. Overall, many methods are available for attacking a network. Many methods and mechanisms must therefore be deployed and further researched to ensure end user security.

Vehicular Ad Hoc Networks show definite promise in the functionality it is intended to provide. The ability to send information about road conditions, accidents, congestion warnings from indirect neighbours, to name a few, is useful as discussed by Younes and Boukerche [78]. The wireless technology employed to do this is quite efficient in enabling the operations of VANETs, but like any other infrastructure, specifically wireless oriented ones, vulnerabilities to attack the network arise. Rawat, Sharma and Sushil [63] present home attacks that are directed towards taking control of vehicles using, and not limited to, the Internet, so that internal vehicle components are exploited and taken over. Works shown in [10][16] [32][38] [59] present multiple attack surfaces that are exposed through external components and allow compromise of the internal network components of the vehicle objects. There are many attack vectors that are of the following:

- OBD II port – direct physical access to internal components of the vehicle
- “PassThru” device – Device that connects to OBD II port for analysis of system buses and firmware updates

- Media devices (e.g., MP3s, USBs, CDs, etc.) – direct physical access to internal components of the vehicle
- Bluetooth – short range communications access to internal components of the vehicle
- Cellular – long range communications access to internal components of the vehicle
- Broadcast Channels – long range communications access to internal components of the vehicle

The work presented by Checkoway et al. [10] explains how full vehicle compromise (for e.g., vehicle acceleration and braking, to name a few) was attained and all possible ways they have managed to successfully do it. Vehicle objects have shown vulnerability from direct physical access to the vehicle's OBD II port. If an attacker manages to get access to this port when the driver is not present, the culprit can listen in on the internal network components and debug the communication in attempt of reverse-engineering the internal protocols. The user can use packets that he/she crafts, based off the debug output, to take control of the vehicle. This is the most efficient way of compromising a vehicle, but physical access to the port is hard and is noticeable by users since the car has to be broken into. "PassThru" devices, which are used by vehicle manufacturers, authorized dealerships and mechanic shops, are used to update and gain access to a vehicle's internal network components (CANs, LINs, FlexRay, etc.). Once this device is connected, they can update and maintain the firmware, which would be periodically done when a vehicle comes in for maintenance schedules and safety checks. These devices can also use wireless communications and allow an untrusted third party to connect to it. When the device connects to the OBD II port, the attacker could gain access to the internal components of

the vehicle shown by Checkoway et al. [10]. No authentication checks are done by the internal components when a PassThru device connects to it, meaning anyone connected to the PassThru gains automatic access to the OBD II port. Authentication means would need to be implemented to stop this from happening. An attacker could also upload malicious packages to the PassThru device so that whenever it connects to a vehicle, the files are uploaded to the vehicle to compromise the internal network. This method would allow multiple unsuspecting vehicle objects to be infiltrated. Media devices such as CDs and USB devices can also be used to upload malicious information to vehicles if inserted in the proper access channels. It has been show by Checkoway et al. [10] that if CDs contain malformed audio files, they can update the firmware inside the vehicle through a buffer overflow attack.

Bluetooth has also shown to be vulnerable inside vehicles. Checkoway et al. [10] demonstrated that through Bluetooth device and car pairing, the vehicle can be compromised. With the use of "Bluesniff", which is used to sniff and capture Bluetooth MAC addresses, brute-forcing methods can be done to pair to the vehicle. Approximately nine PINs per minute can be brute forced to pair to a vehicle according to trials successfully made by Checkoway et al. [10]. Although this does not sound like a lot of attempts in the given time frame, this technique could be done in a public garage where thousands of vehicles may be present, brute-forcing one within seconds. This is plausible as tests presented by Checkoway et al. [10], demonstrate that a single vehicle was compromised within fifteen minutes. This time significantly reduces when there's more than one vehicle, and, once the device of the attacker is paired to the vehicle, custom applications can be used to gain access to the vehicle's network.

Just like Bluetooth, long range communication means can also be used to exploit buffer overflow vulnerabilities inside the vehicle to fully compromise it. Cellular communication can

be used to breach a vehicle's security, which demonstrates how volatile and dangerous wireless communications can be when exploited. AqLink, a protocol used to send and receive voice communication on cellular channels, has been reverse-engineered by Checkoway et al. [10]. This protocol changes analog bits to digital ones so that they can be interpreted by the internal systems. This opens up the possibility of using audio playback to trigger an exploit that was successfully done in the presented research. They were able to phone a remote vehicle that is within cellular range and play an audio file through an audio device, and it compromised the vehicle through a buffer overflow exploit. The issue with this type of attack is that the transmission speed is limited and can only send data at a certain limited rate; a certain amount of data must therefore be delivered before a timeout occurs to trigger the attack. Well-crafted and short code must be done to successfully exploit the vehicle object. Other mediums such as 3G or addressable channels, such as OnStar, allow for faster delivery mechanism with a much bigger payload, but the vehicle must be within range of 3G transmitters to be contacted. Work discussed by Cai et al. [7] shows that Bluetooth can further be exploited with the use of antennas to boost signals and coupling with devices that have more than one antenna (in this case vehicles). The vehicles do not need to be in line of sight, and with the use of multiple antennas, the vehicle object and Bluetooth device can be paired, making it much harder for an attacker from being detected since visual cues are not available.

Many attack surfaces exist in vehicles for targeting their internal components that interact with the vehicle itself or vehicular network of this infrastructure. In fact, Miller and Valasek [44] and Smith [68] have both published comprehensive guides/handbooks about their research and methodologies used to hack actual vehicles in their possession. Chung [12], Greenberg [24] and The Associated Press [69] reported on both Miller and Valasak's research successes. They were

both funded by the United States Department of Defense (DOD) to look into the matter and that is how their project started in the first place; this shows the interests (and problems) that vehicles can really have, especially if government agencies are willing to find out more about them (also see Markey [41]). Fox-Brewsters [18] reported there was even an open source tool released by an ex-Tesla employee which directly interfaces with the on-board vehicle CAN and takes control of the vehicle if vulnerable. This demonstrates that security standards must be kept under constant revision to ensure that all components are secured and cannot be easily exploited, if not impossible, since security in VANETs is extremely important to ensure end user safety and well-being. Figure 2 shown below depicts a diagram of previously mentioned attack surfaces by Checkoway et al. [10], which are to be considered when it comes to vehicle and user safety, which should be paramount.

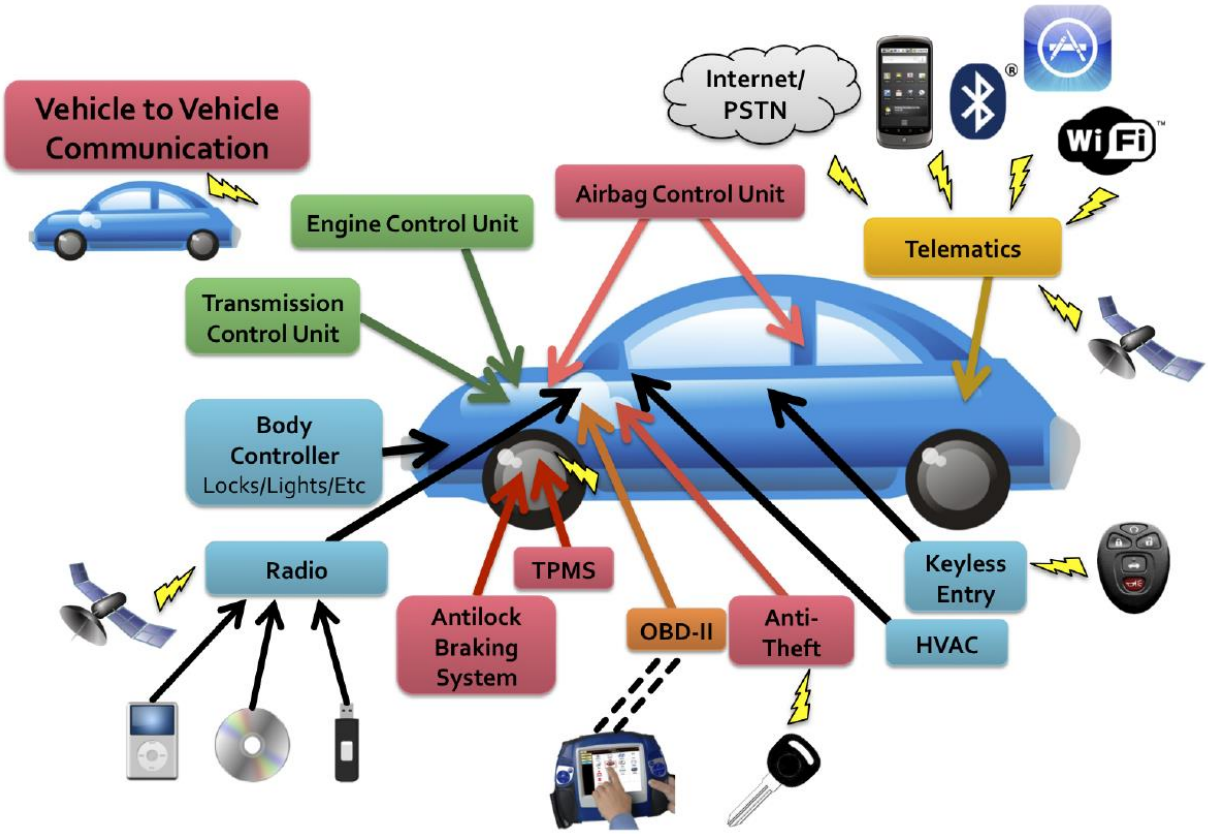


Figure 2. Attacks surfaces in VANETs [10]

Chapter III – Understanding Forensic Analysis

The realm of forensics is all about the analysis of material and evidence so that one can associate it to an event and/or person, especially when crimes are the reason for the investigation in the first place. This subject is quite prevalent in law enforcement agencies as their main goals are to prevent and solve crimes using forensic means. In the current day and age, digital forensics are becoming the norm for finding clues and evidence since many crimes are becoming digitalized or involve it to some aspect. This chapter will discuss generic digital forensics as well as some legal concepts for the province of Ontario in Canada to give the reader an appropriate background of the field and further understanding of the following chapters/sections and main point of the research.

3.1 Digital Forensics Model

As presented by Reith, Carr and Gunsch [64], digital forensics is the derivation of evidence from any type of computer source or device with computational capabilities. The methodologies used to obtain such data is done through specialized software and tools, which allow interpreting the information properly so it can be used to advance and solve investigations. Until recently, there was lack of standardization due to the high complexity of computers and number of methods to acquire data for analysis. Reith, Carr and Gunsch [64] had the objective of establishing an abstract model and framework that law enforcement could use to properly acquire and present digital evidence and is as following:

1. Identification – determination and recognition of different types of incidents
2. Preparation – preparation of techniques, search warrants, tools, management and monitoring authorization

3. Approach strategy – formulate an approach that minimizes impact to victim while maximizing data collection
4. Preservation – ensure that the digital evidence is secured, isolated and not tampered with for further analysis
5. Collection – duplication of data sets using proper tools and methods as well as recording the physical scene
6. Examination – thorough analysis of acquired data sets for specific evidence while keeping detailed documentation of the search
7. Analysis – determination of significance of evidence and making conclusions accordingly based on evidence found
8. Presentation – summarization and explanation of arrived conclusions
9. Returning Evidence – acquired digital and physical property must be returned to rightful owner and have criminal evidence extracted properly off the aforementioned property

These guidelines are used to ensure proper handling of cases when it comes to forensic evidence in general. Other frameworks can be used but in this case, Reith, Carr and Gunsch [64] give a more specific approach to take to ensure evidence integrity and its proper handling. It is important to note that the steps presented can be adjusted accordingly based on the case itself but it is useful to follow a similar process, especially in the case of digital forensics. Overall, as long as steps are taken to respect the following four phases showed by Baryamureeba and Tushabe [6], the entire process should be legitimate:

1. Collection – entire process of collecting evidence and its documentation
2. Examination – visibility of evidence is made clear and explained

3. Analysis – determine value of evidence and its significance for the case
4. Reporting – documentation of entire process and pertinent data recuperated

Some models go deeper and have more steps and phases to ensure legitimate handling of evidence but this shall not be covered as it is not the goal of this research; a general understanding of the framework for a forensic case and its handling will suffice simply for context of the topic.

3.2 Provincial Implications and Processes

When it comes to the legal aspect of forensics, certain laws and regulations must be followed when it comes to acquiring electronic devices from a potential suspect. As per the Ontario Provincial Police in this case as an example, many procedures are established to ensure that the acquisition of said devices and data is correctly acquired and within legal boundaries. Their search warrant guidelines [55][56][57] give a thorough description of what a forensic examiner is expected to obtain while out on a case and analyzing data sets. Guidelines are also presented on how to handle such evidence in the case of court, as shown by Gonzales, Schofield and Hagy [22]. There are respective guidelines to follow for computers (infotainment systems would fall into this category), cell/smartphones and GPS devices when it comes getting and enforcing a search warrant. As long as the specifications of the warrant itself are not overlooked and established restrictions are respected, the suspect will know exactly what law enforcement agencies are entitled to look into when evidence is being analyzed so their expectation of privacy is not violated. For example, a warrant for a computer acquisition can specifically limit the scope of the search to fraud so a forensic analyst would only be entitled to search for files that would show evidence of fraudulent activities. Of course, the warrant itself specifies that the

search itself could entice looking for hidden files/file systems for further analysis but as long as the search itself remains in its scope, it is legal.

As per the Articulation of Categories provided by the OPP [49], it is also important to note that there are different classes of data. Each category helps the investigation in its own way and are as followed:

1. Communications – all data that relates to communication between the suspect and potential accomplices and victims, which includes any of the mediums of communications such as voice, text and multimedia
2. Usage of device – all data that points to the specific usage and time spent on resources by the suspect before, during and after the offence so that patterns can be established and facts verified due to time stamps and system clocks
3. Ownership – all data that links data and computer resources to the owner or respective users to determine if the suspect was involved in specific actions and events on the device since multiple users are a possibility
4. Multimedia content – all data relating to multimedia file types which includes videos, sound recordings, images and their respective metadata to further analyze their potential implications in regards to the suspect
5. Passwords, encryption keys and access codes – all data relating to authorized access of resources within the device or to the device itself since passwords, encryption keys and access codes can be stored anywhere on the device for redundancy, which would allow the forensic examiner to further his investigation without being locked out of electronic resources

6. Device and software configuration – all data that relates to the configuration of the device itself (and installed software) so that the forensic examines can better determine on how to properly proceed with handling the device due to different file system types and potential obfuscation techniques employed by the user to hide data

As a side note, as shown by Raghavan [62], it is important to note that metadata is "data about data" and applies to all data types and artifacts as it exists on all organized data structures (i.e. system/file system metadata, geographical metadata, application-specific metadata, digital image metadata, etc.). The metadata itself is information relating to data types, timestamps of when created and modified, location coordinates, ownership and file size to name a few examples. Separating the different data types acquired makes the approach more systematic and helps clarify the approach used in finding potential evidence. As computers and technology evolves, more and more data sets are available and being stored so it is important not to confuse any of them, especially in a criminal investigation. The articulation of categories [49] is important to know in this case as it applies to every electronic device with storage capabilities regardless of the exact platform.

In terms of other procedures for proper handling of computer related evidence, the OPP provides many more guidelines for physical handling of devices such as analog/digital video evidence seizure, physical seizure of a computer and cell phone/mobile device physical seizure (even relating to specific devices such as iPhones due to proprietary nature) [48][50][51][52][53]. These guidelines basically ensure that data is not corrupted or compromised (i.e. leave powered off devices off, powered on devices on, remove SIM cards if present, do not attempt to brute force passwords, document surroundings, etc.). This will not be

further looked into as simply the knowledge of proper physical handling is needed to understand that data sets could be influenced by its improper handling.

3.2.1 Legal Force Elements

In relation to the articulation of categories and proper handling of evidence [49], specific aspects have direct implications to the legality and integrity of a court case. Park, Lee, Kim and Shon [58] discuss five elements that have legal force:

1. Hash function – these functions generate a pseudo value of fixed length for a program, application or file. Basically a signature unique to a specific digital entity that cannot be replicated due to it changing when its content is also modified. This would ensure that copied images that were analyzed were not modified since their extraction and analysis
2. Logging – it is important to record every step of every process to keep the integrity of the chain of custody intact in between different case phases as well as exact processes performed on the target system
3. Timestamps – every procedure done on a case is sequential therefore having timestamps further preserve the integrity of the case
4. Proven tools/devices – methodologies, tools and devices that have been already proven successful through testing can demonstrate validity of results
5. Reporting – every process and step taken has to be documented in a comprehensive fashion for non tech-savvy individuals in the courtroom for proper understanding of how and what evidence was obtained

3.2.2 Case Law Example.

As per the Court of Appeal of Ontario [14][54], this case law is an interesting example as it demonstrates the handling of cellphones/smartphones by law enforcement with expectation of privacy. To summarize, two suspects were arrested for a robbery and had a non-password protected cellphone that was seized and searched without a warrant on the scene of arrest. Communication-related evidence was found at that time but the suspect claimed it was an invasion of privacy as there was no warrant.

This is the most relevant example in showing that investigators and the court of justice will face challenges when it comes to validating evidence and/or access to a mobile device's data. In our modern times, cellphones (now majorly smartphones) are closely intertwined to our personal lives which directly relates to reasonable expectation of privacy in any case. Reason for probable grounds to search such a device without a warrant at the time of arrest can and will be constantly challenged due to the aforementioned expectation of privacy since smartphones are literally handheld mobile computers (and with the case of computers, they require pre-authorized warrants on their own). They obviously can have evidence on them and help point to other suspects due to (draft) messages and call logs which would be valid reasons of immediate search, but the complexity of modern devices would allow anyone to justify why it is unlawful and for that procedure to not be within the expectation of privacy if not properly justified. The use of passwords and locked screens further complicates the process as they emphasize the expectation of privacy. One would debate that no one is allowed on their respective device for personal and sensitive information being revealed hence why they have a password. As the case mentions [54], for such a device to be searched immediately, four conditions must be met (assuming the contents can be accessed at the time of the arrest):

1. Lawful arrest – suspect's arrest must be valid and based on probable grounds
2. Search is incidental (not the object) of the arrest – Suspect is seen holding hostages at gunpoint and communicating on his mobile device at same time (i.e. potentially talking to accomplices)
3. Search's extent and nature is tailored to the arrest – Using the above example, communications would be the area of interest (so Short Message Service/Multimedia Message Service messages (SMS/MMS respectively – also known as text messages) and call logs and messaging applications only)
4. Search itself must be documented in detail – this is important as without it, some details could jeopardize the case if not noted (e.g. if sent messages were delivered but not read)

There could even be the added reason for protecting the data as devices are now being implemented with methods/encryption schemes that would allow a phone to be completely locked out and made unusable if the screen locks or if a password is required (i.e. as per The Indian Express [70], the Apple vs. Federal Bureau of Investigation (FBI) case – all data is encrypted under the lock screen passcode encryption key which Apple cannot decrypt. The FBI wants backdoor access). This case shows the relevance and potential legal limitations on the technology industry side and/or government entities and could apply to any mobile devices such as infotainment system.

3.3 Digital Forensic Processes

The process of data acquisition can be as easy as connecting the target device to your computer/tool but sometimes it can be as difficult as creating or finding a custom built solution

for it. This also all depends on the platforms involved and available methodologies. Mukasey, Sedwick and Hagy [45] demonstrate that there are many types of device storage due to the information technology environment and its advancement. From personal computers, to portable storage such as USB sticks and external hard drives to more diverse network oriented solutions such as cloud computing. These also employ different hardware platforms for storage ranging from the traditional computer hard drive (HDD) to flash memory chips. Considering the varying existing technologies, different tools and methodologies have been developed to extract data regardless of the platform it is stored on.

3.3.1 Extraction Types.

Generally, when it comes to acquiring data off a device, there are two methods shown by Ashcroft, Daniels and Hart [3]:

1. Physical extraction – This extraction process is done without regards to the file system itself and at the physical level of the drive. Methods used in this include keyword searching across the drive, file carving to search for specific types of files and extraction and examination of partitions and unallocated space to ensure the entire drive is accounted for
2. Logical Extraction – This extraction process is done in conjunction with the file system and will use it to identify directory structures and all file attributes, recovery of deleted files and all metadata used within the file system; another extraction, referred to as a file system extraction, can also be associated to a logical extraction (it may extract additional hidden files or deleted information but generally associated to a logical extraction due to their similar nature)

It is important to note that there is a third type called manual extraction and will be discussed in a later section. File carving at the physical level of extraction is an effective method of recovering specific data artifacts as it looks for types of files. As per Yoo et al. [77], file carving locates specific data artifacts by looking for specific matches of metadata. In this case, the forensic analyst would use metadata provided in the header and footer of the file and seek for specific signature matches which directly identify a file's type. This method is particularly useful for finding specific images or documents. As per Ashcroft, Daniels and Hart [3], this does not mean that some potential evidence cannot be overlooked as techniques exist to conceal the data. An examiner must ensure that the data types are truly what they seem by checking the header and footer of the file's metadata so that they match. The access to compressed and encrypted files is also paramount to an investigation as a lot of data can be hidden there. It is a matter of reversing the process and/or finding these hidden directories to ensure all the data is accounted for potential evidence.

3.3.2 Live Memory Acquisition.

Data acquisition off the storage unit (for e.g. hard drive, flash storage, etc.) is not the only location data can reside on as data extraction from live volatile memory (i.e. Random Access Memory (RAM)) can also hold potential information due to its nature of storing all running information on a device. Vömel and Freiling [73] present many different methods to acquire data stored on live memory:

- Dedicated hardware – use of specialized hardware inserted in PCI slot of computer that makes Direct Memory Access (DMA) operations for a physical copy of the live memory

- Specialized hardware bus – use of the Firewire port to send DMA operations to copy the content of the RAM
- Virtualization – the virtual memory file located on the host PC will contain the suspended memory of the virtual machine that needs to be analyzed.
- Software crash dumps – use of the crash dump files generated when Windows based operating systems unexpectedly halt. These contain the entire memory dump of the system when it was running and can be triggered as well as analyzed by Microsoft owned tools or manual methods
- User level application – use of custom specialized software to extract data from live memory and parsed to readable format
- Kernel level applications – use of specialized vendor distributed software to extract data from live memory
- Operating system injection – use of an independent operating system injected in the target system which creates a snapshot of the volatile data by freezing the state of the host system
- Cold booting – use of artificial cooling on RAM modules after power down to preserve memory contents followed by cold booting of custom operating system that allows the data to be analyzed and extracted
- Hibernation file – use of the Windows based hyberfil.sys when the system state and suspended (i.e. hibernation and sleep mode) which holds a snapshot of the live memory

It is important to know that some of these methods are already well know forensic tools and applications which have been in use for a while for all intended forensic purposes. Extraction of

live memory, when possible, is a definite objective of a forensic case due to the potential information and data sets it holds but some methods are more appropriate than others in terms of deployment and use according to Vömel and Freiling [73] (i.e. kernel level application methodologies and virtualization when available… the other methods have their respective use but more limitations). Seo, Lee and Shon [67] mention an important tool that is used in our research for infotainment system forensics which is 'dd.' This function is a default one on Linux systems and can be used to copy specific portions of the devices including all of the storage blocks and live memory. There are many different tools and applications that can be used enumerated by Rafique and Khan [61] such as Encase, Forensic Toolkit (FTK) and Sleuth Kit (Autopsy) which were also utilized to analyze different file systems in this research project.

3.3.3 Network Related Forensics.

Digital forensics does not limit itself to search for evidence on one specific device or having access to just one. Many services are offered online that allow anyone to communicate with anyone through many mediums may it be instant messaging applications, email services, file transfer protocols, etc. It is important to have a basic understanding of the implications of online forensics and what information is relevant. Gonzales, Schofield and Hagy [23] present and explain aspects of Internet related forensics. Depending on what evidence is being sought, a forensic examiner must keep in mind the following devices and services to check when conducting such an investigation. Gonzales, Schofield and Hagy [23] list them as the following:

- User's computer
- Internet Service Provider of anyone involved
- Log files of involved routers, firewalls, web servers, email servers and any other utilized services

Internet Service Providers (ISP) can also host a lot of information on users when it comes to examining potential evidence. Luckily, there is legal precedence which allows law authorities to get proper warrants for requesting more information about users using that particular ISP. Gonzales, Schofield and Hagy [23] demonstrate the following list of potential information that can be acquired:

- ISP account information – all information relating to the user's account with the service provider (for e.g. name, billing, maintenance notes, caller line identification number, etc.)
- Email address information – all information relating to the user's email address including the address itself, to whom it is associated, the password if it is on file, etc.
- Internet protocol address information – all information regarding the Internet Protocol (IP) details including to whom and when it was registered when successful connections were made
- Domain name information – all the information relating to the identification of the user that registered and manages a specific domain on file
- Web page information – all information relating to the identification of the user that created and manages a specific web page hosted by the service provider
- Telnet session providers – IP history and Telnet logs of the user that made use of the Telnet service for specified time and date
- Point-of-presence information – all the information relating to the Point-of-presence (POP) that issued IP configuration to the user for a specific date and time

- Outgoing telephone records – all information relating to the telephone service employed by the user if subscribed and details of usage (for e.g. outgoing call logs, incoming call logs, voicemail, etc.)

A forensic examiner may also make use of network forensic tools such as WireShark listed by Rafique and Khan [61] which focuses on the analysis of specific network data. Gonzales, Schofield and Hagy [23] mention network elements such as packets and for simplicity, packets can be summarized as the embodiment of data traveling over the internet. They contain the data and metadata in regards to where content is headed and sourced from. Such network elements will contain potential evidence when it comes to solving a case with online connectivity involved.

Overall, all these details combined can help a forensic examiner assemble the pieces much better for finding out more information about the users themselves or getting a lead as to where to look for more evidence.

3.4 Challenges in Digital Forensics

The constant growth of the Information Technology industry is enabling many more advancements in this sector but this does hinder digital forensics. As per Al Fahdi, Clarke and Furnell [1], this will bring technical challenges (such as anti-forensics, steganography, encryption, compression which will further be elaborated in this chapter), legal challenges (such as jurisdiction issues) and resource challenges (such as larger amounts of data to acquire and analyze). This is simply an overall generalization but Zareen, Waqar and Aslam [80] provide much more detail in regards to specific issues, especially on the technical and resource aspects.

The following list applies to the overall field of forensics including mobile and network forensics presented by Zareen, Waqar and Aslam [80]:

- Data protection – storage units and individual chips can be fully encrypted and/or access to devices locked due to passwords
- Data volatility – live memory acquisition techniques required to ensure all data off RAM modules is extracted if a suspect device is found in powered on state
- Operating System variety – many varieties and flavors of operating systems available for multiple devices which can hinder some forensic tools and methods
- Proprietary hardware – for mobile devices, no standards for data and power cables and respective interfaces therefore many cables could be required to extract data off the device
- Hardware changes – for mobile devices, constant change of hardware with newer functions (sometimes added proprietary ones such as new iPhones and iOS password encryption) which sometimes limits compatibility with certain tools and applications
- Application diversity – forensic tools and applications needed for many different application and program data sets due to their easy and diverse availability online.
- Source synchronization – coupling of devices due to synchronization services and functions (e.g. smartphone and computer)
- Third party services – information stored elsewhere through other services based on functionality of different applications and source device (e.g. emails, instant messages, call logs, etc.)

- Short-lived information – Data stored online changes at fast rates therefore a forensic investigator would need to be quick to acquire it if required
- Quantum of network traffic – limitations to capturing full network data sets due to extremely high loads therefore can only be done in segments
- Wireless Networks – malicious activity on wireless networks due to high availability and easier access through masquerade and clandestine methodologies which can hinder forensic examinations

To further elaborate on wireless network related challenges and for an example of an issue in digital forensics and its specific challenges, Mutanga et al. [46] discuss the challenges in regards to evidence acquisition through wireless ad-hoc networks. As previously mentioned, wireless networks are prominent in modern infrastructure to their offered capabilities. Forensic examiners will have to face more situations where wireless networks could potentially be involved in their forensic investigation. Mutanga et al. [46] present these challenges as followed:

- Mobility – wireless ad-hoc networks incorporate mobility due to its nature so it is hard for forensic analysts to determine the exact number of nodes within a wireless network at any given time since connections and disconnections happen whenever due to the range of these networks. Accuracy of collected data can also change due to the proportioned rate of distance to nodes and transmission errors
- Existing security mechanisms – due to implemented security methods and mechanisms in wireless networks to prevent its malicious use and having vulnerabilities exploited, it becomes harder for forensic examiners to remain anonymous or not viewed as a malicious node since evidence needs to be

collected and the network may perceive this as illegitimate actions. Nodes can also be impersonated therefore this hinders the process and adds false positives

- Topology changes – wireless ad-hoc networks can undergo topology changes at any moment due to its mobile nature and this will cause membership issues. A forensic investigator will attempt to determine them and the state of the network based on past events which may be challenging by itself
- Unreliable channels – high mobility networks have higher rate of packet loss therefore potential evidence could also not be lost in the retrieval process
- Multi-hop communications – wireless ad-hoc networks incorporate multiple hops between users therefore tracing the source of data can be tricky. Data can also be modified by one of these hops, especially if a malicious one, which could also be an accomplice of the suspect in an investigation
- Low power devices – wireless access nodes can be low power devices so power constraints are an issue as well as data storage constraints for them due to the power ones. Efficient data collection methods must be developed and/or employed by the forensic investigator to properly retrieve information
- Inter-operability with other networks – it is desirable for wireless ad-hoc networks to function with other types of networks for added functionality therefore tracing the source of a crime is more difficult due to other network types factoring inside the environment

The details presented by Mutanga et al.[46] showcase that even specific forensic environments have their own set of issues and challenges that needs to be addressed.

Although a forensic examiner is faced with many challenges, there are many methods, applications, tools and combination of them that can help solve these issues and by knowing the limitations, a better solution and approach can be taken.

3.4.1 Anti-Forensics.

This section of the chapter will briefly explain the concept of anti-forensics which, as the name suggests, relates to methods and techniques for hindering and compromising forensic analysis. There exist simple ways to do this as explained by Wundram, Freiling and Moch [76]. Three simple to employ methods are encryption, compression, steganography or a combination of them. Encryption simply put is the method of changing data to unreadable format with a specific key (e.g. a password) that can encrypt and decrypt the data. Compression is the method of compacting data to save space on storage devices and alters the content of the target file(s) to accomplish this. Steganography is simply the technique used to hide a particular file into another one, mainly using multimedia files as the source of concealment due to their large size according to Raghavan [62]. These methods have been around for a while but more complex ones have presented themselves to hinder forensic processes. Wundram, Freiling and Moch [76] elaborate further on the goals and target of an attacker/suspect and are listed as followed:

- Attacker's goal
    - Avoidance of investigation through evidence removal or creation altogether
    - Delay of the investigation with manipulation of evidence
- Attacker's target

- Evidence itself – the attacker can try to erase, encrypt and hide data altogether or have large amounts of unnecessary data and use unusual hardware
- Forensic tools – code injection in the forensic tools, buffer overflow exploits, directory loop attacks and changing hash sums in hash databases
- Forensic examiner – pre-contamination of device with forensic traces and well as timestamp manipulation

Malicious file system loops and injections attacks are more sophisticated techniques that can further hinder the overall forensic process. As per Wundram, Freiling and Moch [76], a malicious file system loop has the objective of manipulating entries in the device's file system which point to resources on the storage devices. By changing these values, the operating system may remain in a loop state and this will stop it from executing necessary commands to boot or load specific information. Code injection on forensic tools has the objective of infecting legitimate software for it to report false information. Wundram, Freiling and Moch [76] present an example where the report generating tool of a hacked application executes any command that was written in a specific file accessed by the software. In this case, the entire device can be compromised. Knowledge of these concepts are important due to the fact that suspects may use any means available in attempts of not pleading guilty to computer related charges. Forensic examiners must remain vigilant when facing all the challenges relating to digital forensics.

With all of this said and done, digital forensics will become a continuously harder process as time goes on. As per Garfinkel [19], the methodologies required to acquire and parse information will be harder to come by as more formats are developed; encryption will also become a huge hindrance as these schemes become more and more complex (if possible to solve

at all in the first place that is). Another factor that Garfinkel [19] mentions is the management of data; storage standards are becoming larger and large by the months and it can take weeks to do one simple acquisition off a device which could be problem. This is why continuous research efforts and methodologies must be developed for forensic examiners so that their work flow is alleviated and as much information as possible can be successfully acquired and parsed.

3.5 Mobile Forensics

Mobility within the technology realm has increasingly become more popular, efficient and necessary due to many business and technological processes. Traditionally, digital forensics involve a "static" environment, so to speak, where one investigates large, on-site devices that cannot be moved that easily or hidden. With the evolution of the mobile device and embedded functionalities and more advanced components, these devices can be anywhere (including on the suspect/user) and hold a multitude of information, if not more than a desktop/laptop computer; most mobile devices have embedded GPS hardware to track the location of the user, may it be for safety, navigation of application reasons. The ability to browse the Internet anywhere has majorly contributed to the ever expanding market of cellular/mobile devices as shown by He et al [28]. This trend also applies to criminal activities as these devices enable them to communicate and coordinate more easily as shown by Carney [9]. The following sections focuses on the mobile forensic aspects and delivers an overview of what to expect when it comes to acquiring information off mobile devices.

3.5.1 Mobile Forensics Overview

Over the years, mobile devices have evolved beyond a linear trend; starting off as simplistic devices that use integrated circuits to send simple SMSs and phone calls to become

full fledge mobile computers (also known as smartphones). Although the devices are smaller and less powerful than traditional desktop/laptop computers, Barmpatsalou et al. [5] discuss that the forensic acquisition methods are the same as digital forensics performed on traditional computers. The three main types are:

- Manual – manually browsing through the device to see what is contained on it (may also use a camera to capture pictures)
- Logical – forensic tool extracts all known files and directories on the file system of the device
- Physical – bit by bit copy of the device storage to access all potential information stored on the device

Although manual extraction is prone to human error and potentially alternating data, which is not forensically sound, it should only be considered as an alternative approach and also as a validation technique against forensic tool interpreted data. Logical and physical acquisitions are the best methodologies to extract information on mobile device as the data integrity is preserved and a lot more information can be recovered due to the functions performed by such acquisition methods.

Just like ordinary computers, mobile devices are available in a flavor of different operating systems due to the complex nature of the devices, not to mention multiple manufacturers that offer different features and functionality. Although the market for phones is fierce, Android operated devices are the most popular among the competition according to Barmpatsalou et al. [5]. Other popular operating systems are Apple's iOS, Blackberry's QNX and Windows Mobile. It is also important to note that Android, iOS and Windows Mobile are capable of being given root level privileges through "rooting"/"jailbreaking" methods, which

accesses protected areas of the operating system for added functionalities as reported by Barmpatsalou et al. [5]. These methods can play a role when it comes to accessing and extracting information with forensic tools which is discussed in section 4.4 Acquisition Methods and Observed Data in a later chapter of this paper.

Unlike desktop and laptop computers, mobile devices do not employ traditional hard drives to store data. Barmpatsalou et al. [5] mention NAND flash memory is the main component for storing information as it is compact and highly efficient for these devices that require high storage capabilities. Contrary to hard drives, these are integrated on the device component board itself and cannot be removed like a hard drive. This sometimes makes extraction of data more difficult and would require the chip to be sanded off the component board (known as a "chip-off which can be done through heated and non-heated methods), explained by Ayers, Brothers and Jansen [4]. The chip can then be connected to specialized chip readers for direct access to the data if required since this is a destructive method (the mobile device would no longer work after the flash memory is removed). This method is known to be extremely delicate and complicated since interaction with the NAND chip is required and it could be damaged in the process. Ayers, Brothers and Jansen [4] also discuss Joint Action Test Group (JTAG), another method which is similar to performing a "chip-off" but in a non-destructive matter in most cases. Standards and methodologies are developed to access the data on the flash memory chips through use of the component board itself. As an example, a special connector is connected to the component board (component boards will have input pins on the board for debugging purposes… these can be used for data extraction). These two methods are considered to as a hardware solution for forensic extraction but should not be overlooked as they are effective with mobile devices and the nature of their storage. It is also important to mention

that mobile devices such as cellular phones make use of a Subscriber Identifier Module (SIM) card. These cards allow SIM-enabled devices to communicate with a cellular service provider and stores information such as device contacts, SMS/MMS data, its unique identifier serial number, etc. As shown by Canlar et al. [8], SIM cards used to be the main focus of forensic efforts but due to the evolution of mobile devices, more sophisticated tools needed to be developed to perform all types of data extractions, including the SIM card as it still holds valuable information.

Another challenge discussed by Barmpatsalou et al. [5] that forensic examiners may face when it comes to mobile devices is the use of password/lock screens and encryption of the devices themselves to protect the data stored on the device. Just like a traditional computer, these devices may be subjected to this and makes a forensic acquisition harder, unless the device is still unlocked/turned on. A logical acquisition of any live device will allow access to its files and directories, not to mention acquiring the memory (RAM) of the device. This potentially allows recovery of encryption keys/passwords that would negate the encryption. External media cards can also be encrypted in the same fashion as most mobile devices allow storage expansion through them. These techniques must be kept in mind as it may hinder forensic processes and data gathering due to the evolving encryption standards and features of mobile devices since security and privacy are built-in aspects within the realm of computerized devices since they are highly mobile.

3.5.1.1 Deleted Artifacts

Following the trend of mobility, it has been shown by Glisson et al. [21] that mobile devices hold various data about its users. Due to this nature and somewhat limited storage compared to traditional hard drives, data is moved around more as well as deleted. This could

cause issues when trying to recover data, especially from a logical standpoint. Glisson et al. [21]'s research objective was to determine whether a phone can tell anything about its previous owners after they attempt to completely wipe their phones. A physical acquisition methodology would be needed to ensure that deleted data could be recovered (assuming the unallocated space where the data is stored is not overwritten). Many phones of different brands, price ranges, version models and operating systems were acquired by Glisson et al. [21] for the sample. It is important to note that all of these devices were second-hand therefore had been previously owned and data had been wiped. Three forensic kits (either hardware/software solution or purely software based) were used for the acquisition of data stored on the phones:

- Cellebrite's Universal Forensic Extraction Device kit (UFED)
- XRY Forensics' Examination kit
- Radio Tactics' ACESO kit

Initially, the use of these data kits was attempted to acquire the mobile device data using no SIM cards. If that did not work, a cloned SIM card was used and if that failed, the original SIM card, if present, was used. This specific approach and process allowed Glisson et al. [21] to determine the limitations of the extraction processes based on what components they had; they replicated many scenarios which potential buyers could have access to the old SIM card or not. Table 1 shows the total amount of recovered artifacts after they have supposedly been wiped off the phones. The results shown by Glisson et al. [21] clearly demonstrate that data remnants on mobile devices reside after deleting the original content (in this case, sensitive content was obtained by them). This process helps establish that infotainment system would also hold the information on storage if not overwritten. Second-hand vehicles and respective infotainment

systems possess operating systems that are based off mobile variants due to the mobility of both types of devices.

Table 1. Categorization of recovered artifacts [21]

Type	All	Personal	Personal and sensitive	Deleted	Deleted and personal	Deleted, personal and sensitive
Audio	516	481	0	15	3	0
Calendars	28	26	0	0	0	0
Calls	1,562	0	0	0	0	0
Contacts	1,740	1,470	7	86	86	0
Email	46	28	6	12	12	5
Files	128	5	0	0	0	0
Images	3,100	2,076	180	334	291	2
MMS	44	34	1	0	0	0
Notes	3	2	0	0	0	0
Others	440	1	0	0	0	0
SMS	3,356	2,795	46	1,481	1,310	18
Tasks	3	3	0	0	0	0
Videos	169	97	10	6	0	0
Total	11,135	7,018	250	1,934	1,702	25

3.5.1.2 Forensic Tool Variance

It is important to know that even though many tools are available for mobile forensic acquisition, not all of them do the same job and/or or produce the same results. Glisson, Storer and Buchanan-Wollaston [20] discuss in their paper the variance between different tools and the different acquisition techniques; in this case physical, logical and manual. Three toolkits were compared in terms of forensic ability:

- Cellebrite's Universal Forensic Extraction Device kit (UFED)
- XRY Forensics' Examination kit
- Radio Tactics' ACESO kit

From these three toolkits, Glisson, Storer and Buchanan-Wollaston [20] subjected them all to a logical acquisitions, XRY and UFED to a physical one and ACESO to a manual one. Although each toolkit reported a high successful recovery rate (over 90%) on the artifacts they discovered, this does not mean they reported the same quantity of artifacts; unseen data remnants do not count as part of the recovery rate as they were not attempted to be recovered. Glisson, Storer and Buchanan-Wollaston [20] reported that XRY was the most successful tool being the only one to have the logical and physical acquisition recover more than half of the total amount of artifacts found by all the toolkits. This is important to note as this still does not mean that XRY would be the best solution as artifact verifiability needs to be taken into account; the same artifact found by more than one toolkit and missing artifacts than one toolkit recovered and another did not. This work demonstrates that more than one methodology is needed to detect all potential data remnants and information on any device as this does not only apply to mobile forensics due to the nature of computers and these forensic tools.

3.5.2 Windows Mobile Forensics Overview

An overview of a Windows enabled mobile device is given in this section as some infotainment devices are based off Windows Automotive (Windows OS based off Windows CE). Current Windows mobile phones are all based off the same architecture and base kernel as discussed by Schaefer, Hofken and Schuba [66]. According to them, Windows 7 for mobile devices is based off on the Windows CE 6 kernel. As any other modern operating system, Windows 7 offers these mobile devices the use of a web browser, multimedia applications, social media application, contact integration, etc. In their work, Schaefer, Höfken and Schuba [66] mention that one method to extract data from the phone is to create and install an application in the phone itself that would send stored data to a connected device with little

change to the data itself. This approach has risks as it requires elevated privileges for access to large volumes of data and can potentially overwrite protected data but changes can be documented to ensure data accuracy and that all modifications are accounted for. Mobile application developers for this OS are given limited rights (concept of least privileged applied to developers). The researchers can achieve higher access rights through the use of manufacturer Dynamic-Link Libraries (DLLs) that native applications use. This would allow developer applications methods for elevated calls. At first, the custom application built imports the “Windows.Phone.interopService” DLL which gives access to the "RegisterComDLL" method. This function allows for further DLL importing, specifically manufacturer DLLs. With the use of ChevronWP7, a tool that can be used on a jailbroken phone, the Microsoft publishing process is circumvented and application use on the phone is allowed. Schaefer, Höfken and Schuba [66] made use of a community developed application called TouchXperience and a custom developed application entitled Una, both using client-server architecture with the server running Zune based software. The server would receive data from the phone, order it and present it in human readable form. Read, write and executive rights as well as access to the entirety of the Windows based file system were granted to the users. TouchXperience had slight limitations while Una had less including access to general device information, running processes and the registry. Virtually all the data stored on the phone was accessible through this method. All of this was achieved on a HTC Trophy 7 smartphone. The research discussed by Grispos, Storer and Glisson [25] demonstrate that data artifacts can be recovered without your own custom built solution. UFED, as mentioned above, is a well-known tool capable of doing such extractions and works well with Windows enabled devices as shown by Grispos, Storer and Glisson [25]. Access to registry files, internet history, pictures and videos (acquired through carving or not)

and more would be of great value and some of these tools can help achieve that, if not all. Theoretically speaking, this would also be possible on Windows based infotainment systems embedded into vehicles if the correct methods and tools are used and depending on the generation employed. This is important as current on road Ford manufactured vehicles make use of their SYNC infotainment platform, which run Windows Automotive. Some aftermarket infotainment systems run off Windows CE so similar methods may be applied.

Canlar et al. [8] demonstrated additional techniques of mobile device forensics and data acquisition on Windows based phones. The tool created by this research is called LiveSD Forensics. With the use a custom-built tool developed by Canlar et al. [8] and HaRET (Linux based kernel) stored inside an Secure Digital (SD) card, live data acquisition off the mobile device's RAM can be done as well on Electrically Erasable Programmable Read-Only Memory (EEPROM) chip data access. The only physical step that needs to be done is to plug the SD card inside a phone that has an SD slot. Here is a list of what LiveSD Forensics can achieve based off the work of Canlar et al.[8]:

- RAM acquisition
- EEPROM acquisition
- On-device acquisition
- Control over running processes
- Minimal memory footprint

When HaRET is initiated, the Windows OS state is frozen so that the Linux OS can boot. To ensure no data is overwritten in the RAM, it is dumped onto the SD card for preservation. EEPROM is also secured against data tampering since HaRET reads and writes only to the SD card so data stored on EEPROM is simply read through the custom-built tool's calls. The results

shown put further emphasis that the Windows based environment is vulnerable to data acquisition and these can transfer over to vehicle employing Windows Automotive for infotainment systems. Access to live memory gives access to all types of information on a mobile device as its functions are the limit of what types of data that can be extracted:

- Pictures
- Videos
- SMS/MMS data
- Username
- Passwords
- Emails
- Etc.

This type of information is a gold mine for forensic analysts as live memory acquisitions are not normally encrypted if the acquisition is possible and successfully completed. Canlar et al. [8] help put in perspective the level of access that can be obtained by well-crafted applications and forensic utilities. The ability to perform such tasks through SD cards is noteworthy as another methodology to consider when performing forensic acquisition processes.

3.5.3 Cloud-based Forensics

With such an architecture implemented, millions of network objects would be added on top of daily Internet traffic so the logical choice for application handling would be web based. The work presented by Quick and Choo [60] present possibilities of acquiring data remnants on mobile devices and computers that use cloud storage applications, specifically in this case, Google Drive. With the use of an iPhone 3G and a hard drive used by 36 Virtual Machine (VM) instances running different browsers, the analysis was undertaken. Multiple forensic toolkits

were used as well as WireShark (a tool for Internet traffic analysis) since communication between the cloud service and base machine is a core aspect of cloud storage. Four browsers on a Windows 7 PC were also tested to determine if some would reveal more information than others:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Apple Safari

Based off the tests perform when accessing data on the cloud or storing it, many temporary files and links are created and kept on the file system as Quick and Choo [60] have documented. Files such as “snapshot.db” and “sync_config.db” are easily recoverable and contain path information to where files are downloaded and synchronized as well as URL access links, file sizes, checksum values and resource IDs. Through most cases, usernames can be found in clear text in these files and while doing live web traffic analysis. Account passwords are also disclosed through the use of Internet Explorer and its temporary files it creates. Live RAM analysis has also disclosed the passwords of users using Google Chrome, Internet Explorer and Mozilla Firefox. Similar tests were also done on Microsoft’s SkyDrive (now known as OneDrive) and Dropbox. Key files similar to “snapshot.db” and “sync_config.db” were found as well as the disclosure of usernames and passwords. Table 2 below displays a summary of these results. The results shown here are important for vehicular forensics research as vehicles will make use of such services directly or indirectly, not limited to Google Drive, Microsoft’s OneDrive and Dropbox. These results show that many remnants of data can be found so temporary files and cached data must be regularly wiped although Quick and Choo [60] have

demonstrated that they have been able to locate data remnants after running applications such as "CCleaner" and "Eraser." These programs' functionalities are mainly for deleting temporary Internet files, history, cache and such so being able to recover such artifacts shows forensic potential.

Table 2. Summary of online cloud services data remnants [60]

Service	Client software config files	Username	Password	Mobile device
Dropbox (Quick and Choo, 2013b)	Versions prior to October 2011; **config.db** and **filecache.db**.From version 1.2.48 the files **config.dbx** and **filecache.dbx** are encrypted.	Located near text; **u'email':**	Located in Memory; **free name periods login_email**	Client software: **com. getdropbox. Dropbox. plist**
SkyDrive (Quick and Choo 2013a)	**SyncDiagnostics.log** and **OwnerID.dat**	Located near text; **&login=**	Located in Memory; **&passwd=**	Client software: **keychain-backup.plist'**
Google Drive	**sync_config.db** and **snapshot.db**	Located near text; **? – Email ?? Email <email>**	Located in Memory and on Hard Drive; **&passwd=&passwdagain=**	Browser; **History.plist** and **cookies. Binarycookies**

As discussed in this chapter's section, mobile forensics are becoming increasingly popular due to the fact that virtually everyone has a mobile device to the many functionalities offered by them. The concepts discussed can apply to any type of mobile platform since the operating systems used to power them are a basis of popular known ones which have been already tried and tested forensically. The application of these processes to infotainment systems could leverage results in theory and must be kept in mind due to the impact it could bring to criminal courts with the involvement of telephones in crimes as shown by Carney [9] and their potential interactions with vehicles. Vehicles are already accessories to crimes in some cases therefore different methodologies must be considered and attempted to extract information on them.

3.6 Android Forensics

Operating systems demonstrate great relevance when it comes to the fields of forensics as the more that an OS penetrates a market in terms of popularity, the more that its file structure and

architecture is known and studied. This leads to the development of many tools and specialized software packages for forensic purposes/data acquisition and parsing. This is especially the case when it comes to open source OSs such as the Android platform. Since its inception in 2008, Jovanovic and Redd [31] mentions that the push for open source enables many manufacturers to adapt to it as it cuts down costs for software production. This is a problem as different hardware is interfaced with varying software as manufacturers develop their own distributions of Android. This section of this chapter will give an overview of forensics relating to the Android operating system since it is widely popular and available for all types of platforms including infotainment platforms.

3.6.1 Android Forensics Overview

The Android operating system was developed by a coalition of over 50 mobile technology giants ranging from phone manufacturers to software developers and such (for e.g., Google, Intel, HTC, Acer, Sprint, T-Mobile, etc.). This collaboration effort was known as the Open Handset Alliance (OHA) as discussed by Lessard and Kessler[36]. The OHA's main objective was to offer a standardized platform so that the end user can have an overall better experience with mobile devices.

When it comes to obtaining information off the Android device, it can be stored in multiple locations according to Jovanovic and Redd [31]. NAND flash storage, SD cards or even on the device's connected network. The data that can be recovered through logical or physical acquisition ranges as followed:

- Multimedia collection
- SMS/MMS
- Contacts

- Call Logs
- GPS coordinates
- Internet browsing history
- Application Data
- Etc.

This goes without saying that live memory acquisition of these devices also gives access to information such as relevant application data, encryption keys, usernames, passwords and system services information as discussed by Jovanovic and Redd [31]. Android systems are also susceptible to the same hardware forensic techniques mentioned in the prior mobile forensics section, such as JTAG and chip-off since NAND/EEPROM flash storage is the main method of storing information on these compact devices. Commercial forensic software can also be used to extract such information (this does not exclude freeware solutions). Lessard and Kessler [36] have achieved successful forensic acquisition processes with the use of UFED which extracted a multitude of information including SMS/MMS, contacts information, call logs and multimedia files. This demonstrates that many methodologies are widely available to extract information off Android based platforms and devices.

3.6.1.1 General Acquisition

The Android operating system, just like other mobile devices, makes use of NAND flash memory chips to store information due to the small size but high capacity of this component type. Most Android systems make use of the Memory Technology Devices (MTD) system discussed by Vidas, Zhang and Christin [72]. This shows all memory access points as a single interface. Specific Linux utilities (for e.g., NAND dump) can be used to dump the data off MTD enabled NAND flash memory and if not the case, the built-in “dd” utility (tool that copies data

bit-by-bit in raw format) works and grabs all data from every memory block. Vidas, Zhang and Christin [72] also mention that data might be missing from the extraction process if an SD card is within the device as some application/user data might be stored there depending on which programs are installed on the device and their configuration parameters.

The MTD system itself is divided into multiple partitions for segregating types of data in the Android phone. Regardless of the file system, EXT4 for newer devices or Yet Another Flash File System 2 (YAFFS2), six partitions are typically found on the device:

- System
- User Data
- Cache
- Boot
- Recovery
- PDS (configuration data)

These partitions depend on the manufacturer and extent of functionalities of the device as there might be more than six as displayed in Table 3 below shown by Vidas, Zhang and Christin [72].

To actually perform the entire process of MTD block extraction, there are certain prerequisites required on the Android phone to gain access to the MTD system directly. Specifically, Android Debugging (ADB) must be enabled and the device most be rooted as shown by Lessard and Kessler [36]. ADB enables a host system (in this case, a forensic examiner's forensic computer) to connect to the Android device and communicate with it. ADB's functionalities also range from transferring data freely between devices, sending commands from the host device, debugging the Android device's outputs, browsing its entire file system, etc. ADB can be enabled through "Developer Options" in the system settings menu in

the Android device by toggling the option on. Once it is turned on and the lock screen is bypassed, the device may be connected to the host to start communication session. Lessard and Kessler [36] mention the Android Development Tools (ADT) which are part of the Android Software Development Kit (SDK) and these tools are used by the host machine to detect connected ADB enabled devices. The ADT is composed of tools/utilities that will give root access to the user once executed as performed by Lessard and Kessler [36]. Once this process is complete, the forensic examiner could shell into the device and have root access to all files (not just the files within the file system). From this point on, “NAND dump” or “dd” could be executed to perform a physical acquisition off the MTD partitions. Due to the open source nature and available developer tools/kits for the Android platform, this method in general should always work when it comes to extracting information off any MTD-enabled system due to the NAND flash memory components embedded in all types of mobile devices (for e.g., infotainment systems).

Table 3. General layout and purpose of Android MTD blocks [72]

Path	Name	File System	Mount point	Description
/dev/mtd/mtd0	pds	yaffs2	/config	Configuration data
/dev/mtd/mtd1	misc	–	N/A	Memory Partitioning data
/dev/mtd/mtd2	boot	bootimg	N/A	Bootable (typical boot)
/dev/mtd/mtd3	recovery	bootimg	N/A	Bootable (recovery mode)
/dev/mtd/mtd4	system	yaffs2	/system	System files, Applications, Vendor additions, Read-Only,
/dev/mtd/mtd5	cache	yaffs2	/cache	Cache Files
/dev/mtd/mtd6	user data	yaffs2	/data	User data (Applications)
/dev/mtd/mtd7	kpanic	–	N/A	Crash Log

3.6.1.2 Live Memory Acquisition

As mentioned above by Jovanovic and Redd [31], live memory recovery is important as it holds a multitude of information in regards to user data: authentication credentials and encryption keys being the most notable. Ntantogian et al. [47] have used Linux Memory Extractor (LiME), an open source forensic tool used for live memory acquisition of Android devices. They took a memory dump of a mobile device running thirteen different applications that can be separated in the following four categories:

- Mobile banking applications
- Financial/online shopping applications

- Password Managers
- Data hiding and encryption applications

The important observations made by Ntantogian et al. [47] was that most passwords and usernames could be recovered in plain text format through the live acquisition process. This presents great opportunities for forensic examiners to identify potential users and accessing more information if required. The only issue is that such information can be overridden once application "log-in" is complete; opening any other application or service may delete this data so it is paramount that a forensic examiner acquires the RAM dump as soon as possible as pointed out by Ntantogian et al. [47]. It is important to note that this type of extraction pulls more than just passwords and usernames and such information can be just as valuable to a forensic examiner, therefore these types of extractions need to be attempted whenever the opportunity arises due to the volatility of the data.

3.6.1.3 Live SD Acquisition

The use of external storage methods can also help achieve a physical acquisition of an Android device (assuming certain features are enabled on the device). Chen, Yang and Liu [11] make use of the HTC Desire in their research to run a physical dump process disguised as an Android OS update through the built-in "Recovery Mode" of the device. This mode is used to revert the mobile device to previous versions if the operating system crashes. Chen, Yang and Liu's [11] process involved inserting the tool within an SD card and then into the mobile device. The HTC smartphone was then rebooted and launched into "Recovery Mode" and then selecting the update option as the Android OS detects the "update.zip" file (Android recognizes any file as the "update" file if it is named "update.zip"… if the device is also rooted, any distribution of

Android could be installed). This method of extraction is highly effective if a forensic examiner only has portable forensic tools on external media as it offers a more "mobile" solution if needed.

3.6.2 Instant Messaging Forensics

Many types of application exist on mobile devices for communication sessions between users, may it be for sending emails, accessing social media accounts, SMS/MMS and one finally instant messaging applications. The latter offers one of the most effective way of communication in terms of speed as well as the popularity it has among all mobile devices users. WhatsApp, being the most distributed one among all platforms, especially Android, was acquired by Facebook as shown by Anglano [2]; there is over 400 million active users with billions of messages sent on a daily basis. Mahajan, Dahiya and Sanghvi [40] also mention of the Viber application with over 140 million active users which is still a considerable amount of users among all instant messaging applications. Both were evaluated by Mahajan, Dahiya and Sanghvi [40] due to their popularity. Although their basis service is the same, WhatsApp offers more functionality than Viber and ae as followed:

- Text messages
- Sending/receiving pictures
- Sending/receiving videos
- Sending/receiving audio clips
- Directly sharing contact information
- Group chat
- Voice call
- GPS coordinates

3.6.2.1 Viber User Data

Viber does offer free text messaging and voice call through data usage as WhatsApp requires a subscription fee to make use of its services. It is important to note that the Viber application makes use of a unique "Viber number" to associate the user's mobile device number to the application and both are linked to one another. Through the use of a Cellebrite UFED toolkit, Mahajan, Dahiya and Sanghvi [40] established that Viber made use of three databases to store all of the application's user data:

- Viber_call_log.db – stores call logs
- Viber_data (directory with multiple files) – stores Android metadata, phonebook contacts and data, Viber numbers and calls
- Viber_messages (directory with multiple files) – Android metadata, messages, sqlite_sequence, threads and participants

Their goal was to determine what exact information was stored on Android phones from using the applications (five in their case with varying version of the Android OS). UFED ran its extraction process and managed to pull many types of information from the Viber application. The information could then be viewed with a "SQLite Database Browser" due to the files containing the information were formatted as .db files. Examples of extracted information were recipient phone numbers, source phone numbers, plain text messages, timestamps, etc. Table 4, shown below, displays all types of information found by Mahajan, Dahiya and Sanghvi [40] in Viber user data.

Table 4. Discovered artifacts on Viber [40]

"Viber" Application Artifacts	**Artifacts Found in file "Viber_data"**	**Artifacts Found in file "Viber_messages"**
	Viber Numbers	1. Messages to Viber Users in Plain Text
	Total number of calls done by user	2. Phone No.s to whom messages were sent
	Phone No.s at which calls were made	3.Phone No.s from whom messages were received
	Duration of Calls to each Phone no.	4. Date of sent & Received messages
	Date of Call	5. Phone No. with whom conversation took place
		6. Total number of messages sent to a particular number

3.6.2.2 WhatsApp User Data

As previously mentioned, WhatsApp has many functionalities when it comes to the application itself. Group chat, voice call, sending/receiving multimedia and audio clips,

exchanging contact information from within the application and traditional text messages. Similar to Viber, Android stores database that would hold user data and is shown by Anglano [2]:

- wa.db – contacts database
- msgstore.db – chat database
- msgstore.db.cryptmsgstore-<date>.crypt – encrypted backup of chat database
- UID.j (UID is identifier of specific contact) – avatars of contacts and a backup
- whatsapp.log / whatsapp-<date>.log – log files
- *Various files* – used for storing sent/received files and user configuration for settings and preferences

Compared to Viber, there is much more information stored on an Android device relating to WhatsApp data compared to Viber. Anglano [2] did use a different approach instead of a commercial tool approach such as the use of Cellebrite's UFED kit; Virtualization allowed Anglano [2] to create a software emulated Android device through the YouWave virtualization platform which is known to faithfully replicate Android device behavior. Android version 4.0.4 was utilized as well as WhatsApp version 2.11. Once the virtual environment and the application were setup, WhatsApp was used to generate random data to fill the application's database for test data. SQLiteman and Notepadd++ was used to view the user data; WhatsApp uses SQLite version 3 to store the information within its databases and textual files were produced as well. AccessData FTK Imager version 3.1 was used to then extract the contents of the virtualized environment, in this case the Android WhatsApp's database files.

In the previously mentioned WhatsApp databases, Table 5, shown below by Anglano [2], gives a preview of what to expect in term of messages contents. As displayed, information is shown based on the type of data that was sent or received. Plain text messages are simply shown

within its respective field if the type was set as a text message; a link to data is provided if a multimedia file was sent or received. Notice that longitude and latitude data is also displayed if a user was to send his coordinates to one or multiple contacts. Figure 3, also shown below, gives an example of a multimedia file being sent and its respective metadata that can be found in the Android message database.

Table 5. Messages table concerning content [2]

Field name	Meaning
media_wa_type	message type: '0' = text, '1' = image, '2' = audio, '3' = video, '4' = contact card, '5' = geo position)
data	message content when media_wa_type = '0'
raw_data	thumbnail of the transmitted file when media_wa_type = {'1','3'}
media_hash	base64-encoded SHA-256 hash of the transmitted file (when media_wa_type = {'1','2','3'})
media_url	URL of the transmitted file (when media_wa_type = {'1','2','3'})
media_mime_type	MIME type of the transmitted file (when media_wa_type = {'1','2','3'})
media_size	size of the transmitted file (when media_wa_type = {'1','2','3'})
media_name	name of transmitted file (when media_wa_type = {'1','2','3'})
media_duration	duration in sec. of the transmitted file (when media_wa_type = {'1','2','3'})
latitude	latitude of the message sender (when media_wa_type = '5')
longitude	longitude of the message sender (when media_wa_type = '5')
thumb_image	housekeeping information (no evidentiary value)

Figure 3. Multimedia file being sent [2]

It is important to note that all other mentioned databases share the same features in terms of having the needed fields to identify information about relative user data, shown by Anglano [2] (for e.g., the wa.db contacts' database contains fields that identify the name of contacts and their phone numbers).

This clearly demonstrates that a forensic examiner could use instant messaging applications to pull information about a particular user and find out the activities the user engaged in and full communication sessions between persons of interest. Many types of information are available ranging from potential GPS coordinates, text messages, senders/receivers' information, phone numbers, links to multimedia files (or the files themselves), timestamps (found in message attribute tables as shown by Anglano [2]) and user settings and configuration parameters. The importance of such data can be paramount in investigations and also helps identify persons of interest or users in general. Infotainment systems constantly relay information between itself and connected devices so potential is to be found in information it could store.

3.6.3 Locational Data

As more functionalities are embedded in the millions of mobile devices distributed worldwide, more applications are being tailored to make use of these utilities to their fullest extent. An important aspect of mobility is localization (for e.g., GPS enabled devices/applications). Kramer [34] discusses the relevance of this type of information in his research. The prevalence of social media applications such as Facebook and Twitter encourages users to include their location in any activity they engage; this is especially true when pictures are involved as location data is normally embedded in EXIF data (meta-data about pictures taken with cameras). Kramer [34] also mentions the use of Google enabled services (especially on Android devices) such as Google Maps, which work with exact longitudes and latitudes. This gives a forensic examiner potential in retrieving exact GPS coordinates based on a user's phone activity. This can be particularly useful at linking someone to a specific location based on a specific event.

Kramer [34] developed an application for retrieving localization data on Android devices called DroidSpotter. Its main objective is to seek out locational information off any and every artifact of an Android-enabled platform (in his case, an Android image) and narrow that information down to feasible locations. In his work, Kramer [34] used his personal Twitter account to send a tweet with locational services enabled. A picture taken by his Android device with GPS enabled, was also attached to the tweet. DroidSpotter recovered the longitude and latitude positions of the user when the tweet was sent; EXIF data from the picture could have also been used to determine such localization information. Another example Kramer [34] provided was with the use of Google Maps. When a user searches for destinations through this

service, multiple database are created on the device. The following information was collected from these databases:

- UNIX Timestamps
- Name of Destination
- Latitude and Longitude of Destination
- Latitude and Longitude of Source
- Search History

The information recovered is quite relevant when trying to determine places that a user was attempting to go or has been to. This searches can also help tie the user to a particular location, in this case potentially anywhere depending when and where he made the exact searches.

GPS related information does not just apply to Android-enabled devices as GPS systems/tracking devices can be embedded in virtually anything. The importance of this data can be paramount when a specific location can be tied to a user. Forensic examiners must always hold this type of information as high value due to the implications they can bring. With modern applications having localization used for enhanced usability, potential GPS breadcrumbs can be left everywhere inside digital evidence and can be used to clarify certain events in the forensic analysis process.

3.7 Vehicular Forensics

The current state of vehicular forensics is quite new considering how the field of digital forensics is fresh as a whole versus the already established traditional forensic methodologies which have been around for much longer. With the addition of ECUs and more sophisticated systems such as infotainment platforms, more data is logged and stored in vehicles themselves.

Their high proprietary nature due to the amount of different manufacturers makes accessing this information not as straightforward as a traditional computer running known software on standardized formats. This section of the thesis will present what has been done in the specific field of vehicular forensics as it is still an emerging field and vehicles will only contain more information in regards to themselves and their end users as more technology is embedded into them.

3.7.1 Forensic Potential of Infotainment Systems

Modern vehicles are becoming quite sophisticated in regards to current technologies in terms of internal components. Once VANETs are fully implemented, the added layers of interconnectivity between vehicle objects will bring transportation to the technological frontier. Vehicles are now being embedded with high-end infotainment systems with the goal of facilitating driving with applications and services for user friendliness, efficiency and added security (for e.g., IntelliDrive, a third party device which monitors driver habits, can send notifications out to a third party insurance company if thresholds are broken). These infotainment systems are also embedded with localization services and GPSs for easier navigation. From that being said, it is only natural that these platforms will produce and circulate a lot of data such as media content between external devices, internal logging, localization data, etc. The report written by Wall [74] suggests that third-party navigation systems have and are most likely collecting such information in terms of localization data only.

There are many infotainment platforms currently deployed in the transportation market and are mostly proprietary: Ford SYNC, GM OnStar, BMW Assist, Lexus Enform, Toyota Safety Connect, Hyundai BlueLink, Infinity Connection, Etc. These platforms are some of the interfaces offered to the end users when driving their vehicle. These systems have the goal of

making driving experiences user-friendly and give the driver and respective passengers' constant connection to the vehicle. Applications are offered to interact directly with the vehicle's systems, for e.g., remote start and unlocking/locking doors. Users can stream multimedia content from mobile devices for entertainment experience. On top of this, Thilakarathna, Petander, Mestre and Seneviratne [71] explain that social media applications such as Facebook and Twitter show prominence due to the increased usage of mobile devices and their capabilities, especially now that these mobile platforms are being integrated into vehicle functionalities and infotainment systems. The combination of the former and latter will bring potential to streamlining application services within vehicles. Work shown by Guo, Ahmed and Saddik [26] elaborates on how web services will be an integral part of vehicles since infotainment system are becoming increasingly popular and implemented by default into vehicles due to their utility and potential resourcefulness. The Internet (and its access) will enable these systems to directly interact with web services for increased functionality and entertainment of end users within the vehicle. Finally, Maaroufi and Pierre [39] discuss the potential of VSNs (Vehicular Social Networks) which is the embodiment of the aforementioned since it integrates mobile social media applications into vehicles, which would redefine its entire community and this would allow multiple functionalities and potential.

A lookout for future Android-powered infotainment platforms must also be considered. Recently, many technological giants and vehicle manufacturers have formed a coalition entitled "Open Automotive Alliance" (for e.g. Google, NVIDIA, Ford, Dodge, etc. to name a few – see http://www.openautoalliance.net). This coalition's goal is to provide a common, open source platform for vehicles so that a seamless and safer experience is provided.

Cohen [13] specifically worked with Ford SYNC modules since the automaker developed high-end infotainment systems in its current market. SYNC, as shown by Cohen [13], runs off a Windows-based operating system, Microsoft Automotive, also known as Windows CE. It also employs three generations of SYNC modules, first/second generation being with older vehicles compared to the third one. It is important to note that Cohen's [13] presentation refers to the third generation as the second one and the first/second generation refers to the first one. This will simplify references of a more recent work that talks about these three generations, having the first and second combined. The first/second generation (2007 – 2011 models) separates the SYNC and navigation modules. The SYNC module stores phone related information since it interacts mainly with mobile devices. The navigation module (main head unit with GPS) stores media files and navigation data through the use of a hard drive. The third generation (2011 – 2014/2015) integrates both the navigation unit and SYNC module into one and employs software-locked SD cards for data storage, wireless streaming with 802.11 technology and external media. For first/second generation Ford infotainment modules, all the data of the SYNC module is stored on a NAND flash chip. Cohen [13] shows that through chip extraction, SYNC data can be extracted through raw binary output. It is important to note that the actual third generation of SYNC has been released and integrated in today's current Ford models but not much is known as research is still underway to gain internal access in these modules.

Illera and Vidal [30] showed how it is possible to extract data from Erasable Programmable Read-Only Memory (EEPROM) (discussed below), which allows for more input for data reconstruction. Kopylova et al. [33] have researched ways of reconstructing accident events more accurately through the use of an extended Event Data Recorder (EDR). They have shown four approaches to solidify EDRs:

1. In-vehicle application integration to improve log recording (for e.g., access to sensors and diagnostic modules)
2. Include VANET communications for dynamics and localization of nearby vehicles while accident occurs
3. GPS rectification through witness vehicle data
4. Data sufficiency through rotating logs and use of “accident witness” and “self-involved” crash reporting mechanism

These added methods shown by Kopylova et al. [33] would make accident reconstruction better in terms of event accuracy and detail. The latter, more specifically, uses a threaded approach so that multiple events can be reported at the same time if a vehicle is directly involved in a crash but can report details as a witness to other vehicles part of the accident. Overall, all of these would ensure that all details from every perspective are communicated and stored when gathering information relating to the accident. Since ECUs are accessible and contain data in non-volatile fashion, infotainment systems are suspected of storing information as well. If infotainment information is also kept and stored, the driver’s actions and environment could potentially be determined (for e.g., multimedia volume strength, GPS breadcrumbs, end-destination, etc.). This would help assess an accident reconstruction event much better.

3.7.2 Forensic Challenges in Mobile Ad Hoc Networks

While remaining in the realm of helping authorities better determine event sequences, Mutanga et al. [46] pointed out to the challenges of acquiring evidence through digital forensics. Their research aims at finding better methods of doing so on wireless Ad-Hoc networks, VANETs obviously being taken in consideration in this case. The work presented the added

challenges of evidence collection done onto these types of networks. Here is a list of these issues:

- Mobility – node localization is difficult due to network changes
- Existing security mechanisms – forensics in malicious network are easily detectable
- Topology changes – network state determination is difficult because of constant network condition changes
- Unreliable channels – packet loss due to nature of wireless networks
- Multi-hop communication – source of suspected traffic is difficult to trace
- Low power devices – power constraints for data collection and data selection (except for VANET)
- Interoperability – crime point of origin is difficult to determine

Mutanga et al. [46] showed that Ad-Hoc networks in general give malicious users a simplified method of launching attacks from nodes as a source onto the Internet. This makes it much harder to trace. The use of infotainment system data might help determine points of origin through local GPS data acquisition, breadcrumb trails and end point destination. The use of vehicle cameras might catch the perpetrator in the act (would most likely be using a computer device on board a vehicle or tampering with the controls on his vehicle). Analyzing data remnants of applications used by the infotainment systems could also help determine the malicious user (for e.g., unknown application being used and/or illegitimate uses of legitimate applications). Carney [9] makes a case of mobile devices being used more extensively for forensic investigations due to the rise of mobile devices in criminal activities. Although Carney's [9] work is about mobile phone devices, the mobility aspect still applies to vehicles. Just like mobile

device forensics, vehicular forensics is new and the concepts apply to either, as vehicles will be able to connect to mobile devices through Bluetooth, direct physical interfacing and Wi-Fi hotspots. Vehicles could then store the same information, and mobile forensic laws could apply the same way so it is important to know what is being stored inside infotainment systems. Windows-based file systems are widespread across many types of computerized systems and having Ford SYNC utilize Microsoft Automotive as the base operating system makes plenty of information potentially accessible as Schaefer, Hofken and Schuba [66] have demonstrated through their custom- and community- built forensic tools. In regards to localization data, which is of value to law enforcement for forensics and investigations, Hannay [27] makes a good case for the classification of such data. Table 6 summarizes how localization data would be classified in accordance to type and confidentiality levels since vehicular data acquisition, especially from infotainment systems, would have legal boundaries and must be justified. Some infotainment systems, such as Ford's SYNC modules, have GPSs embedded into them when manufactured. Since the infotainment platform produces this type of data by design, it is clearly highly confidential. It must be determined how this data is stored inside the vehicles, and for how long. Depending on the model and enabled functionalities, these devices will be capable of connecting to external platforms for connectivity such as WiFi and cellular carriers. This can help identify information about a user and his or her whereabouts although in an indirect fashion. Hannay [27] also points out the multitude amounts of metadata produced by current/future in-car applications as well as social media applications which can help place users behind certain actions if enough information is collected. This is why boundaries must be determined, but methods to access and determine how the information is stored must also be established.

Table 6. Classification Summary [27]

Class	Identifying Features	Confidence
Implicit	- Locational by design - Locational information and confidence can be determined without significant external information	High
Connectivity Based	- Locational information dependent on external data sources - Requires additional information to determine location	Variable
Metadata	- Embedded within an artifact as part of secondary functionality - Requires additional information to determine confidence	Limited

3.7.3 Recent Vehicular Forensic Efforts

At this state and time, not much work has been put into digital forensics of vehicles, especially considering the use of infotainment system in modern vehicles. Based off recent trends, security vulnerabilities seem to be the main focus for the research community in the overall field of VANETs and internal vehicle technologies. Checkoway et al. [10], for example, demonstrate how the technology within vehicles can be exploited to compromise and control them. Mejri and Ben-Othman [43] even mention that DoS attacks are more than likely to happen to disrupt legitimate services within vehicles and VANETs. Many counter-measures must be deployed to ensure user safety hence why so much research is invested in the security portion of the field. Wei, Yu, and Boukerche [75], for example, discuss such means of defense and protection with the use of trust based security methods so that interactions are properly evaluated when monitoring communications with third-parties. With this in mind, this suggests why there

is a clear lack of documentation when it comes to the aforementioned forensic field. This therefore raises the question of the potential of research that can be done in this specific field. Some of the first works that touched on vehicle forensics was presented at DEFCON 19 by Cohen [13]. The work demonstrated forensic techniques employed on the Ford SYNC platforms. The researcher has shown vehicle modules can be tapped into to retrieve stored data. Chip extraction techniques of NAND flash proved to be successful using Data IO Flashpak III, which is a hardware-based solution. Overall, regardless of the SYNC generation employed, different information can be extracted and is as follows:

- Bluetooth-paired MAC IDs
- Phone contacts and logs
- SMS messages
- Multimedia files (for e.g., pictures, audio files, videos)
- Navigation data
- Generic car information

The work shown also hints that spare USB ports and JTAG ports are accessible. Media and localization data can be retrieved through the on-board hard drive. The work shows that reimaging the hard drive, exfiltration of data through the upload process and re-flashing the firmware are all successful methods of extracting data from the hard drive. The second/third generation of SYNC, as mentioned earlier this chapter, integrates both the SYNC module and navigation unit using write-protected SD cards that contain the Windows-based OS. If this specific card is not present, the navigation unit simply does not function as a failsafe. Work shown by LeMere's presentation [35] demonstrates that Ford SYNC third generation modules can have data extracted through traditional imaging tools and data analysis. JTAG ports are also

hinted as a possibility and were being looked into for a streamlined solution. Flash chips dumps are also achievable but require a custom-built solution, which was achieved by LeMere [35].

Most vehicles on the road today make use of "black box" modules or a Crash Data Retrieval (CDR) function, also known as EDRs, to collect information pertaining to a vehicle crash occurring locally. The CDR function/EDR stores the data on airbag ECUs since they are well protected as shown by Illera and Vidal [30]. This can be very useful for reconstructing accident events. Illera and Vidal [30] gave a presentation at DEFCON 21 showing how they were able to successfully develop custom hardware at very low cost to read and write data to/from these modules and showed what is needed to build them. Proceeding with this, information kept from the CDR function relates to the vehicle's speed, accelerator pedal position, brake use, revolutions per minute (RPM), etc. When an accident occurs, the data collected by the EDR/CDR function is dumped onto the EEPROM of the airbag ECU. The presentation points out that there are three ways to retrieve this dumped data:

1. Extraction through OBD II port and CAN bus (authentication required)
2. Extraction through airbag ECU module (authentication required)
3. Direct extraction from EEPROM module (no authentication required)

From what Illera and Vidal [30] showed, ECU authentication is not hard to break, but it is much easier without authentication. The presentation showed that the software to analyze the data dumps is free to download but in need of a parser if you do not want to buy expensive hardware that would come with the software. Luckily, their custom hardware comes into play and allows for direct integration of the EEPROM chip for data extraction. The first two methods can also be achieved with this custom hardware since Illera and Vidal [30] show how to break the seed

authentication process. These techniques demonstrate that data retrieval of non-volatile components is possible.

Although research is limited compared to other vehicle related fields such as VANETs, the information provided by the aforementioned work shows promise and potential that infotainment systems can store information within its storage components. It gives a solid baseline of what to expect and what other type of information can be found outside infotainments systems if it was required. As predicted, custom solutions or specialized tools are required to extract information off manufactured labeled infotainment systems but it is not impossible and different methodologies should be explored and utilized to extract the target information off these platforms.

Chapter IV – Vehicular Infotainment Forensic Findings

Throughout the entirety of this research, many types of forensic methods were reviewed to get a better grasp of these methodologies and to understand what types of information are available to a forensic examiner. Although there are many methods, many types of devices are available to users and different methodologies may be required to obtain information from them; this is especially true for the case of infotainment systems which are the main focus of this chapter and entire research. The following chapter will present all methods used to retrieve information from different types of infotainment systems as well as the pertinent data itself. It is important to keep in mind that although some of the data is relevant to law enforcement and user identification, data extraction through infotainment systems could also be used by researchers and any other users trying to better identify the structure of these systems for more than just forensic reasons (for e.g., configuration files to identify potential flaws and exploits).

4.1 Research Objective

As per the hypothesis of this thesis, the main objective is to determine what types of information that can be stored on infotainment platforms and the vehicles they are linked to. The implications brought by this research are varying as it opens many avenues considering the overall realm of technology; digital forensics has evolved over the years to face many challenges and emerging technologies. The nature of forensics can make a fast changing environment a hard variable to deal with considering that documentation and validation techniques must be used for proper forensic preservation techniques and analysis of the data. When new technologies are revealed to the world, regardless of their intended functions, it can be used as an accessory to a crime and because it is new, it might not be well documented (if not at all) and this

makes forensic work for investigators more difficult. They would then need to research the technology in question and understand how it works before any forensic process is undertaken. This is particularly true when it comes to infotainment system found in vehicles. These devices are not the most recent technology standalone, but it is its coupling with vehicles that makes it a new market in terms of forensic research. The vehicle manufacturing industry is absolutely massive with so many makes and models available and due to the proprietary nature of this industry, infotainments systems are custom built themselves and in this case are referred to as OEMs. With each individual vehicle model and make, a different operating system could be used and the hardware can change itself, not to mention various revisions to base operating system and builds of the platforms to ensure that are up to par with current technology and the vehicle market. This demonstrates a clear lack of standardization between various platforms and the vehicle it can end up in. Although Google's Open Automotive Alliance is pushing for standardization across technology firms and vehicle manufacturers, there is still a long way to go if a standard was to ever be imposed across infotainment systems. Android Auto and Apple Carplay systems are a stepping stone for this if it ever happens. Even among aftermarket systems, there are so many brands and flavors to choose from, with each having their own base operating system and builds, that it is hard to keep track of and not many methodologies are available for legitimate forensic processes. Currently, Berla iVe is the only known tool to perform valid forensic acquisitions of OEMs and this will be discussed in a later chapter.

Regardless if standardization will ever see the day of light across these platforms, it is important to state WHY this objective is important and what it means overall, including to law enforcement and investigators. First of all, it is important to know that infotainment system are embedded computer systems, and by that nature they inherent all traits of computer systems

including storage of digital artifacts. This means that they can be used to store potential evidence just like any regular computer system (the whole basis of digital forensics is based on computer systems) which means that any data found on infotainment platforms could potentially be evidence. Such evidence can relate to user activity (pre, during and post said activity), ownership of the device, multimedia content, communication sessions with other users, device configurations and passwords, GPS coordination, etc. All of this information is valid to investigators and their case as it helps them corroborate evidence or even solve a case entirely. Just as any other piece of evidence, these systems are barred to the legal constraints of search warrants. If the search warrant is correctly drafted, then all the recovered evidence within the search warrant's scope is relevant and can be presented in the court of law. This is what investigators seek as they want to solve their cases and use all relevant evidence that can help prove if someone is guilty or innocent. This is why it is important to have a general idea of what infotainment systems can store so if a vehicle is ever seized and has a system like this, that system could hold potential evidence that could swing a case in a complete other direction. We have to acknowledge that these systems are vital to digital forensics and more work and methodologies must be developed to ensure forensically sound means for data acquisition and the parsing of its data.

A concrete example demonstrating the practicality of vehicular infotainment forensics can go as followed: a 2015 Dodge Challenger gets stolen. The culprit abandoned the vehicle and it is moderately damaged. The culprit has not been apprehended as the vehicle was recovered hours after the victim reported the crime. The Challenger has a higher-end infotainment system residing inside the vehicle (OEM manufactured with the vehicle). The investigators acquire a consent form from the victim allowing the law enforcement agency to perform an acquisition off

the device. Once the acquisition is processed and the data is parsed, the agency finds a GPS "breadcrumb trail" in the internal infotainment system's log files. They also find out that an unknown Bluetooth device was connected to the vehicle at a timestamp shortly after the vehicle was reported stolen. The device's name is "John'iPhone4S". The GPS "breadcrumbs" show a few coordinates of local businesses and residences. Of these businesses, cameras were on scene and recorded the vehicle pulling in and the suspect getting out of the vehicle with a clear head shot of the individual. Witnesses are brought in and another suspect is found as the infotainment system's log files demonstrated that a passenger door was opened at a residence linked to a GPS coordinate. After a few days of analyzing the data and following up on leads, the main suspect is apprehended and confesses to the crime.

The example described above showcases exactly why it is important to know what these platforms store as it can help directly solve a crime or corroborate evidence to solidify a case. The recovered information is all potential evidence and in the eyes of the court of law, any evidence is good evidence. We are hoping to make a point to why infotainment system forensics is important and further make case investigators jobs easier. It is important to note that this work is not exclusive to law enforcement as end users of any sort should be aware of what information is stored on the vehicles as it can directly or indirectly identify them. May it be for privacy reasons, the general public must be made aware that a lot of information can be potentially found in their own vehicles, which seems to be dismissed by many, especially with the interconnection of mobile device to infotainment systems. This would allow for more information to be potentially extracted from infotainment systems without even touching the mobile device (for e.g. a personal smartphone). This could further help law enforcement investigators in their

respective caseloads when a vehicle is involved and a mobile device was not recovered for the same implications mentioned above.

4.2 Targeted Infotainment Systems

Just like any manufactured computerized platform, vendors vary from one to the other creating many different systems; this is especially true with Originally Manufactured Equipment (OEM). OEMs, for infotainment systems, vary the most as a manufacturer would build their platform off the base of an OS (for e.g., Windows, QNX and Linux), modify it to their liking including custom proprietary applications, builds and tools. These systems would then be rebranded accordingly and have the source code of the OS kept secret due to being proprietary (for e.g., Current Ford SYNC platforms up until 2015-2016 are running off Windows Automotive but newer models will have a QNX based platform, as shown by Mearian [42]). Realistically, it would not be feasible to include all infotainment system due to limited resources and time; the objective of the research is to determine what is kept on a select few of these systems so that a general understanding can be established as well as concepts for extracting data off infotainment platforms which could then be applied to all infotainment systems due to their similar functionalities and operations. OEMs were not the only systems considered; aftermarket systems were also tested due to the simple fact that infotainment systems can be third-party manufactured and used in vehicles as replacement units or simply adding an infotainment feature to vehicle that did not have one (for e.g., basic trim of vehicle without one or older vehicle that never had option prior to these systems being released). The following is a list of the infotainment platforms that were tested and the type of acquisition performed on the system:

- 2012 Ford Fiesta SYNC Generation I – Physical Acquisition

- 2013 Ford Focus SYNC Generation II – Physical Acquisition
- 2013 Ford F-150 SYNC Generation II – Logical Acquisition
- 2013 Dodge Durango uConnect version 8.4 – Logical Acquisition
- Aftermarket Ouku Windows CE – Logical Acquisition
- Aftermarket Pumpkin Android Kit-Kat 4.4.4 – Physical Acquisition
- Aftermarket Pioneer Android-based OS (Android Auto and Apple CarPlay ready) – Physical Acquisition
- Various Volkswagen infotainment platforms – Manual Acquisition
- Various Audi infotainment platforms – Manual Acquisition

The data sets recovered from these systems will give a solid baseline of what to expect in terms of infotainment content and how it could be associated to end users. Although the acquisition methods vary, these are all valid acquisition techniques which all have their proper place in forensics in general as the methods used to extract such information will always vary depending on specific circumstances and/or, in the case of law enforcement, legal permissions and warrants.

4.3 Acquisition Methods

As stated in the previous section, more than one type of acquisition is used but the interesting aspect of the acquisitions themselves were the technicalities that were faced in acquiring the data. Although the acquisitions were successful, the means to achieve some of them were not traditional methodologies and "outside-the-box" thinking had to be used, especially for aftermarket systems. It is important to note that the acquisitions were not done using write-blockers for aftermarket systems as the interfacing between the host machine and the infotainment device would not allow a connection. Although forensically sound to do so, the

purpose of this research was to simply obtain the data and identify its use and how it is linked to end users. Also, no live memory acquisitions were attempted as realistically speaking, most infotainment systems acquisition methods require the vehicle/infotainment system to be powered off at a certain point before any acquisitions of any type can be made due to the intricacies discussed below; legal reasons such as the need for search warrants for vehicles could also halt this process from the legal perspective. The following sections will discuss the acquisition methods used per-category of system; the acquisition method will be explained first before the respective system results' section if it is the same acquisition methodology used for more than one system; there will be an acquisition sub-section per infotainment platform if its method varies per individual platform or type and it will be presented before the respective results sub-section.

4.4 Acquisition Methods and Observed Data

4.4.1 Audi/Volkswagen Acquisition Method

These systems' data were acquired through manual acquisition; specifically this was done as there were no tools nor established methods for interacting with the infotainment systems developed by Audi and Volkswagen. The manual acquisition involves simply interacting with the systems and using its user interface to see if any data can be recovered or saved to external media. The OWASCO Audi and Volkswagen dealership located in Whiby, Ontario, Canada, helped the research effort by giving us access to their four different previously owned and new vehicles to tamper with in order to determine if data could be recovered by interacting through their respective infotainment system user interfaces. The four vehicles in question were as followed:

- 2013 Volkswagen Passat – previously owned, no GPS and basic infotainment system with limited functionalities
- 2014 Volkswagen Touareg – previously owned, GPS and higher end infotainment system with many functionalities
- 2012 Audi Q5 – previously owned, GPS and high end infotainment system with many functionalities
- 2014 Audi Q7 – new, GPS and high end infotainment system with many functionalities

To access the information, simply turn the vehicle on and interact with the system itself; all available menus and options of the infotainment system were accessed and viewed to determine what type of information was available to any user. Data could be extracted and stored to an external SD card if available and inserted in the system slot (this method applied to all the systems found in sub-section 4.4.2, 4.4.3, 4.4.4 and 4.4.5… please see Various Audi/Volkswagen Manual Acquisition Setup appendix for photos of the acquisition process).

4.4.2 2013 Volkswagen Passat Data (Previously Owned)

This was the first vehicle that was analyzed through manual acquisition. It is important to note that this specific Volkswagen infotainment was basic in terms of functionalities. The system would only show phone related information of currently connected devices including contacts that may have been saved prior to disconnecting the device. Table 7 enumerates the data found on this infotainment while tampering with the UI:

Table 7. 2013 Volkswagen Passat Extracted Information

Data	Data Type	Relevance
Bluetooth Devices	User Data	Lists currently and previously Bluetooth connected devices by user defined name
Contacts	User Data	Lists only contacts of currently connected device

This does not provide much information apart from any other device that was connected to the system in the past. This could be useful for linking a specific mobile device to a vehicle if the device was named something more personal. The display of contacts of the currently connected device could be relevant if the mobile device was still within premise or recovered and kept alive to attempt a connection to the system. Basic infotainment systems do not provide much information but it could still be relevant depending on the given circumstances.

4.4.3 2014 Volkswagen Touareg Data (Previously Owned)

The second vehicle that was analyzed through manual acquisition did offer a higher-end Volkswagen infotainment system with more features and functionalities which showed more promise. The export/import functionalities were enabled on this device which could allow more information to be secured. Table 8 enumerates the data found on this infotainment while tampering with the UI:

Table 8. 2014 Volkswagen Touareg Extracted Information

Data	Data Types	Relevance
Contacts/SIM entries/Call Logs	User Data	Lists all contacts and call logs that were saved to the system (public profile) and current mobile device contacts which includes contacts saved to the mobile device's potential SIM card
VIN Number	System	Identifies the exact vehicle
Number of Programmed keys	System	Displays amount of keys linked to vehicle
Media/Navigation versions	System	Displays system media and navigation versions
General Profiles/Bluetooth Devices	User Data	Lists associated mobile device profiles as well as mobile device names that were connected through Bluetooth
GPS Information	Application Data	Lists exact GPS coordinates of saved locations

Please see the 2014 Volkswagen Touareg appendix for examples of this data. The information accumulated from this type of acquisition shows more relevant information in terms of identifying end users. Leftover contacts, GPS coordinates, call logs, profile information and such can better place end users behind the wheel of the vehicle and even at exact coordinates. This information can be quite useful depending on the circumstances of the acquisition. It is important to note that any information that is imported to the system is then now part of the public profile on the system meaning more information can be exported when this process is performed.

4.4.4 2012 Audi Q5 Data (Previously Owned)

The third vehicle that was analyzed through manual acquisition had a high-end Audi infotainment system with a good set of features and functionalities. Exporting and importing

was part of this system's design which allowed more information to be observed. Table 9 enumerates the data found on this infotainment while tampering with the UI:

Table 9. 2012 Audi Q5 Extracted Information

Data	Data Types	Relevance
Contacts/SIM Entries/Call Logs	User Data	Lists all contacts and call logs that were saved to the system (public profile) and current mobile device contacts which includes contacts saved to the mobile device's potential SIM card
VIN Number	System	Identifies the exact vehicle
Media/Navigation Versions	System	Displays system media and navigation versions
Bluetooth Devices	User Data	Lists all mobile device names that were connected through Bluetooth
GPS Information	Application Data	Lists exact GPS coordinates of saved locations

Please see the 2012 Audi Q5 appendix for examples of this data. The acquired information also shows relevance to a specific investigation as contacts, call logs, GPS coordinates and a Bluetooth device list were observed; identifying potential users of a mobile phone that belong to someone is of great interest. This infotainment system also had the option to password protect user data on the system that would prompt a password screen if the public profile was attempted to be accessed although the feature was disabled. Just as the prior system, importing contacts opens the opportunity for extracting more information at a later time depending how many imports are done on the system.

4.4.5 2014 Audi Q7 Data (New)

The last manual acquisition was performed on a brand new vehicle. Due to not having prior data on the system, the features and functionalities were noted and my personal mobile

device was connected to the system (as all prior systems) for a point of reference. This platform was a high-end Audi infotainment system with similar features and functionalities as the previous Audi system. Table 10 enumerates the data found on this infotainment while tampering with the UI:

Table 10. 2014 Audi Q7 Extracted Information

Data	Data Types	Relevance
Contacts/SIM Entries/Call Logs	User Data	List all contacts and call logs that were saved to the system (public profile) and current mobile device contacts which includes contacts saved to the mobile device's potential SIM card
VIN Number	System	Identifies the exact vehicle
Bluetooth Devices	User Data	Lists all mobile device names that were connected through Bluetooth
GPS Coordinates	Application Data	Lists exact GPS coordinates of saved locations of currently connected device

Please see the 2014 Audi Q7 appendix for examples of this data. Similar to the previous Audi system, relevant information such as call logs, contacts and a Bluetooth device lists could be exported or found on the system though UI browsing. Memory and GPS information was only accessible in relation to the currently connected device so one could not tell the number of entries imported/saved from other previously connected devices and favorited locations. Importing information would work the same if exported later just as in previous systems due to the information being stored publicly.

4.4.6 OEM Infotainment Systems Acquisition Method

During the research stage of the project, it was found (and predicted) that OEM systems would be the most difficult systems to acquire information due to their proprietary status and

interface setups. But this is not the only issue as hardware placement also hinders the acquisition process; normally, to make a system acquisition, one would simply connect the device to a write-blocker which is connected to a forensic host machine (for e.g., a hard drive or mobile device through SATA or USB respectively). Access to these components is pretty straightforward as you simply remove them for their initial location (for e.g., hard drive bay, SD/SIM card trays, etc.). In the case of infotainment system, USB connections do not work as they are only enabled for mass-storage mode (debugging is disabled and re-enabling it may not be done unless access to source code/reverse-engineer is completed). Also, finding the correct module inside the vehicle is quite the task as wires and vehicle schematics are needed in the first place to locate the storage module for the infotainment system. Once it is located, most of the vehicle's dashboard must be unmounted to retrieve it (see Extra appendix for examples of this process).

For our case, we acquired an entire Ford SYNC Gen I infotainment platform off "Sonshine Auto Parts", a junkyard dealer located in Ottawa, Ontario (see the Extra appendix for acquired Ford SYNC device completely separated from the dashboard). The entire Ford SYNC Gen II infotainment system and Dodge uConnect logical acquisition were given to us through the OPP's TCU. Once the Ford modules were in-hand, a JTAG physical acquisition process was performed on the modules' board themselves for all of them. The software and hardware solution used to achieve this was Berla iVe version 1.7.1 which can be used to extract such information and works with some OEM manufactured devices. The JTAG acquisition was set to only read data (no write operations allowed but can be if configured accordingly). The process depiction is shown in the OEM Infotainment System appendix for a point of reference. The process is as followed (applied to all the systems found in sub-section 4.4.7, 4.4.8, 4.4.9 and 4.4.10):

1. Locate storage module
2. Open encasement to expose the components board
3. Connect JTAG pins to proper location on board
4. Run Berla iVe
5. Let the software detect the board
6. Execute acquisition process

The Dodge uConnect logical acquisition, which was already in our possession thanks to the OPP's assistance, had been done through USB port connection with a host forensic machine running Berla iVe and performing its acquisition process… this was the only acquisition process that would have been straightforward and not require extended methods. With this software/hardware solution in-hand, the process can be relatively straightforward as the data is properly extracted and parsed well by it. This process requires the user to be careful when interacting with the hardware of the infotainment system as it can be fragile to many things including breakage and electrostatic discharges.

Important note: The extracted data was viewed through the use of open source forensic tool Autopsy version 4.1.1 (Graphical User Interface version of Sleuthkit) and Notepad++ version 6.4.5. Reports generated by Berla iVe were also viewed as part of the data analysis portion.

4.4.7 2012 Ford Fiesta SYNC Generation I – Physical Acquisition Data

This module was the first to be physically acquired thanks to the Berla iVe tool. The system itself had offered basic infotainment features and functionalities and did not have a built-in navigation unit; its main feature was Bluetooth connectivity to mobile devices such as cellular

phones for facilitating call management and such. Table 11 enumerates all types of information found on this device's physical acquisition:

Table 11. Ford Fiesta SYNC Generation I extracted information

Data	Data Type	Location	Relevance
Device Lists	User Data	/__TFAT_HIDDEN_ROOT_DIR__/ MediaCache/	File that list devices that were connected and their names
Device Serial Number	User Data	/__TFAT_HIDDEN_ROOT_DIR__/ MediaCache/	Files that list devices' serial numbers of all connected devices
Device playlist	User Data	/__TFAT_HIDDEN_ROOT_DIR__/ MediaCache/ /__TFAT_HIDDEN_ROOT_DIR__/ MediaCache/	Files that list devices' artists and songs as well as visited radio channels of all connected devices
Contact Names	User Data	/__TFAT_HIDDEN_ROOT_DIR__/ GrammarFSM/ /__TFAT_HIDDEN_ROOT_DIR__/ Windows/phonebook iVe Report	Arbitrary files list contact names of all devices that were connected iVe report lists all contacts that were downloaded to infotainment system
SMS	User Data	/__TFAT_HIDDEN_ROOT_DIR__/ TxtMsgApp/	Potential SMS information (file content unsuccessfully recovered)
Registry	System	/__TFAT_HIDDEN_ROOT_DIR__/ Documents and Settings/	System.hv registry hive file located (registry viewers could not parse information; some potential information viewable in Autopsy)
User Activity	User Data	/__TFAT_HIDDEN_ROOT_DIR__/ Windows/LogFiles/	Potential user activity recorded by system
Windows Dump	System Data	/__TFAT_HIDDEN_ROOT_DIR__/ Windows/DumpFiles/Ce010103-01/	Windows memory dump files
System Events	System	/__TFAT_HIDDEN_ROOT_DIR__/ Windows/ LogFiles/	System generated events
Internet History	Application Data	/__TFAT_HIDDEN_ROOT_DIR__/ Windows/Profiles/Guest/Cookies/ /__TFAT_HIDDEN_ROOT_DIR__/ Windows/Profiles/Guest/ Temporary Internet Files/Content.IE5/ /__TFAT_HIDDEN_ROOT_DIR__/ Windows/Profiles/Guest/History/ History.IE5/	index.dat file located but functionality on system was disabled (potential internet history if feature would be enabled and used)
Bluetooth Addresses	User Data	iVe Report	Bluetooth MAC addresses
System Information	System	iVe Report	Infotainment system information
Files	System	iVe Report	All files that were extracted in the acquisition

Please see the 2012 Ford Fiesta SYNC Generation I – Physical Acquisition appendix for some examples of the acquired data. As we can see, a lot more information was extracted from this type of acquisition. All contact names that were downloaded are shown including playlist information on a per-mobile device basis which is of important relevance when trying to identify end users. Serial numbers and Bluetooth MAC addresses can be tied to specific devices that were connected to the vehicle which will be then linked to an end user. System generated events can also show potential user activity (for e.g. USB device connecting to the system include names of files stored on it for potential clues). The information discovered on this device would help forensic examiners get a better grasp of their respective cases in hopes of identifying relevant information simply with the connection of a mobile device to the infotainment system.

4.4.8 2013 Ford Focus SYNC Generation II – Physical Acquisition Data

This module's physical acquisition, compared to the first generation, extracted more information due to the fact that this infotainment system had more features including a navigation system. Bluetooth connectivity was also observed and demonstrates relevant data. Table 12 enumerates all types of information found on this device's physical acquisition:

Table 12. Ford Focus SYNC Generation II extracted information

Data	Data Type	Location	Relevance
Bluetooth Data	User Data	iVe Report	Lists all devices that were connected including name and MAC address
Device Serial Number	User Data	iVe Report	List devices' serial numbers of all connected devices
Call Logs	User Data	iVe Report	Lists call logs of connected devices.
SMS	User Data	/img_partition3.img/	Canned SMS data was extracted; potential for user generated as feature may not have been used
Email	User Data	/img_partition2.img/Documents and Settings/ /img_partition2.img/cache/syncp/ iVe Report	Emails that were parsed by the extraction (probably from contact information) syncp folder had no emails in them (feature might of not been used)
Log Files	System	/img_partition2.img/$CarvedFiles/	Log files relating to interactions with vehicles by end users and system
System/ Configuration Files	System	/img_partition2.img/UATemp/ /img_partition2.img/ssl/ /img_partition2.img/Installer/cache/	System and configuration files, certificates and potential security keys which could be used to exploit the system further if needed ECU responses to infotainment system also found
Contacts	User Data	/img_partition2.img/Nuance/VCA/ /img_partition2.img/Documents and Settings/	All devices' contact names and phone numbers
Media Playlists	User Data	/img_partition2.img/Nuance/VCA/ /img_partition2.img/Gracenote/	Media related information of all connected devices
Registry	System	/img_partition2.img/Documents and Settings/	System.hv registry hive file located (registry viewers could not parse information; some potential information viewable in Autopsy)
Odometer Readings	System	iVe report	Odometer readings
Navigation data	Application Data	/img_partition3.img/ iVe report	Some GPS coordinates/breadcrumbs have been extracted and timestamped
User Activity	User Data	/img_partition3.img/ iVe report	User vehicle interactions are recorded such as system time change, when vehicle doors are opened, when the driver shifts gears and USB connections to infotainment system
Files	System	iVe Report	All files that were extracted in the acquisition

Please see the 2013 Ford Focus SYNC Generation II – Physical Acquisition appendix for some examples of the acquired data. As seen in the prior analysis of the first generation SYNC, the second one pulls similar expected results and additional information due to the added functionalities of the device. As per usual, contacts, device lists, media playlists, system events and such can be retrieved for identification purposes but the exception here is that more debugging information is produced and logged by the system such as when doors are opened and closed or gears are shifted. This is particularly useful if a forensic examiner was trying to associate an end user to a specific location since GPS breadcrumbs were also collected in the extraction. GPS data is extremely useful and can place the vehicle at exact locations which help determine specific circumstances for end users and where they may have been at specific times. It is important to note that GPS coordinates are also associated to user interactions to the system and vehicle shown in the iVe reports. Potential SMS and email entries are also useful as additional information about a particular investigation may be put to light and/or helps to identify end users if available.

4.4.9 2013 Ford F-150 SYNC Generation II – Logical/File System Acquisition Data

This extraction is similar to the previous one since both system were of the same generation but on a different vehicle. The content will be more limited in terms of observed information as the data acquisition was given to us directly (no image) by the OPP for analysis and at the time Berla iVe did not generate reports and had limited support for the extraction process. The fact that only the file system extraction was given makes it similar to a logical acquisition and therefore the recovered data set is more limited compared to a physical extraction. Table 13 enumerates all types of information found on this device's logical acquisition:

Table 13. Ford F-150 SYNC Generation II extracted information

Data	Data Type	Location	Relevance
Email	User Data	/4D902EB42600_11806208/0000000001/ FileSystem/cache/syncp/	Email folder found with inbox and outbox (feature was not used so it was empty)
Internet History	Application Data	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/Profiles/guest/	Internet history related folders found but empty due to unused or unavailable feature
Call Logs	User Data	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/Phonebook/	XML file found containing a call log on a per-device basis
Device names	User Data	/4D902EB42600_11806208/0000000001/ FileSystem/Nuance/VCA/	File containing device names
Bluetooth MAC	User Data	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/Phonebook/	Folder that lists each connected device as per the Bluetooth MAC address
System/ Configuration Files	System	/4D902EB42600_11806208/0000000001/ FileSystem/ssl/ /4D902EB42600_11806208/0000000001/ FileSystem/Installer/cache/	System and configuration files, certificates and potential security keys which could be used to exploit the system further if needed ECU responses to infotainment system also found
Log files	System	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/LogFiles/	Log files tracking user interactions with infotainment system and vehicle as well as odometer readings and GPS coordinates
Navigation Data	Application Data	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/LogFiles/ /4D902EB42600_11806208/0000000001/ FileSystem/UserData	GPS coordinates/breadcrumbs were found
Odometer Readings	System	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/LogFiles/	Odometer readings were discovered
Media Playlists	System	/4D902EB42600_11806208/0000000001/ FileSystem/Windows/LogFiles/	Visited radio stations are listed

Please see the 2013 Ford F-150 SYNC Generation II – Logical Acquisition appendix for some examples of the acquired data. As observed, some minor variations compared to the content acquired from the Ford Focus as there is less due to the format the data dump was given. The device was also not heavily utilized and relatively new when it was recovered and initial acquisition was done. The important things to notice is that regardless of the format (had to use traditional file explorer method to traverse logical acquisition), relevant information was still found such as phone book and email folders, potential Internet history, media playlists, GPS coordinates and so on as shown above. This data set is quite relevant as it shows data can still be extracted and analyzed even if less effective means were used to traverse the given file system and its respectful data; forensic analysts are sometime require to work with whichever means they are provided to identify whatever relevant information they are seeking.

4.4.10 2013 Dodge Durango uConnect version 8.4 – Logical Acquisition

The logical acquisition of this device permitted me to access a good data set with valuable information within the device. This infotainment system was higher-end in term of features and functionalities including WiFi capabilities for devices within the vehicle as well as typical Bluetooth functionality. Table 14 enumerates all types of information found on this device's logical acquisition:

Table 14. Dodge Durango SYNC uConnect version 8.4 extracted information

Data	Data Type	Location	Relevance
Screenshots	System	Extracted with acquisition and stored within a variable named folder in acquisition folder	Any screenshot taken on the system is saved
Contacts/Call logs	User Data	/ExtractedPartitions/fs/etfs/usr/var/wicome/ /ExtractedPartitions/fs/etfs/usr/var/speechTEFiles/extPhones iVe report	Lists all contacts and call logs of all devices stored in many arbitrary named files
SMS	User Data	/ExtractedPartitions/fs/etfs/usr/var/wicome/ ive report	All SMS data sent through infotainment system can be observed in clear text
Device List	User Data	/ExtractedPartitions/fs/etfs/usr/var/wicome/ iVe report	Files list device brand, model, version and Bluetooth MAC address of all connected devices
Emails	User Data	Extracted by iVe	Lists all emails that were downloaded by infotainment system (probably through contact information)
Installed applications	System	/ExtractedPartitions/fs/etfs/usr/var/speechTEFiles/apps/	List of installed applications on the system
User Activity	Application Data	/ExtractedPartitions/fs/etfs/usr/var/qdb/	“pim” file reports on user related activities (Dropbox was used to upload pictures)
System Events	System	/ExtractedPartitions/fs/etfs/usr/var/qdb/	System generated events under “key_value” which can also correlate user activities
System Information	System	/ExtractedPartitions/fs/etfs/usr/var/qdb/ iVe report	“mme” file displays some system information such as default WiFi password shown in clear text Infotainment system information
Odometer Readings	System	iVe report	Timestamped odometer readings are displayed
Files	System	iVe Report	All files that were extracted in the acquisition

Please see the 2013 Dodge Durango uConnect version 8.4 – Logical Acquisition appendix for some examples of the acquired data. As observed through the data analysis, many types of information can be recovered from even a logical acquisition. The infotainment system provided information such as SMS data, all contacts and connected devices, system information, emails linked to the devices and so on. This information is again extremely valuable to forensic examiners as it will lead to the identification of the system end users.

4.4.11 Aftermarket Infotainment Systems Acquisition Method

The acquisition process for aftermarket systems required a bit more research and use of third-party tools to properly establish a connection between devices. Just like OEMs, USB connections are only enabled for mass-storage mode/multimedia content and USB debugging is also disabled. Now, because these systems are aftermarket, there are methods that were tested/discovered for enabling debug mode on either USB or other interfaces. This enabled means of data extractions on systems that initially had such features disabled. Each system below will have a separate acquisition sub-section explaining the process as each platform differed when acquiring its data.

Important note: The extracted data was viewed through the use of open source forensic tool Autopsy version 4.1.1 (Graphical User Interface version of Sleuthkit) and Notepad++ version 6.4.5.

4.4.12 Ouku Windows CE – Logical Acquisition

4.4.12.1 Acquisition Method

As mentioned just above, USB debugging for this device was disabled. The user interface (UI) on the device offered limited functionalities and configuration settings. The most important thing that was taken note was the fact that this was a custom UI running on top of a

Windows system. After further testing, it was noted that the GPS functionality enabled on the system could be activated through path execution; in other words the GPS button on the system would traverse a predefined path and execute whichever EXE located there, which initially was a GPS application. Here are the steps in order executed to hijack this call and initialize acquisition process:

1. Remove GPS micro-SD card from system tray
2. Load Windows CE tools in micro-SD card
3. Place back into system tray
4. Change path to GPS executable to point to folder with Windows CE tools
5. Press GPS button on system
6. Windows CE executable hijacks UI call and runs “explorer.exe”
7. Windows Explorer is loaded and file system is fully accessible
8. Execute “MortScript.exe” which copies file system to micro-SD card

Please refer to the Ouku Windows CE 6 Infotainment System appendix. It is also important to note that the Control Panel could be accessed through Windows Explorer and USB debugging could be enabled through a system call (initially disabled). This would allow a host forensic machine to browse the device through Windows Mobile Device Center as an alternative.

4.4.12.2 Observed Data

This system had to be heavily tampered with to get passed its limited built-in UI. With the use of third-party tools, a file system (logical) dump was achieved by copying all the contents to an external micro-SD card connected to the system’s GPS slot to bypass mass-storage mode. The functionalities of the device include typical Bluetooth connections and a GPS application for

a built-in navigation software package. Table 15 enumerates all types of information found on this device's logical acquisition:

Table 15. Ouku Windows CE extracted information

Data	Data Type	Location	Relevance
Navigation Data	Application Data	/iGO/save/profiles/01/	Favorited locations of any users are saved in the user.upoi file
Contacts	User Data	/Residentialflash3/BT/	Files store contact phone numbers and names
Call Logs	User Data	/Residentialflash3/BT/	Files store all call logs
SMS	User Data	/Residentialflash3/BT/	Potential SMS data is stored on the system at this location but may not be extracted (resources in current use by system)

As initially predicted, not only to the limits of a logical acquisition but to the limitations of the tools, not as much data was extracted from aftermarket systems although some relevant information was still acquired. Although the files were malformed and in unspecified formats, phone contacts and names and call logs were still retrieved. Potential SMS information was viewable in the same location as the contacts and call logs but could not be extracted due to the OS being unable to liberate these files. GPS information was discovered as well which can be valuable to a forensic examiner as it could link end users to specific locations. Another important note to take is that more information was viewable during live acquisition including the registry but the files would not be allowed to be copied out of the system (OS would restrict this action). As much as the registry is useful for data analysis, live memory acquisitions of infotainment systems are highly unlikely due to the car being powered off by the time it is in

possession and tampering with live evidence is a bad practice for forensic examiners. Please see the Ouku Windows CE – Logical Acquisition appendix for some examples of the acquired data.

4.4.13 Pumpkin Android Kit-Kat 4.4.4 – Physical Acquisition

4.4.13.1 Acquisition Method

Similar to the Windows CE system, this Android system also had USB debugging disabled as mass-storage mode is the default mode for USB connections. Normally, ADB can be enabled by accessing developer mode through the systems menu on the device. The device did not have developer options enabled and was not accessible. This causes an issue as ADB could not be turned on for USB ports. Through the use of the "XDA-Developers" forum, it was discovered that root access could be gained through factory settings of the infotainment system. This menu enabled special commands for execution if the right command was entered. The following is the exact process used to enable debugging mode which would allow extraction of data off the Android powered infotainment system:

1. Access Factory Settings menu in Setting menu
2. Enter the following command to enable root access: *#hct#root#
3. Connect infotainment system to WiFi
4. Download terminal emulator on device
5. Access super user privileges in emulator
6. Enable ADB-over-WiFi service in command line
7. Download Android SDK
8. Shell into platform from forensic machine
9. Execute "dd" command on MTD blocks located in /dev directory and save data to micro-SD card to external media

Please see Pumpkin Android Kit-Kat 4.4.4 Infotainment System appendix for specific commands and end result of steps mentioned above. Even with debugging mode enabled, forensic tools could not be connected to the device as it was interfacing with the host device through a WiFi connection which could only be used to deliver commands directly to the infotainment system's command line. This is still quite notable as an alternate method was discovered for accessing root directories of the device which gives access to the entire system as well as running the "dd" utility for data extraction.

4.4.13.2 Observed Data

The following system also produced many issues when it came to the acquisition. After finally enabling the ADB feature, the acquisition itself was successful. The system also had many features including WiFI connectivity, Bluetooth and a navigation application. Although the acquisition was successful and all MTD blocks were successfully imaged to the host machine, parsing the images was not successful (more than one acquisition attempt was made in trying to parse the information but it was unsuccessful). Only the user image (MTD block 11) was successfully parsed but limited information was available as most files could not be read due to their formats (or lack of one) as well as the inability of parsing the certain MTD blocks. Table 16 lists the information found on this device's physical acquisition:

Table 16. Pumpkin Android extracted information

Data	Data Type	Location	Relevance
Google Account	User Data	/img_kitkatIMG12.img/Android/data com.android.google.apps.maps/cache/	This associates a google account to the infotainment system which are needed for some functionalities

Although this is very limited information, the fact that the Google account was found in clear text can be of great relevance when it comes to identifying an end user (a test account was made and logged on to the infotainment system before the acquisition). The rest of the available information is non-existent (a "(2)" depicted by a folder's name in Autopsy means no other files are available as the only folders left in the directory are [parent folder] and [current folder] which are only redirects). Please see the Pumpkin Android Kit-Kat 4.4.4 – Physical Acquisition appendix for some examples of the acquired data. The Google account is normally only associated to one end user and this can be enough information to place an end user inside the vehicle. This analysis is still important as it shows that some systems are still not forensically accessible and that standardized methods need to be developed. Another thing to consider would be that maybe this infotainment system only keeps information about contacts, call logs, SMS and so on live memory and that this data is not stored in any manner; this is possible as the infotainment system could simply re-download the contacts and related mobile device information when a it connects to the system as the infotainment platform this data to properly function.

4.4.14 Pioneer Android-based OS – Physical Acquisition

4.4.14.1 Acquisition Method

This system was also limited to a disabled USB debugging mode as mentioned in this chapter's previous section. Workarounds had to be researched and tested for either enabling ADB or finding an alternative to extracting the information out of this system. It was discovered that during the boot process of the device, any inserted USB stick could trigger the system to boot in a "testmode". This mode enabled debugging by default and the ability to run system

scripts but specific file was needed on the USB device. The process used to enable “testmode” and start the acquisition process is as followed:

1. Format USB memory stick in FAT32 for device computability
2. Create the following file “textmode_a.key” with specifically crafted key and load it into USB device
3. Create “dd” script for MTD system on infotainment device
4. Connect USB device to infotainment system
5. Power on the system
6. Infotainment system reboots in “testmode”
7. “dd” script is executed and data is extracted from the /dev directory and saved to the USB device

Please see the Pioneer Android-Variant Infotainment System appendix for point of reference of method described above. This method proved to be effective and less time consuming. The drawback is that this method is on a “per system” basis meaning it would not work on all Android systems as well as the extraction can only be done through accessing a testing mode which enables scripts to be executed. If WiFi connectivity was enabled on this device, ADB-over-WiFi could potentially be enabled but this was not the case.

4.4.14.2 Observed Data

The following system was the newest one in contrast to all previously analyzed infotainment systems. It did not have WiFi capabilities nor an embedded navigation utility but did allow for the direct interfacing of Android and Apple devices; these features are called Android Auto and Apple CarPlay respectively. These functionalities allow the infotainment systems to make use of the mobile devices’ built-in features such as Internet access and GPS

capabilities. Once the system entered test mode and MTD blocks were acquired, Autopsy was successful in parsing the images. Table 17 enumerates all types of information found on this device's physical acquisition:

Table 17. Pioneer Android-variant extracted information

Data	Data Type	Location	Relevance
Media Playlists	User Data	/img_AVIC_AndroidAuto_FinalImage.img/ Vol_vol24/$Unalloc/	Visited radio stations and connected device media can be located
Deleted Media	User Data	/img_AVIC_AndroidAuto_FinalImage.img/ Vol_vol24/$CarvedFiles/	Deleted media such as images can be located
Emails	User Data	Autopsy extraction	Any email within files can be viewed

Although this is not as much information as originally predicted, there is still information of relevance in associating end users to the infotainment devices such as recovering pictures, viewing media playlists acquired from connected devices and potential emails that may be relayed to the system through other files. Please see the Pioneer Android-based OS – Physical Acquisition appendix for some examples of the acquired data. Based off the Pumpkin analysis and comparing it to this one, it seems like aftermarket systems (and newer Oss) do not seem to store as much user information. This of course is a possibility as infotainment systems, just by their observed behavior, only seem to relay information between connected devices and themselves. This is of course the practical approach when designing such systems as user data sourced from connected devices is stored there originally. This could explain the lack of data for aftermarket systems; this does not go without saying that more standardized acquisition methods should be developed for attempting to acquire more data but it could be a built-in functionality to not store certain personal identifiable information on the infotainment devices. Regardless, the

information discovered can still be of relevance as forensic examiners tend to use what they have to achieve their end goals; any relative information is good information.

Chapter V – Results Implications and Contributions

As stated in the previous chapter, a lot of information can be found in infotainment system (although this can depend on the amount of interactions made by the users, if other systems are linked to the infotainment systems and if the users allow for their devices to synchronize with the infotainment system). It is important that these results are discussed as there is potential to the direct involvement in an investigator's case work. Just like any computer system, not all extracted information is relevant to the investigator's case and the degree of usefulness can vary depending on the type of investigation. The important notion to grasp is that the implications can be huge and life changing, especially if admitted in the court of law as evidence. This chapter will discuss these results further and what they can mean. It is important to note that I have acquired personal experience working as a digital forensic analyst and investigator and these deductions can be made from personal handling of evidence as well as the interpretation of the data and how it can be used as I worked actual cases (not specific to vehicle infotainment systems, but in regards to digital artifacts as a whole).

5.1 Results Summary

The previous chapter has shown many infotainment system data sets being acquired from different platforms from OEM and aftermarket systems alike. This is important as it shows that an acquisition is possible across different vendors regardless of the underlying OS. It also shows variance across the quantity of data acquired as not every acquisition type was the same (manual versus logical/file system versus physical acquisition alike). Infotainment system builds will also cause acquired data sets to vary (OEM versus. aftermarket), not to mention access to the data itself as aftermarket system required creative solutions versus supported forensic acquisition

tools provided for OEM systems. Table 18 below displays and summarize the overall types of data artifacts that were able to be recovered across all the different infotainment system platforms mentioned in the previous chapter ("?" means that there is potential for this information to be recovered and parsed but complications such malformed/unreadable files, features not being used/implemented or file access restrictions were observed):

Table 18. Summary Results Table

	Passat	Touareg	Q5	Q7	Fiesta	Focus	F-150	Durango	OUKU	Pumpkin	Pioneer
Profile/Device Name	☑	☑	☑	☑	☑	☑	☑	☑	-	-	-
Contacts	☑	☑	☑	☑	☑	☑	-	☑	☑	-	-
SIM Entries	-	☑	☑	☑	-	-	-	-	-	-	-
Call Logs	-	☑	☑	☑	☑	☑	☑	☑	☑	-	-
VIN	-	☑	☑	☑	-	-	-	-	-	-	-
# Keys	-	☑	-	-	-	-	-	-	-	-	-
GPS Data	-	☑	☑	☑	-	☑	☑	-	☑	-	-
Software Version	-	☑	☑	-	-	-	-	-	-	-	-
Device Serial #	-	-	-	-	☑	☑	-	-	-	-	-
Device Playlist	-	-	-	-	☑	☑	☑	-	-	-	☑
SMS	-	-	-	-	?	?	-	☑	?	-	-
Registry	-	-	-	-	?	?	-	-	-	-	-
User Activity	-	-	-	-	☑	☑	☑	☑	-	-	-
Windows Dump	-	-	-	-	☑	-	-	-	-	-	-
Internet History	-	-	-	-	?	-	?	-	-	-	-
Bluetooth MAC	-	-	-	-	☑	☑	☑	☑	-	-	-
System Information	-	-	-	-	☑	☑	☑	☑	-	-	-
Files List	-	-	-	-	☑	☑	-	☑	-	-	-
Email	-	-	-	-	-	?	?	☑	-	-	☑
Log Files	-	-	-	-	-	☑	☑	-	-	-	-
Configuration Files	-	-	-	-	-	☑	☑	☑	-	-	-
Odometer	-	-	-	-	-	☑	☑	☑	-	-	-
Screenshots	-	-	-	-	-	-	-	☑	-	-	-
Installed Applications	-	-	-	-	-	-	-	☑	-	-	-
User Account	-	-	-	-	-	-	-	-	-	☑	-
Deleted Media	-	-	-	-	-	-	-	-	-	-	☑

5.2 Various Audi/Volkswagen Infotainment Systems

For this section, we will discuss the meaning of the data types/artifacts discovered on various Audi and Volkswagen infotainment platforms. These artifacts were collected through a manual acquisition methodology meaning it was all done within the infotainment system's user interface and "hidden in plain sight" doctrine. Please refer to sub-section 4.4.2, 4.4.3, 4.4.4 and 4.4.5 to view the specifics of each system data extractions (respectively 2013 Volkswagen Passat, 2014 Volkswagen Touareg, 2012 Audi Q5 and 2014 Audi Q7). The following list will showcase the artifacts collected as a whole across all devices and what they mean on an individual basis for this specific type of acquisition:

- **Bluetooth Devices (name)** – This lists the currently and previously connected mobile devices via Bluetooth. This only displays the name of the device but this holds relevance as it helps corroborate evidence (for e.g. suspect or victim's name as the name of the device) by linking said device to a potential owner
- **Contacts** – Contact information can display potential persons of interest in relation to the device in question (which can include various telephone numbers, email addresses, company name, etc.) and help disprove any claims that the owner of the device does not know a certain individual if said person is in the contacts' list
- **SIM Entries** – Relates to contact information; these entries are specifically saved to a SIM card meaning they are important to the owner
- **Call Logs** – This information shows call records between the device owner and another party; this especially important as it shows that the two parties were in contact at one point and shows user activity (including timestamps)

- **VIN** – This information links an infotainment system to a specific vehicle which is useful to either confirm the vehicle's VIN or if the infotainment system was sold as a standalone unit (taken out of original vehicle) and the need for the identification of the original vehicle is needed
- **Programmed Keys** – Shows if there is more than one key associated to the device (for e.g. investigator looking to find if a vehicle was stolen with a second set of keys versus suspect saying the owner had his keys so it could not be him)
- **Media/Navigation Versions** – Helps determine specifics of an infotainment system and if it can be compatible with forensic tools
- **General Profiles** – This information displays all data saved to the infotainment system from other previously connected devices including call logs, contacts, GPS information, etc. This can help link users to the vehicle and further corroborate the identity of the vehicle's owner
- **GPS Information** – This information showcases "favorited" GPS information and exact coordinates including the "home", "work" and custom saved locations. This is especially useful in identifying the owner of the vehicle and places that he/she may regularly attend. This also places a person of interest at specific locations if said individual ever denies being there

5.3 OEM Infotainment Systems

This section will discuss the various artifacts that were extracted on various Ford OEM infotainment systems (logical/file system and physical extraction types) as well as a logical acquisition off a Dodge OEM system. Logical/file system acquisition extract everything that is

visible within the file system and its traversable tree structure; physical acquisitions will do a bit-by-bit copy of the entire storage space which will included everything found in unallocated space. Please refer to sub-section 4.4.7, 4.4.8, 4.4.9 and 4.4.10 to view the specifics of each system data extractions (respectively 2012 Ford Fiesta SYNC Generation I, 2013 Ford Focus SYNC Generation II, 2013 Ford F-150 SYNC Generation II and 2013 Dodge Durango uConnect version 8.4). The following list will showcase the artifacts collected as a whole across all devices and what they mean on an individual basis for this specific type of acquisition:

- **Bluetooth Devices (name and address)** - This lists the currently and previously connected mobile devices via Bluetooth. The name of the device as well as the Bluetooth MAC address are displayed which holds relevance as it helps corroborate evidence by linking said device to a potential owner (for e.g. suspect or victim's name as the name of the device or linking a seized mobile device to the infotainment platform to place its owner to the vehicle)
- **Device Serial Number** – Similar to the Bluetooth MAC address, this information helps identify a specific mobile device and if it was connected to the infotainment system at any point. This can help place a device's owner behind the wheel of a vehicle or in the very least, as a user of the infotainment system
- **Device Playlist** - This information can help corroborate data extracted from the infotainment system to potentially known information about a user and help identify them (for e.g. device playlist name has first and/or last name of a user or respective children)
- **Contacts** - Contact information can display potential persons of interest in relation to the device in question (which can include various telephone numbers, email addresses,

company name, etc.) and help disprove any claims that the owner of the device does not know a certain individual if said person is in the contacts' list

- **SMS data** - This information can greatly help identify communication sessions between two or many parties and the content of the discussion which can be relevant to an investigation. It also proves whether contact with persons of interest was made and show whether specific plans or events happened (or their respective planning) as well as the timestamps for the communication instances
- **Registry** – The information found in registry files can be of great relevance as it may contain device specific configuration information relevant to the infotainment system, associated users and their accounts, installed applications, user activity, and much more. All this information can corroborate a lot of potential evidence, suspicions and user activity. This depends on the specific hive files extracted and if the file can be parsed correctly (which depends on the infotainment system model and base operating system). Important note: the HV file found could not be parsed by the tools at hand and may need a custom solution to view all of its contents
- **User Activity** – The information found in specific log files correlates to user activity and what applications that have been used on the infotainment system (or relayed to it). This can also include timestamps. The information gathered can be useful as it can place a user accessing specific resources on the infotainment system or used it to perform an action through a mobile device (for e.g. user downloads a specific application through the device's application store and then logs on his/her account through it)
- **Windows Dump** – Although specific to Windows based infotainment systems, the dump file can contain activity held in the memory/RAM of the device which can show a wealth

of information (for e.g. user credentials, user activity, communication instances, call logs, etc.). Important note: The dump file could not be parsed with the forensic tools at hand

- **System data** – This relates to information generated by the infotainment system itself automatically, including "powering on and off" events, communication with internal buses or even ECUs within the vehicle, USB/external media connecting to the infotainment system, related timestamps, etc. This is relevant as it showcases when the device was specifically in use or if specific devise were connected to the platform at certain times which can further help corroborate evidence and/or claims
- **Internet History** – As per its name, this category of data will list the browsing history of users based on their use of Internet browsing clients, not limited to sites visited, timestamps of visits, search terms, downloaded items and so on. This shows relevance to an investigator as it is fully part of the user activity category overall. Important note: the infotainment system this was pulled from did not have a browser so the corresponding directory within the file system did not have any files but shows that the potential is there for infotainment systems with this functionality enabled
- **Files List** – This displays a full list of all files extracted from the infotainment system which can help investigators quickly identify files of potential interest (and check if they are present). This is more to facilitate the analysis as the files themselves would be of actual evidence worth. Important note: this was for extractions done with the Berla iVe tool
- **Emails** - Information found in emails can clarify communication instances between two parties as well as identifying email users, the content of the discussion and timestamps of

communications. Emails are as relevant as SMS data due to the shared similarities in their nature and can display a wealth of information

- **Log Files** – These files hold particular value as they show direct interactions of the vehicle users with the system and vehicle including when doors are opened and closed, gears are shifted, connections of USB/mobile devices to the system and when the system is powered on and off. These specific events all generate GPS coordinates at the time of the happening further helping investigators pinpoint details about the users of the vehicles including their locations, connected devices and potential embarking and disembarking of passengers
- **Application/Service Configuration Files** – These files show information relating to specific configuration of applications and services running on the infotainment system. Although this data does not associate the end users, it can help investigators determine if specific tools are compatible with the device or specific applications and potential exploits that may allow for workarounds if required (for e.g. OpenSSL being used by the Ford SYNC infotainment could have a Heartbleed vulnerable version if unpatched)
- **Odometer Readings** – This information can help determine investigators in assessing and further corroborating the overall journey of the vehicle and if it was left idling or was actually moving if GPS coordinates are strange or remain in same vicinity
- **GPS Information** - This information showcases "favorited" GPS information and exact coordinates including the "home", "work" and custom saved locations. Vehicle and system generated events also generated GPS coordinates which can further be used to prove the vehicle user's exact location at specific times (for e.g. when the vehicle shifts gear and vehicle doors are opened/closed, GPS coordinates are generated). This is

especially useful in identifying the owner of the vehicle and places that he/she may regularly attend. This also places a person of interest at specific locations if said individual ever denies being there

- **Screenshots** – These multimedia-related artifacts can vary in degree of usefulness depending on the exact content that is captured. It can range from a being a trivial picture of a background to a picture of a potential user/owner of the infotainment system/mobile device or picture relating directly to the crime being investigated. Regardless, there is relevance to these if recovered on the infotainment system
- **Call Logs** - This information shows call records between the device owner and another party; this especially important as it shows that the two parties were in contact at one point and shows user activity (including timestamps)
- **Installed Applications** – Just like files list, this information can be useful in identifying all installed applications on the infotainment system which can give an investigator an idea of what to expect and look for when analyzing the extracted information. This is more to facilitate the analysis as the applications and related user data would be of actual evidence worth although it can help corroborate evidence if a person of interest was to deny of ever using an application and this information proved otherwise
- **VIN** - This information links an infotainment system to a specific vehicle which is useful to either confirm the vehicle's VIN or if the infotainment system was sold as a standalone unit (taken out of original vehicle) and the need for the identification of the original vehicle is needed

5.4 Aftermarket Infotainment Systems

This section of the chapter will showcase the artifacts and data types that were extracted on various aftermarket infotainment systems (logical and physical extraction types). Logical acquisition extract everything that is visible within the file system and its traversable tree structure; physical acquisitions will do a bit-by-bit copy of the entire storage space which will included everything found in unallocated space. Please refer to sub-section 4.4.12.2, 4.4.13.2 and 4.4.14.2 to view the specifics of each system data extractions (respectively OUKU Windows CE platform, Pumpkin Android Kit-Kat version 4.4.4 platform and Pioneer Android based version). The following list will showcase the artifacts collected as a whole across all devices and what they mean on an individual basis for this specific type of acquisition:

- **GPS Information** - This information showcases "favorited" GPS information and exact coordinates including the "home", "work" and custom saved locations (depending on the device model, potential for more GPS information is also there). This is especially useful in identifying the owner of the vehicle and places that he/she may regularly attend. This also places a person of interest at specific locations if said individual ever denies being there
- **Contacts** – Depending on the infotainment system, this information displays all contacts from all associated mobile devices (current and prior) which shows potential persons of interest (including their names, multiple telephone numbers, email address, company name, etc.) as well as corroborate whether the owner knows someone or not
- **Call Logs** - This information shows call records between the device owner and another party; this especially important as it shows that the two parties were in contact at one point and shows user activity (including timestamps)

- **SMS data** – This information can greatly help identify communication sessions between two or many parties and the content of the discussion which can be relevant to an investigation. It also proves whether contact with persons of interest was made and show whether specific plans or events happened (or their respective planning) as well as the timestamps for the communication instances. Important note: potential for SMS data was found but the file contents were not accessible due to it being tied to a running process (and could not be extracted for the same reason). The file was found in the same location where call logs and contacts were stored and the file name was suggestive to SMS related information
- **User Account** – This information identifies the infotainment system's users based on accounts tied to applications used by the platform. Although account names don't necessarily identify a user or the owner of the device, it can still be useful in corroborating evidence, especially if a specific account is already being sought in a search warrant. If it is found on the infotainment system, then it helps link the identity of the user and/or which account is being specifically used for specific applications on the infotainment system (this also helps determine user activity specifically)
- **Media Playlist** – This information can help corroborate data extracted from the infotainment system to potentially known information about a user and help identify them (for e.g. device playlist name has first and/or last name of a user or respective children)
- **Emails** – Information found in emails can clarify communication instances between two parties as well as identifying email users, the content of the discussion and timestamps of communications. Emails are as relevant as SMS data due to the shared similarities in their nature and can display a wealth of information

- **Multimedia Content** – The information shown by this data type can be of great importance as it may help identify the owner, victims, potential suspects, etc. The multimedia content can also corroborate other evidence (for e.g. in a drug case, pictures of illicit substances or in the case of child pornography, illicit multimedia content). Timestamps of pictures and EXIF data can also be used by an investigator to further push an investigation

5.5 Forensic Contributions

The body of knowledge in (digital) forensics as a whole is absolutely massive considering how much technology has evolved over the past decades. So many types of computerized platforms have been developed to facilitate our lives for a multitude of reasons. With this, the ability to store and safe keep information has had many perks, including in the context of law enforcement, but the added complexities from the constant evolution and changes brought forth by technology has added challenges in the field of digital forensics. Malicious use of technology and/or malicious intent of accessing data has led to the development of digital forensic suite and tools to tackle such activities. The vast amount and types of computer devices make the process much more complicated so it is important to (try to) stay on top of technology trends to fully understand them and the potential usability of their data, may it be for combatting crime or general understanding/awareness.

The research and content of this thesis has covered and discussed many forensic topics so that a broader understanding of it could be attained and its general theory applied to further advance the field. First of all, the existing documentation on vehicular forensic is very limited so it is clear that the field is new as a whole. Infotainment systems are becoming increasingly

popular and utilized considering technology and its overall daily use. As shown so far, having such systems harbor that much potential information should be of great interest to anyone in the field of digital forensics. This thesis' overall content contributes in terms of education and training as it discusses all the types of data found on these systems and what that data could potentially mean if collected and analyzed. There is already a clear lack of tools to access such data which does not help in spreading awareness of its existence. Law enforcement agencies and the general public must be educated on the potential use or dangers of data residing on these specific computerized platforms. This can give guidelines to know what to look for when attempting to extract information and how the data could be relevant to an investigation (for e.g. depending on the type of investigation, a case investigator could determine if seizing the vehicle could advance and help the investigation). In terms for the general public, this can educate them in the risks of connecting personal mobile devices to the systems and what information could end up on it; this would help them make an informed decision when connecting their mobile devices to the system (for e.g. should we allow the system to sync all of the data to the infotainment platform or limit it/deny it the access). This research's theory can also be applied to train investigators on where to look for specific information at specific storage location if data has already been acquired. It helps them better understand what they can do with it and if they can correlate it to other pieces of evidence. This is why it is important to know what these systems can store as a whole; the importance of establishing a baseline and proof-of-concept that data can be found and utilized is important knowledge that must be made aware of and added to the entire field.

In terms of acquisition of the data itself, the proposed and discussed methodologies can be used as a baseline. It is important to note that these methodologies will not work for every

infotainment system deployed in the public as too many factors come into play (vast variations of operating systems, hardware designs and specifications and software versions/builds). These extraction methodologies are documented and discussed to show that there are solutions and possibilities when tackling undocumented infotainment platforms. The general concept and theory can be applied to attempt to approach new systems and extracting information from them. Although some may require custom built solution (i.e. Berla iVe), it is not impossible to come up with one by approaching these systems from the ground up (for e.g. start by studying the underlying components of these systems to better understand them so you can apply a practical approach in acquiring data). Infotainment system, in general, are built like regular computer systems (just designed more in an embedded form) which means you could apply already known concepts to communicate with these systems. These methodologies demonstrate a general though process to undertake and case investigators could use this added knowledge to better handle these devices with limited documentation. This is also important for general awareness as it may direct users to better understand these platforms so potential data safekeeping measures can be taken (for e.g. disabling potential services, if capable, so that data could be less accessible externally).

Finally, an important final contribution for this work is validation. Validation of data is what one analyst would use to ensure data accuracy even if it varies across different/similar devices; it is very important to prove that discovered data indeed exists on the targeted device for proof of user activities regardless of how much data was collected from the extraction (quality versus quantity – if both can be achieved, even better). One can theorize about data being held and stored on infotainment systems (which this thesis also accomplishes) but to showcase that the data is there is of upmost importance as the data itself has global applications once parsed

and interpreted (not limited to law enforcement investigations). Access to these systems with appropriate tools and techniques is not easily attainable as well as it requires to dismantle the vehicle's interior and removing an entire system for its study (the general population owns vehicles to drive them and make use of their systems, not dismantle them). This research allowed for dedicated means of studying these systems and discussing the acquired results and proving they exist and are attainable. Variation is also important for the sake of data consistency or its comparison if it changes depending on the different infotainment systems. As new models are produced and deployed to the public, data set extractions could vary (for the better or worse) and it is important to make these observations so that data interpretations still hold relevance (for e.g. a new generation of an infotainment system is released and as a result, the acquisition methodology for its previous builds no longer works or only extracts a small subset of data). In this case, the data still needs to be checked and verified as it could be a question of the tool not parsing the information but still collecting it (data carving methodologies required but could potentially recover more data). Any slight alternation to the build of a computerized platform can affect a digital forensic process entirely and potentially break it so validation is an important foundation step for forensics as a whole, especially in newer digital forensic fields. Until standardization is implemented in infotainment system platforms (to a baseline degree in the least), there will be variance in the data that is extracted, especially across different infotainment platforms. In theory, the demonstrated acquisition methodologies, results and their interpretations validate the sought information as originally predicted (to various degrees depending on the specific infotainment system in our case).

The data interpretation, data acquisition process and overall theory can be viewed as a framework to follow when identifying these devices and attempting to extract and interpret the

data off of them. The overall theory of this research contributes to the body of knowledge of forensics from an educational/training aspect and forms a framework to apply when interacting with infotainment systems; these systems are built, at their basis, as general computer systems which helps determine potential approaches for acquiring and analyzing the stored data. This thesis also validates the sought data which is essential for proof-of-concepts. This further advances vehicular infotainment forensics as it demonstrates that the overall potential of digital forensics can benefit from the added methodologies and general thought process to use when interacting with new types of devices.

5.6 Final Thoughts

As a final note to this chapter, it is important to understand that many types of infotainment systems exist across the entire landscape of the automotive industry. Based off these stated observations, OEM and aftermarket system vary greatly in terms of amount of data acquired and methodologies for an acquisition of the data itself. This however can and most certainly will change as future trends in technology emerge and more efforts and functionalities are put into infotainment systems as a whole, especially with data security being an important trend in the past decade.

Although some extractions had limited data sets, all data extracted can potentially be evidence and this will always be useful to a forensic investigator, even to the slightest degree as it may help push a case in a new direction; this is simply the way of digital forensics as not every model and make of every platform is covered and supported by forensic tools due to the ever changing field of technology and the constant release of new devices, models and software revisions. Infotainment system manufacturers could also potentially implement ways of

obscuring user data on these systems through confidentiality/encryption methods and this would add obstacles to digital forensic analysts (these concepts are not new though and methodologies have been developed to circumvent them). Of course, this also depends on the hardware of the system and may limitations could arise. But of course this would add more development efforts and costs to them which could deter fully securing these widely deployed systems. Adding secure mechanisms is entirely up to the makers of the device and is something forensic analysts have dealt relatively well with considering the overall implications and added complications to data extractions and interpretations.

This correlates directly to the variance of the data sets extracted from all the different infotainment platforms used in this research as mentioned above. There may be discrepancies across this data due to the customized operating systems, hardware and software builds (just like mobile devices due to the massive amount of manufacturers and device models/builds). This is simply an element in digital forensics that has to be dealt with as there are many factors to consider when performing an extraction on a specific device, with a specific build using a specific forensic tool (all of these vary vastly by themselves). Data extractions can be difficult to manage and achieve due to all of these aforementioned complexities but it is a known factor within the field of digital forensics. This entire research has a goal of showcasing that valuable information can be extracted from infotainment platforms, may it be for law enforcement use or to raise awareness as a whole. This establishes a baseline for infotainment forensics and the usability of all recovered data artifacts. As more of these systems are integrated in the transportation system, the more information will be available. With future research, a more standardized methodology for acquiring and parsing infotainment system data can be developed

and widely deployed for positive outcomes in the world of digital forensics as more digital information will be available for analysis and interpretation.

Chapter VI – Conclusion

Computerized technological advancements have come a long way ever since the first inception of a computer. With more features and functionalities being developed daily in regards of facilitating end users' lives, it also permits people to engage in criminal activities with the help of these devices. Digital forensics itself is a brand new field compared to the traditional biological forensics field; technology is constantly developing and pushing boundaries which makes methodologies harder to develop, maintain and standardize. Digital forensic examiners must constantly stay on top of technology trends to ensure that all proper techniques and resources are exhausted when analyzing potential evidence. A community of these experts with constant research is the best way to maintain leveled playing-field when tasked with new challenges and technology.

Infotainment systems have impacted the transportation system due to the added features it brings to end users which include vehicle statistics, relaying information from mobile devices, playing multimedia content, navigating end users to destinations and so on. Regardless, the overall implications from this research shows that some infotainment systems can be used to reveal information about its end users and their activity on the system or the vehicle itself. This is very beneficial to law enforcement agencies and respective investigators as any information pulled from these platforms can either be evidence or help corroborate other pieces of evidence; vehicles in nature are very personal to their users therefore it would only helpful to investigators to analyze their systems. They are even more relevant if the vehicle is an accessory to a crime itself, not to mention that end users can connect mobile devices (including computers) if Bluetooth functionalities are enabled. It is important to note that this information could also be accessed by any other third party that may have access to the vehicle so caution should be

exercised by end users, especially when it comes to willingly connecting other devices to infotainment platforms as more information would be circulated. These show great potential for forensic means as a lot of information is potentially circulated to these systems as vehicles are highly involved as criminal accessories and mostly everyone owns a mobile device compatible with them. The information found on them, regardless if system, user or application data, shows to be of great relevance as it can help identify end users that interacted with the vehicles in question. Such information should be viewed as invaluable.

Due to the nature of the digital forensics field, challenges were expected along the way, especially considering the variation among all platforms, including the different vehicle manufacturers and different vehicle models and builds. The infotainment systems were constricted to different software, hardware and builds, which makes acquisition of images a challenge itself; infotainment system are similar to mobile devices and their multitude of tools required to complete forensic acquisitions, as well as their nature since they are also considered mobile devices. OEMs showed the greatest challenge as the acquisition process required a custom third party hardware and software solution (Berla iVe) to just acquire the data, and iVe only works for very specific makes and models of vehicles. Interpreting the data (file system and metadata in the least) is easier as a lot of forensic tools can parse the acquired data structures due to the standardized file system/operating system they use but it is no guarantee as some of these software revisions are modified by the manufacturer and are not recognizable (which can also complicate the acquisition process). The major lack of standardization across OEMs renders the acquisition process to complex means without a proprietary solution; more standardized methodologies among OEMs and aftermarket systems need to be developed to ensure a sound forensic method of acquisition not to mention built-in-tool support for forensic tools for parsing

the data. This does not mean it is impossible to accomplish an acquisition in a forensically sound matter but it currently requires extra resources and time which is sometimes not of the essence when it comes to legal investigations and court proceedings. Aftermarket infotainment systems seem to be the more accessible platform compared to OEMs as they seem to use operating systems that are documented (for e.g. Android/Linux-based and Windows-based) to some extent (less customized then OEMs). Although the pulled data sets seem to be more limited, there is many vendors and builds available to the consumer which means some of these platforms will show variation when it comes to what data is accessible. There also were instances where parsing the storage blocks would results in "reading errors" and our forensic tool (Autopsy) would not be able to parse the content of the extractions. Alas, variation in results from device extractions and its parsing of data is nothing new in the field of forensics due to the varying nature of technology itself. This demonstrates the importance of standardization across the industry when it comes to interoperability of different platforms working in conjunction.

The work that was demonstrated in this thesis paves the way for forensic examiners in what types of information to expect when analyzing such systems. It is clear that more streamlined and efficient methodologies must be developed to ensure that these systems are not left unchecked as the potential for identifiable information has clearly been demonstrated. In terms of future work, further research can me be made in the interactions of the CAN and MOST buses and if infotainment system data can be accessed and downloaded though the CAN; it would be interesting to find out if an acquisition method could be developed by using the CAN bus as the connecting medium. This would give a standardized approach for acquiring data since CAN buses are universal in modern vehicles. It would also be important to research this as it could determine whether exploiting the CAN bus or other internal bus components could lead to

the download of stored information using the MOST bus (for e.g. potential for VANET vulnerabilities being exploited and leveraged against the infotainment system?). An open source methodology could also be looked into in terms of acquiring data from infotainment systems as a whole. Although not impossible, this is probably a difficult task for to accomplish for OEM-based devices, but aftermarket systems have shown to be more accessible. Finally, research into the privacy implications of the data stored in infotainment systems can be researched. To what extent does these systems need personal information to operate? Is it necessary to keep all this data? Should there be an option to wipe these devices from all data (not just user profiles) and have encryption as an option? A question of privacy versus usability and practicability in this case; to what extent can law enforcement use this information and should there be limits? Regardless, the future of vehicular infotainment forensic is bright as much information is available to forensic examiners/law enforcement agencies. This data could very well be used to identify end users when needed, depending on the given circumstances, which can help shine a new light on investigations, stop criminal activities and their culprits and even save lives.

Appendix

Various Audi/Volkswagen Manual Acquisition Setup

2014 Volkswagen Touareg

Export destination options

Lists of previously/current connected Bluetooth devices

Contacts can also be exported to SIM card

Number of items in memory per connected devices (current and prior)

Examples of content that can be exported

2012 Audi Q5

Export destination options

Lists of previously/current connected Bluetooth devices

GPS coordinates found on system

Number of items in memory (current and prior devices)

Export specifications

2014 Audi Q7

It is important to note that this vehicle was not previously owned; device functionalities and their verification were checked and compared to other Audi and Volkswagen vehicles if they would be similar and if data could potentially be acquired through manual acquisition.

Lists of previously/current connected Bluetooth devices

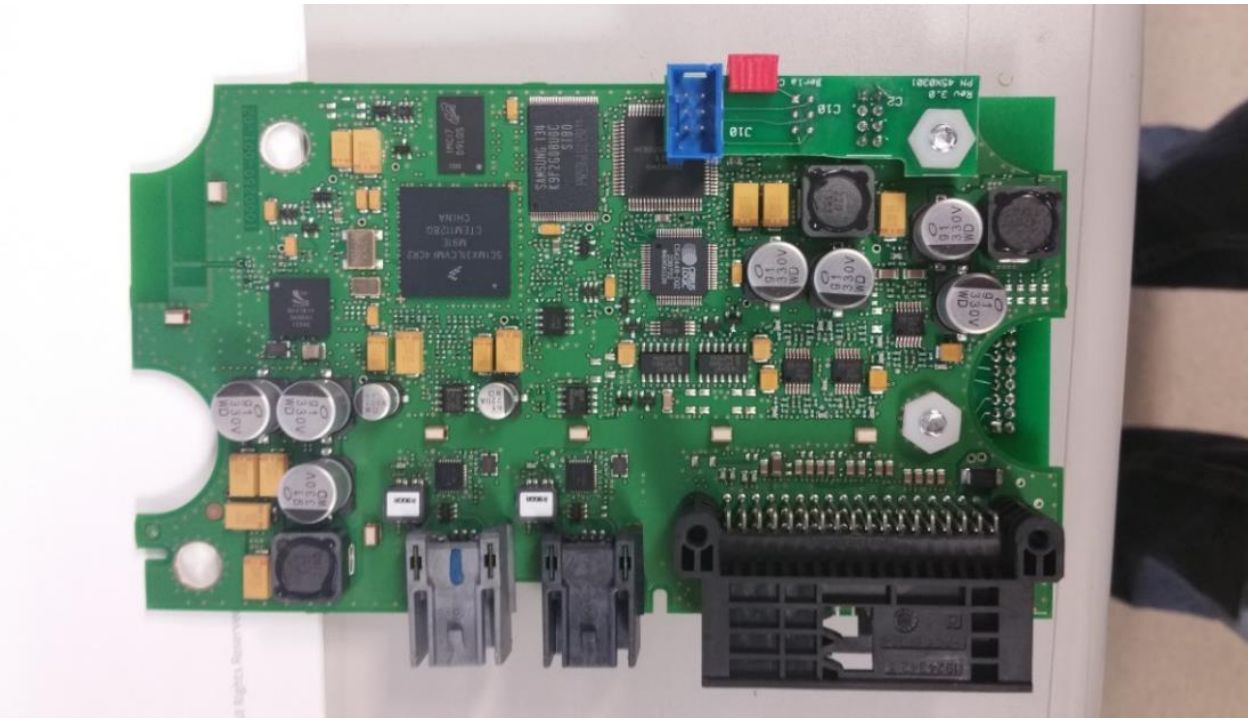
Number of items in memory per mobile device (current and prior devices)

Export capability is enable and functional

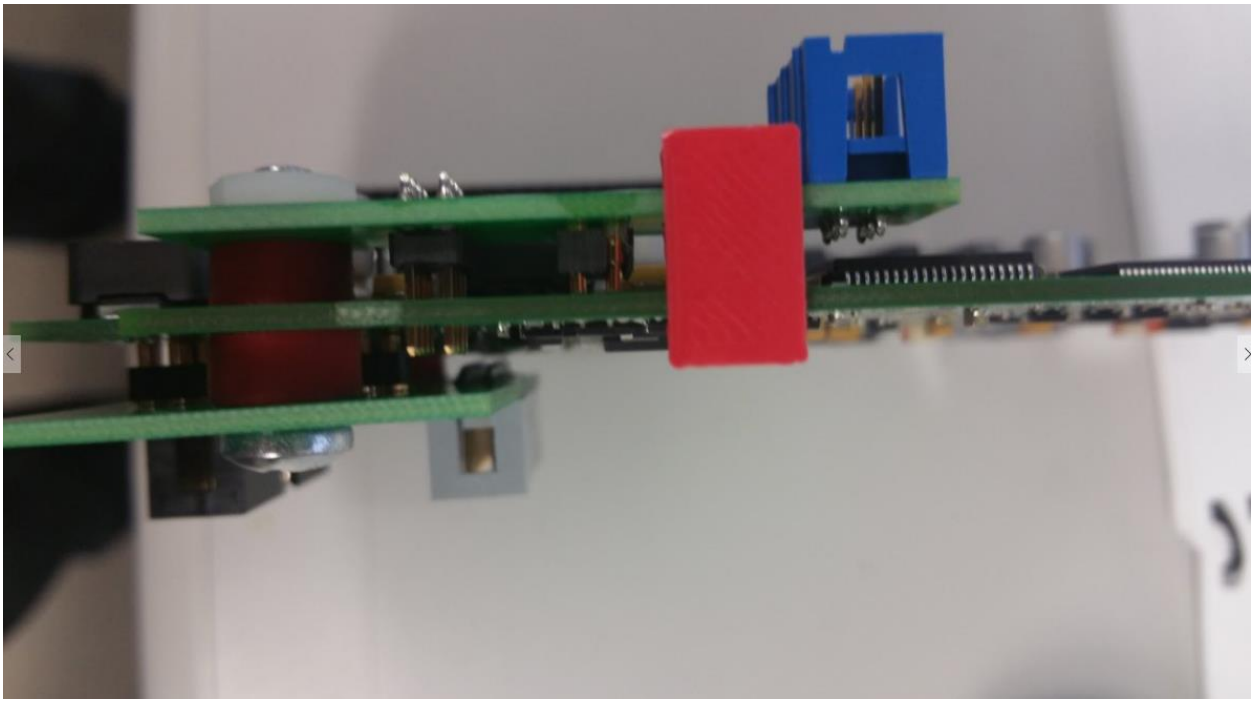
OEM Infotainment System

It is important to note that the process depicted below is the same for SYNC Gen I and II.

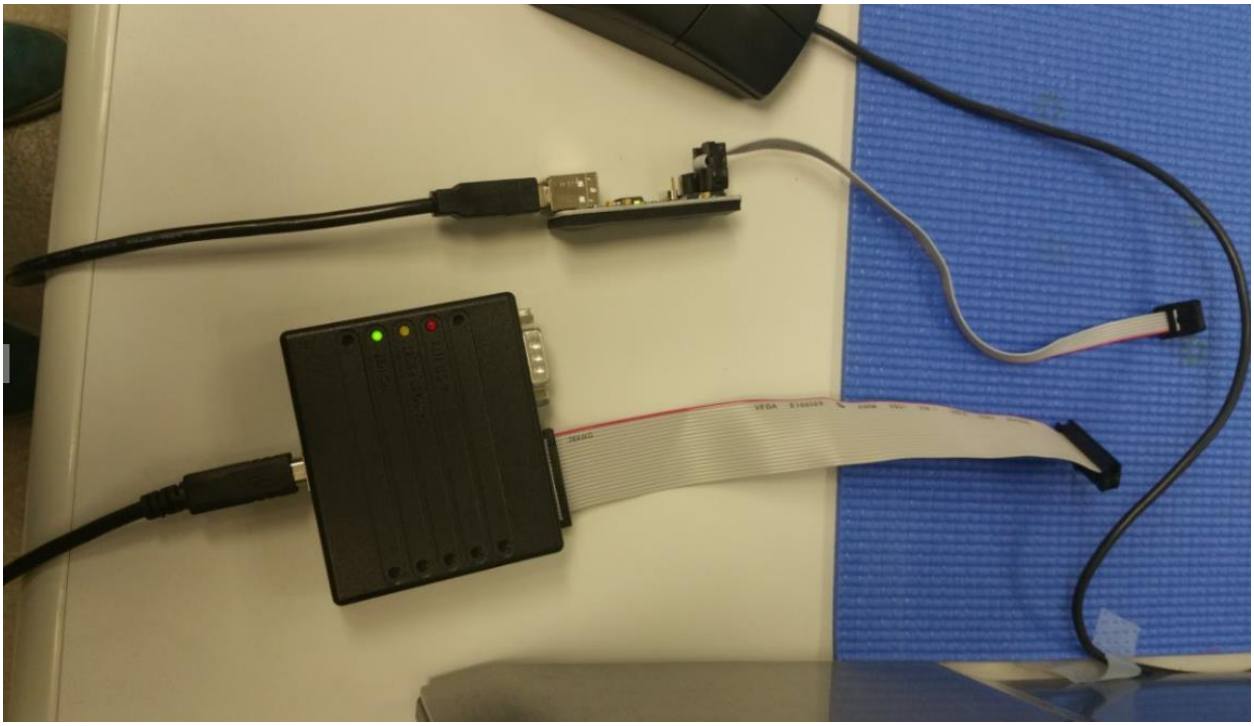
Acquisition Setup Process



Ford SYNC storage module

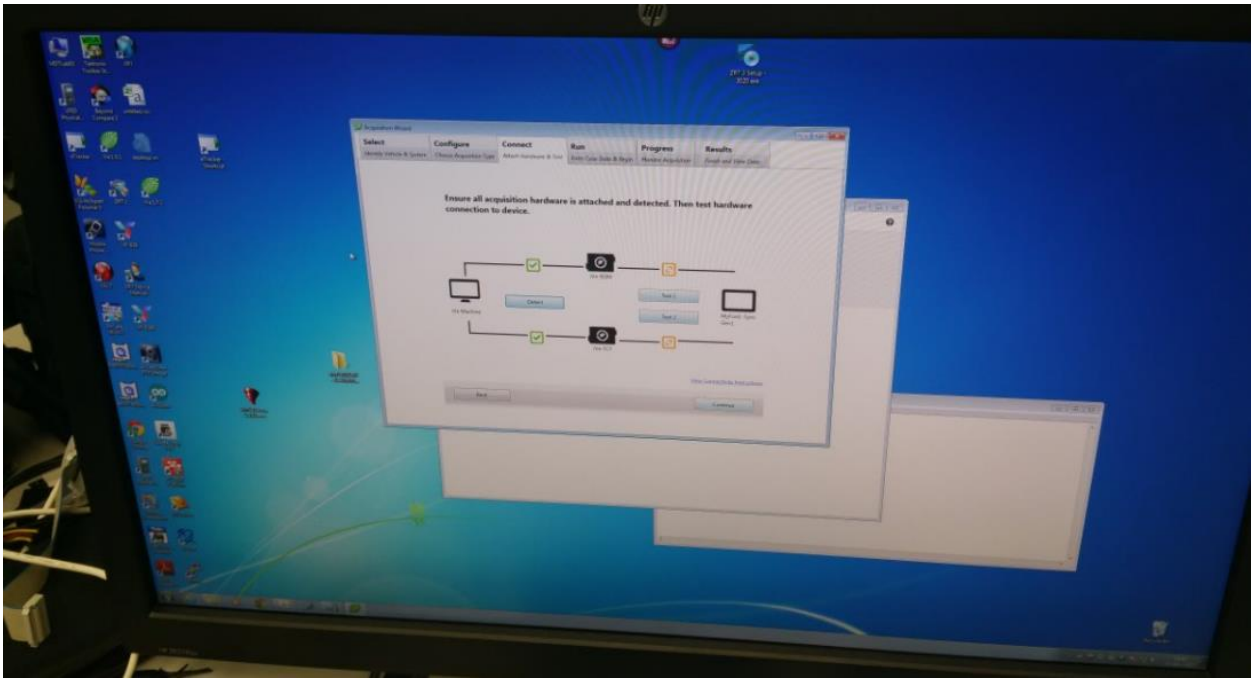


JTAG components attached to Ford SYNC module storage board



Berla iVe JTAG connectors

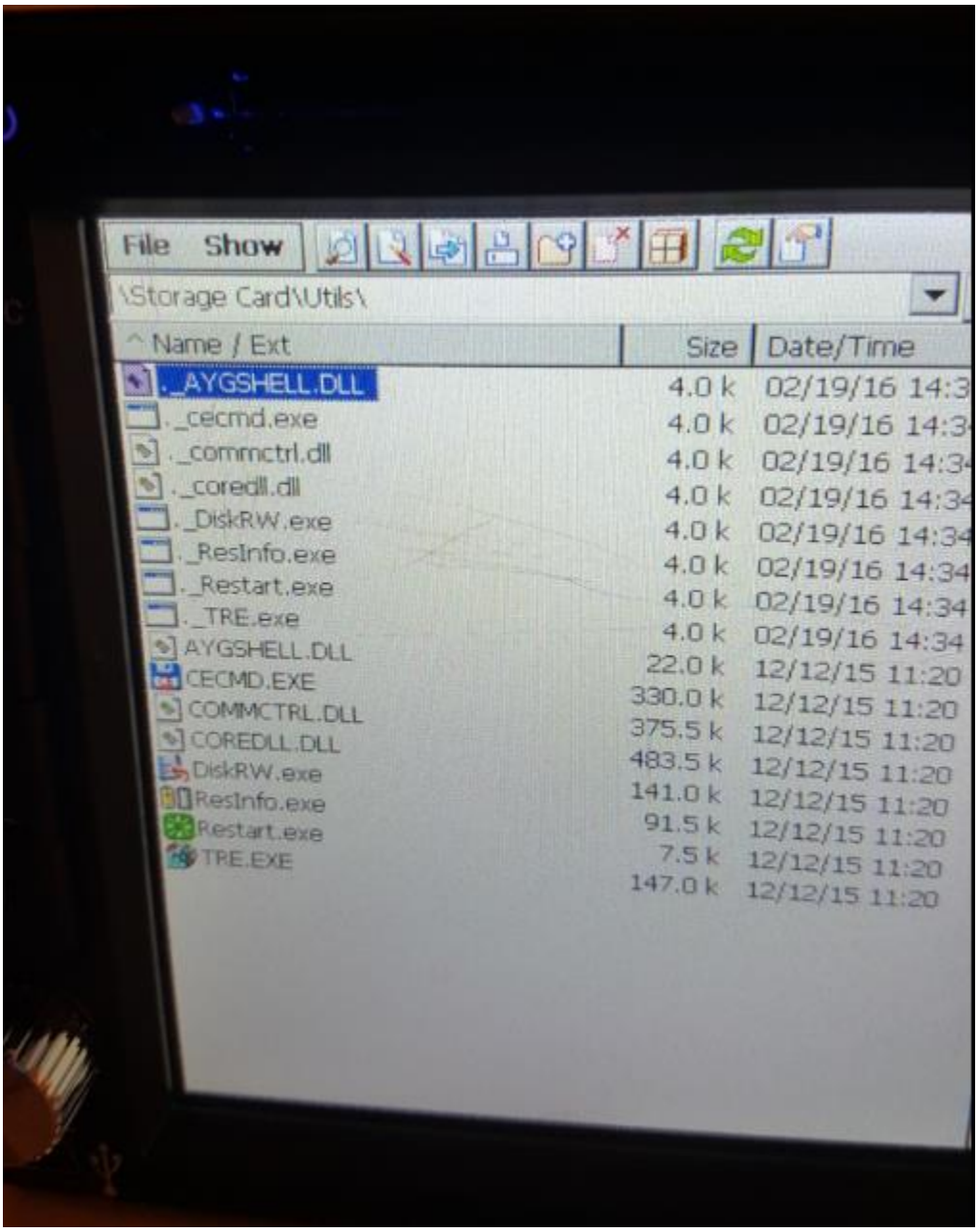
Berla iVe connectors attached to JTAG components connected to Ford SYNC module



Berla iVe software in progress of detecting Ford SYNC module

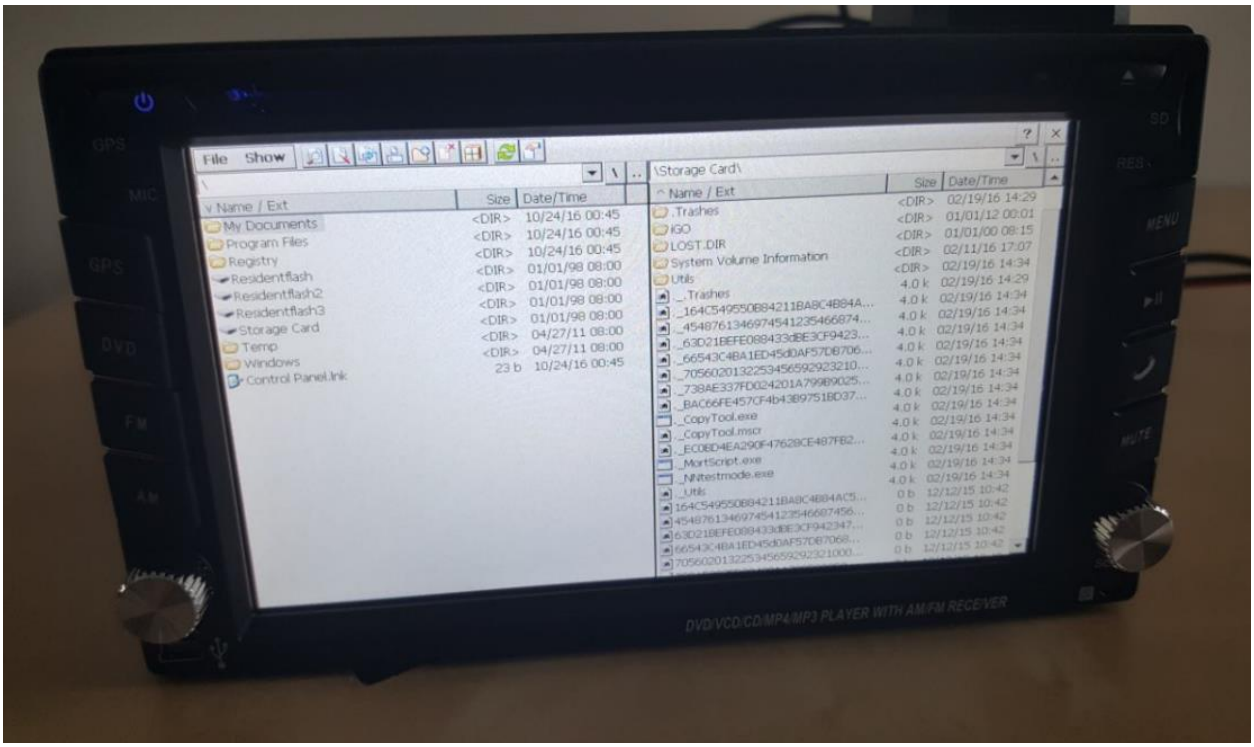
Ouku Windows CE 6 Infotainment System

Acquisition Setup Process

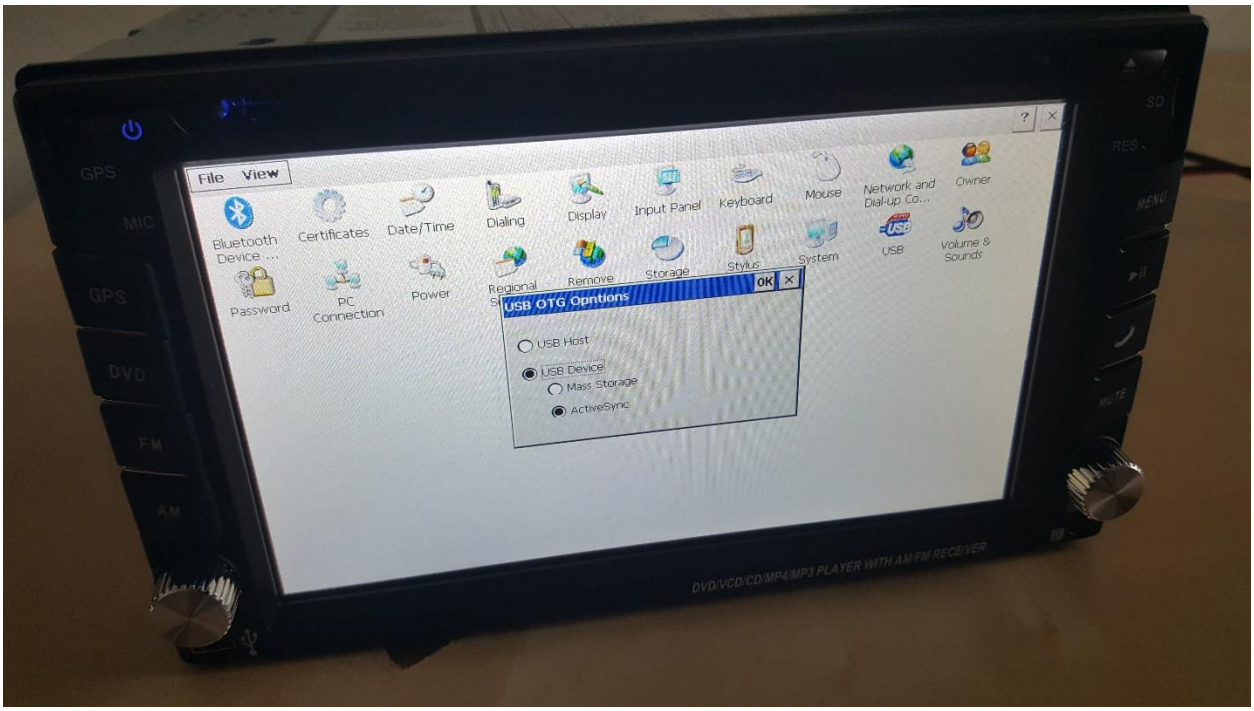


Utilities loaded in micro-SD card that will be inserted in GPS micro-SD slot

GPS button path now points to new executable file



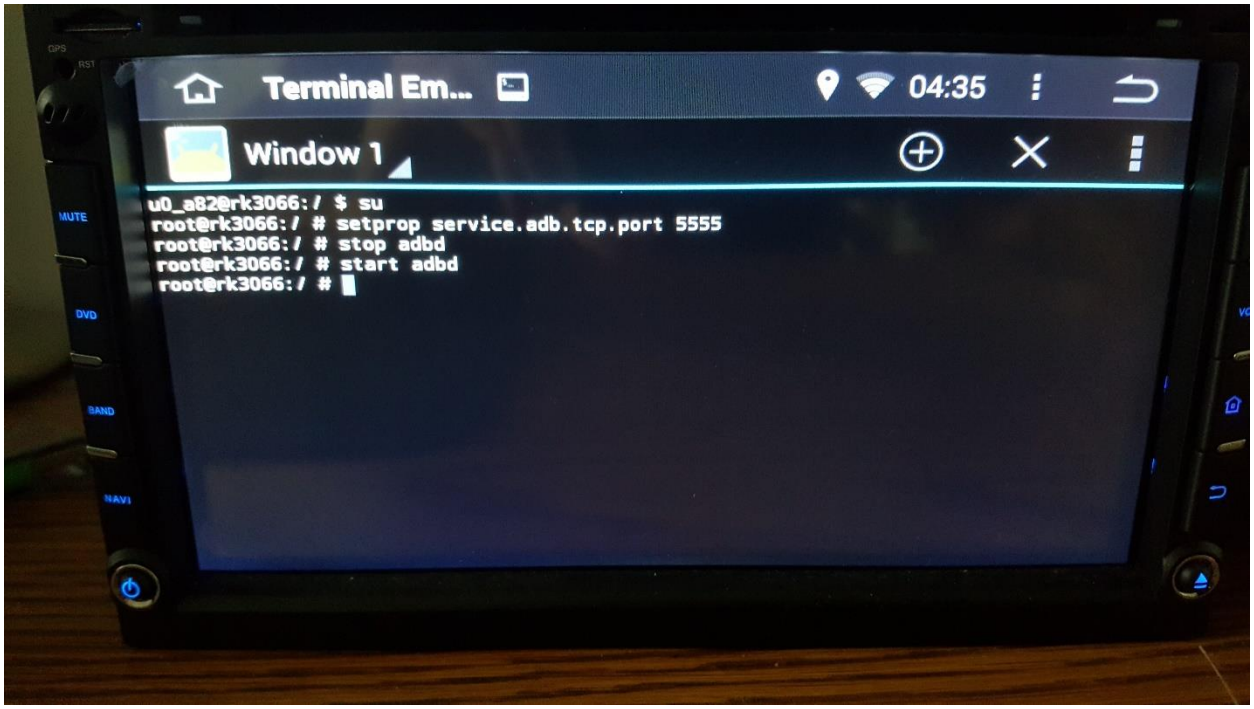
Result of executing CECMD.exe and file system view (here you can copy files to /Storage Card)



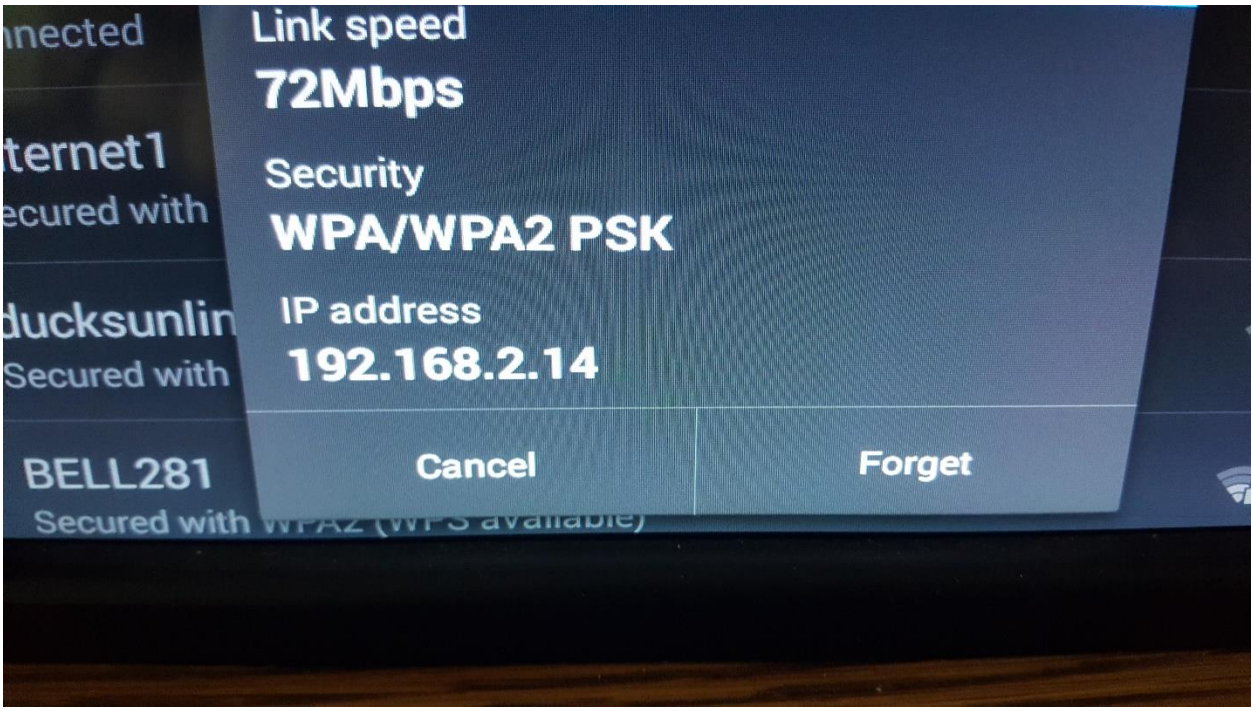
Alternative way of accessing files through Windows Mobile Device Manager

Pumpkin Android Kit-Kat 4.4.4 Infotainment System

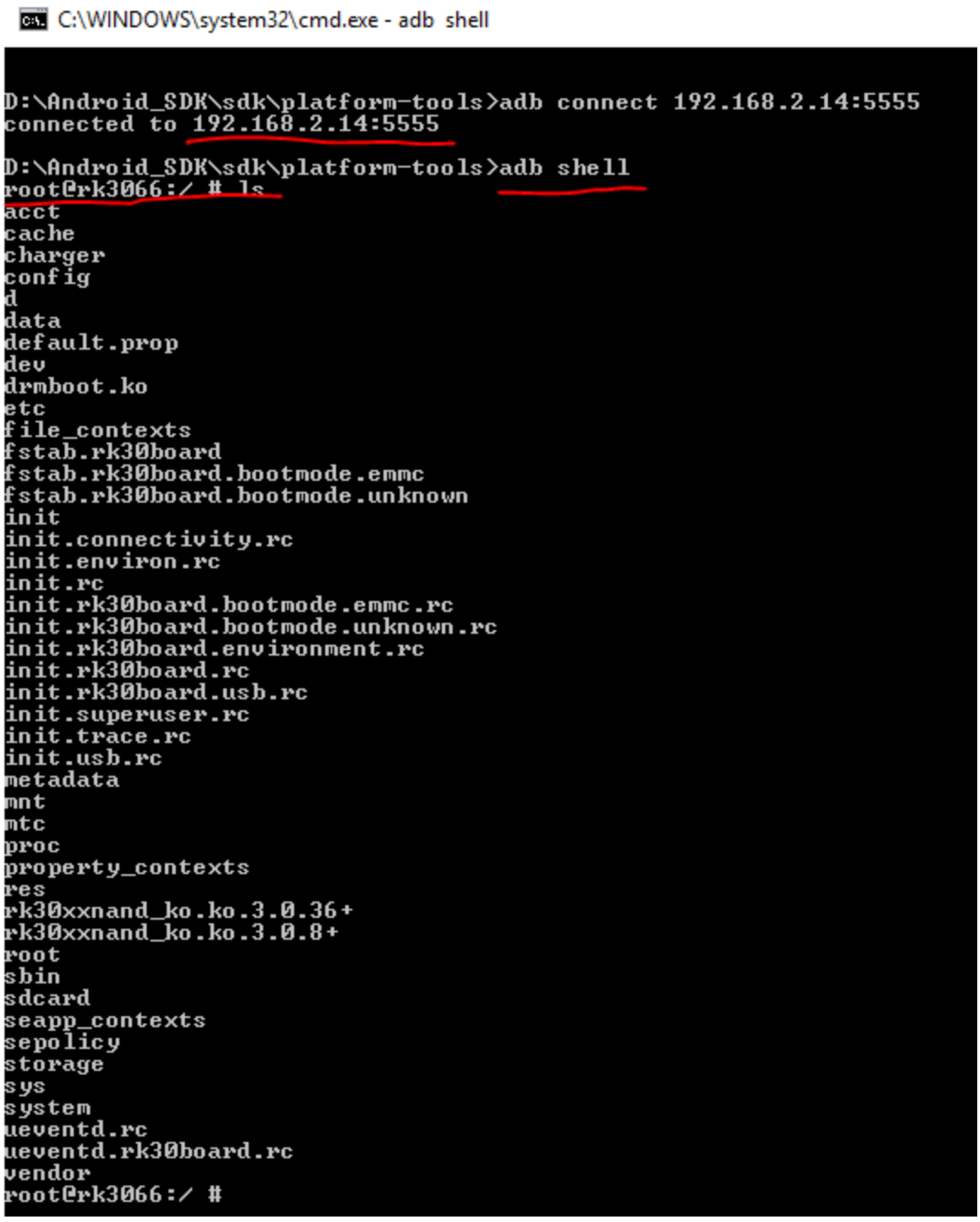
Acquisition Setup Process



Commands inputted on Pumpkin platform for enabling ADB-over-WiFi



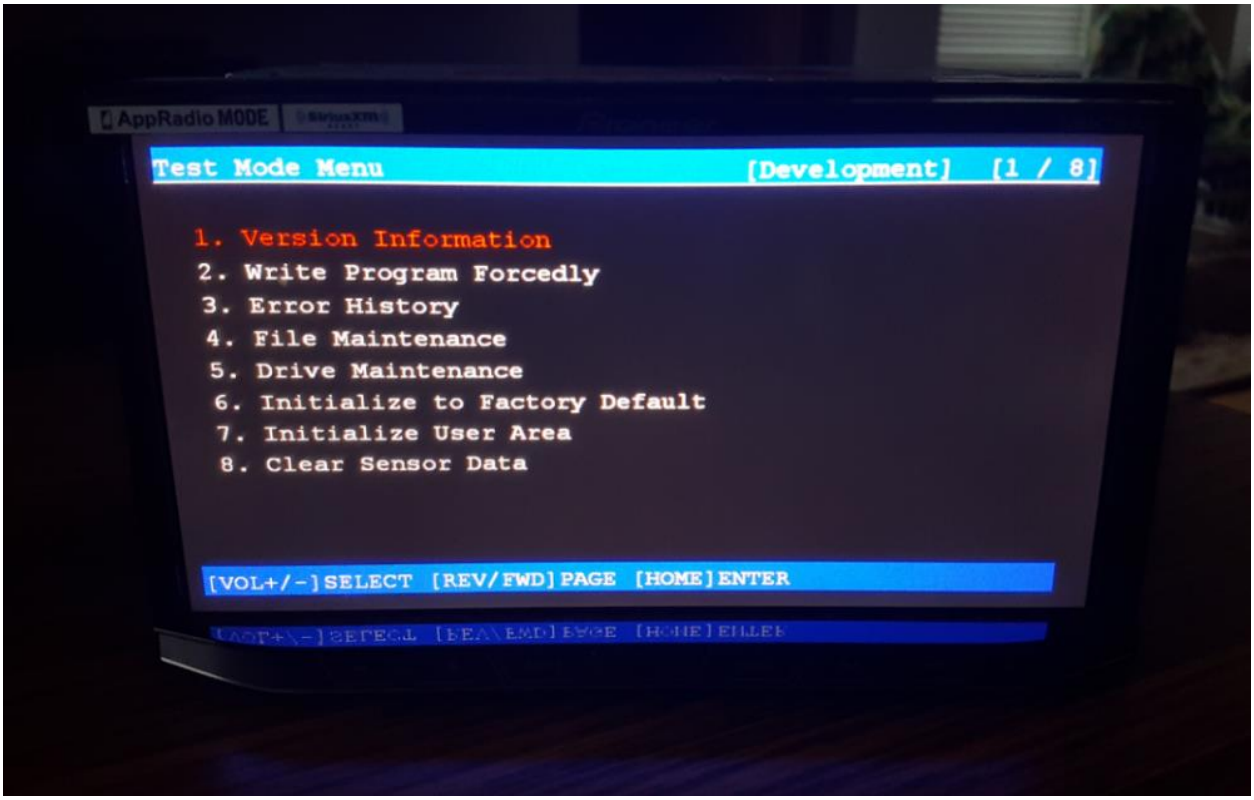
IP address of infotainment system



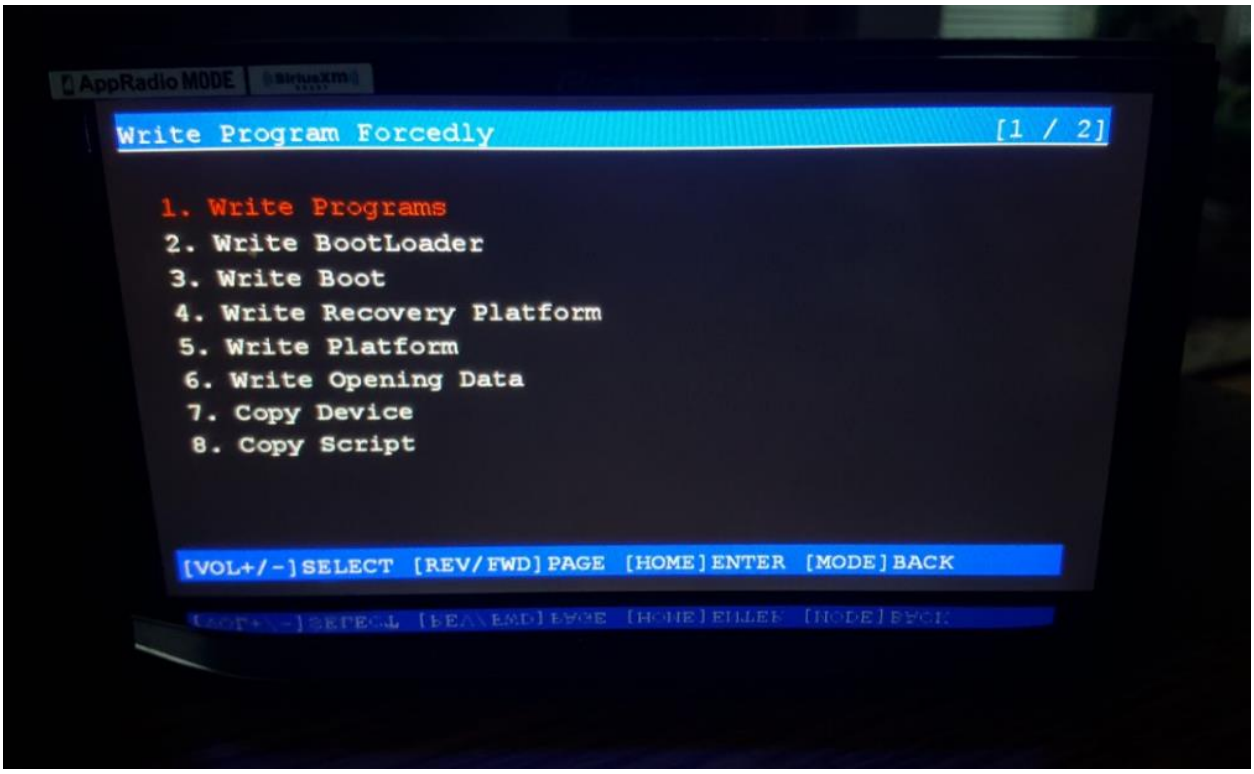
Connection to Pumpkin platform through WiFi and input for shell access

Pioneer Android-Variant Infotainment System

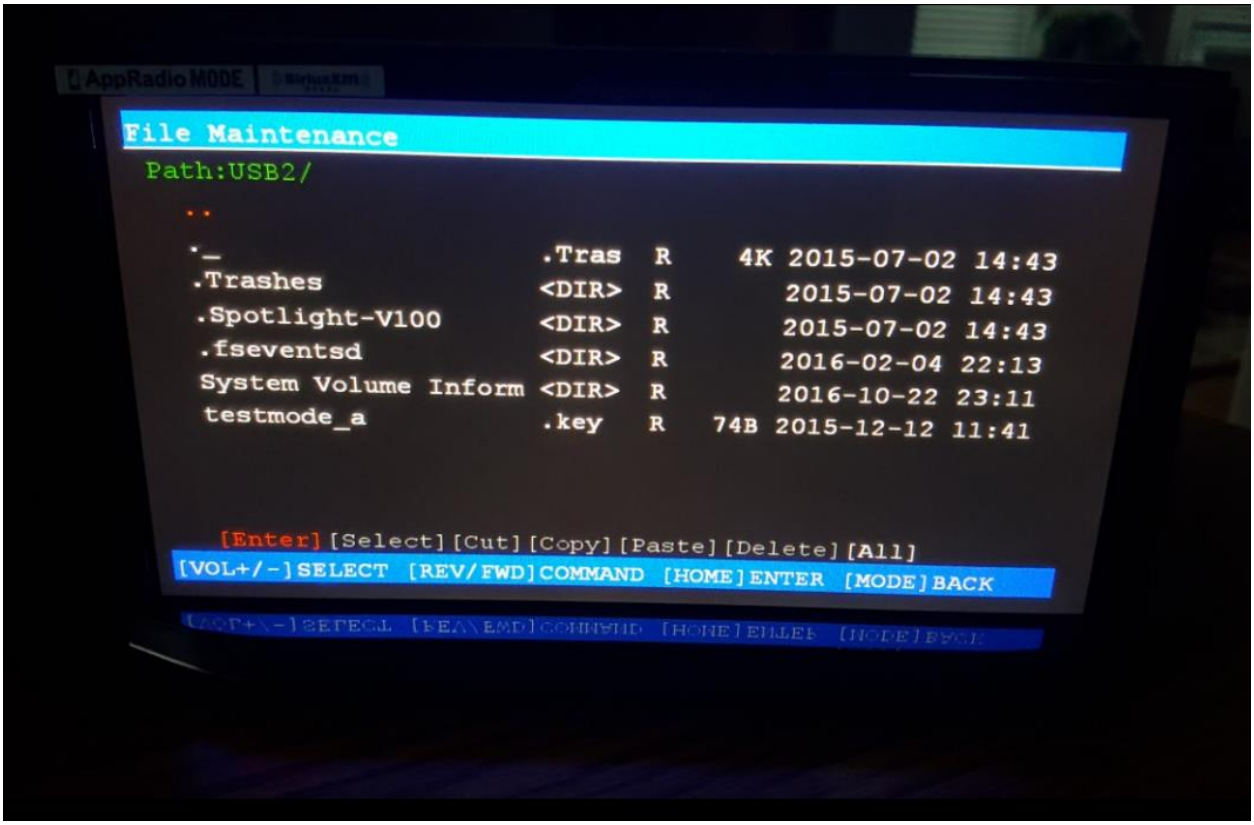
Acquisition Setup Process



Access to Test Mode successful



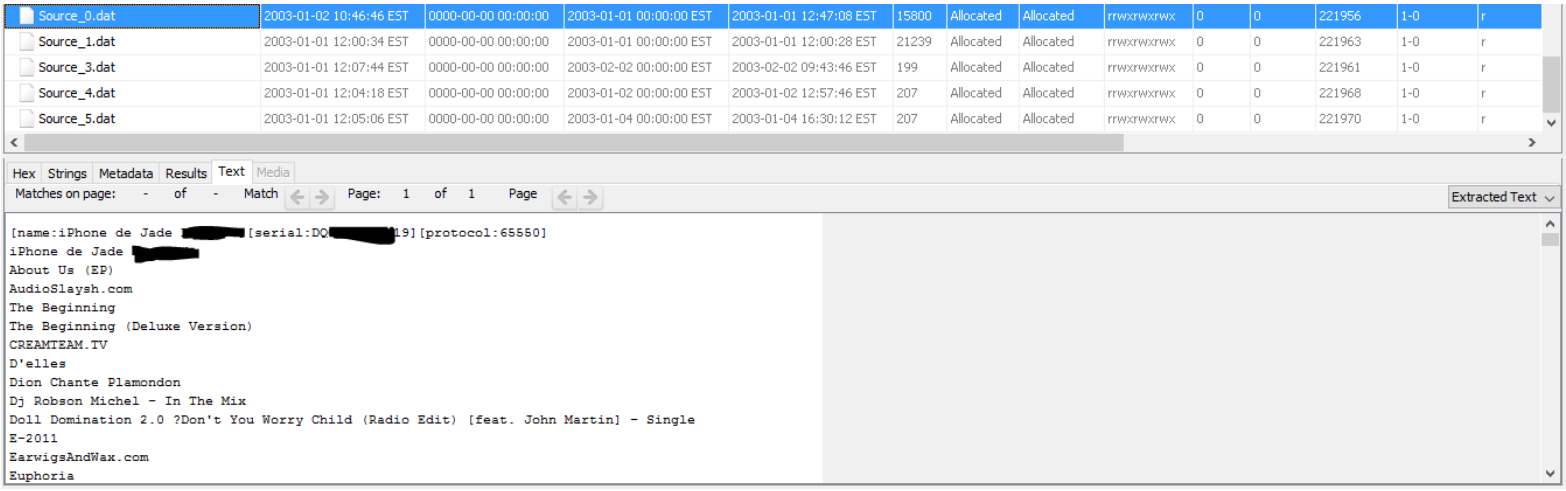
Access to force write options on system



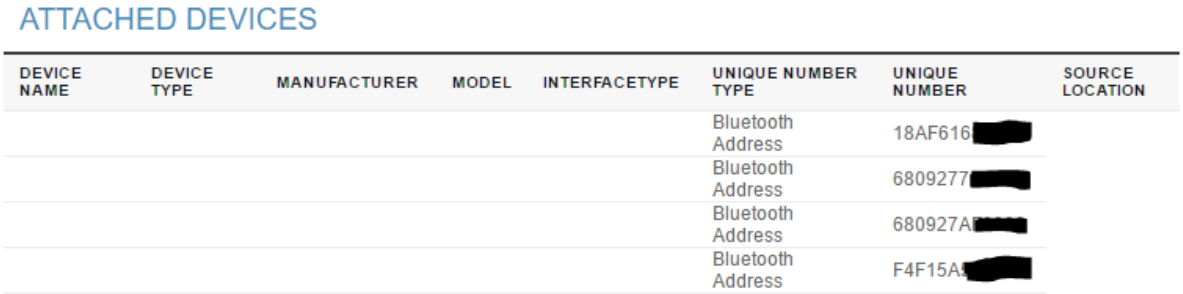
Location to run scripts and of testmode_.key file (script was not on USB at time of picture)

Observed Data Examples

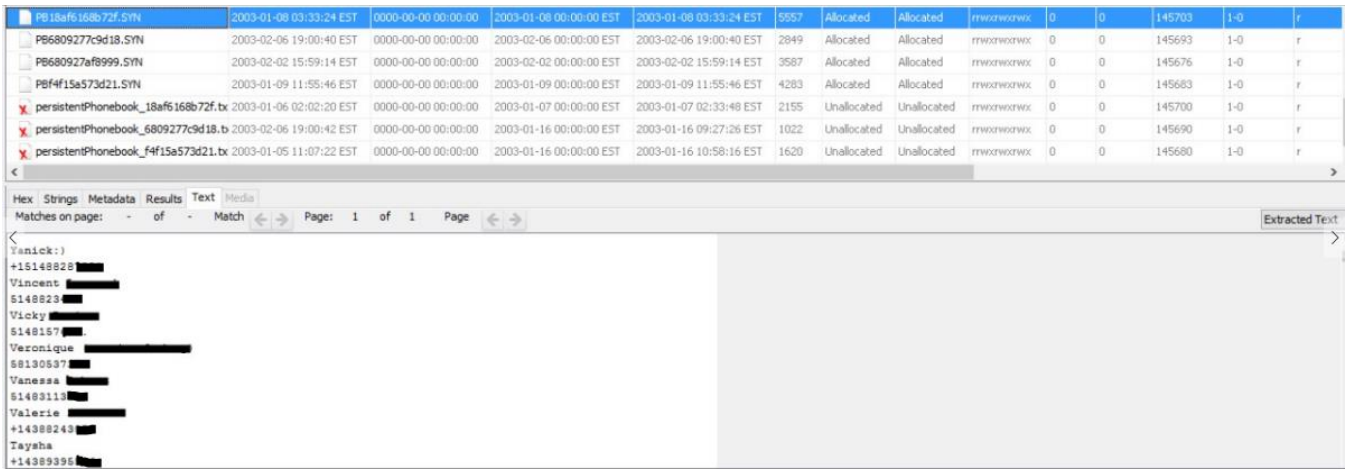
2012 Ford Fiesta SYNC Generation I – Physical Acquisition



Device name, serial and multimedia information



iVe report showing Bluetooth MAC addresses



Contact names and phone numbers

ENTEREDVIN	3FADP4EJXCM183940
VEHICLEYEAR	2012
VEHICLEMANUFACTURER	Ford
VEHICLEMODEL	Fiesta
VEHICLETRIMLEVEL	SE
VEHICLEECU	Sync Gen1

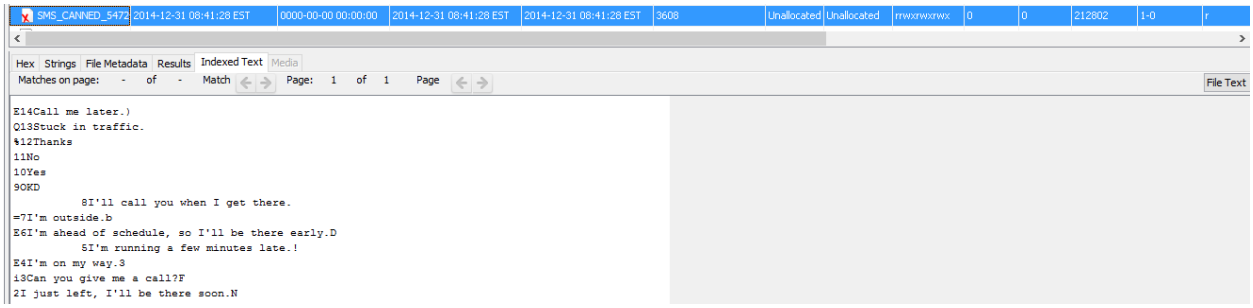
iVe report of system information

CONTACTS

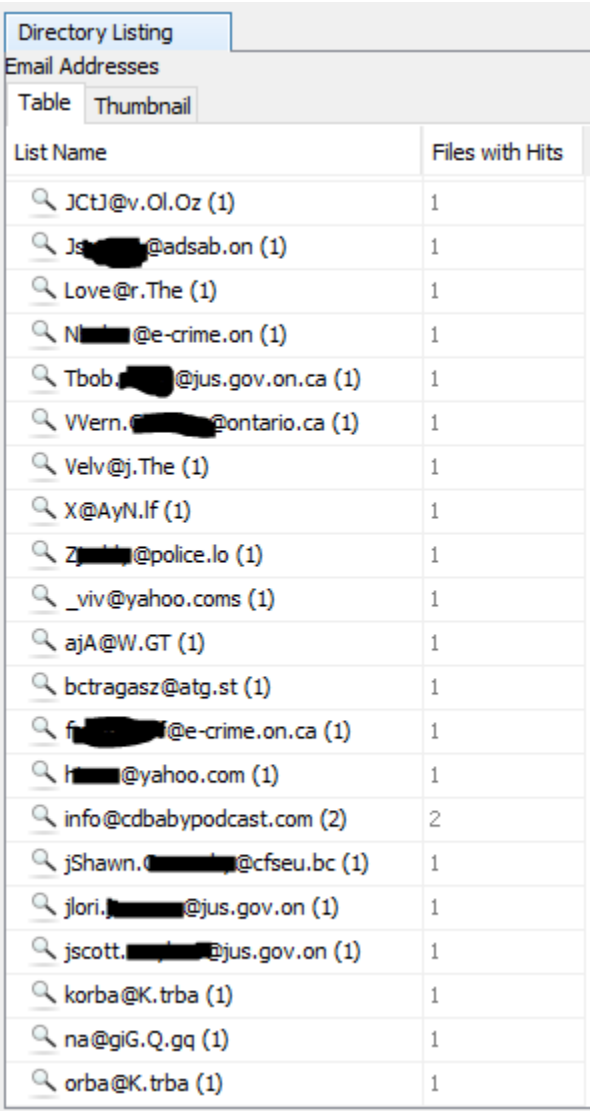
PHONE NUMBER	WORK NUMBER	HOME NUMBER	MOBILE NUMBER	FIRST NAME	LAST NAME	COMPANY	EMAIL	DEVICEIDENTIFIER
+15148828[redacted]					Yanick:)			18AF6168[redacted]
5148823[redacted]				Vincent	[redacted]			18AF6168[redacted]
5148157[redacted]				Vicky	[redacted]			18AF6168[redacted]
5813053[redacted]				Veronique (cousine	[redacted]			18AF6168[redacted]
5148311[redacted]				Vanessa	[redacted]			18AF6168[redacted]
+14388243[redacted]				Valerie	[redacted]			18AF6168[redacted]
+14389395[redacted]					Taysha			18AF6168[redacted]
5142228[redacted]				Taxi	[redacted]			18AF6168[redacted]
5146561[redacted]				Tattoo	[redacted]			18AF6168[redacted]
4389311[redacted]				Tanya	[redacted]			18AF6168[redacted]
5148891[redacted]				Steve	[redacted]			18AF6168[redacted]

iVe report of contacts associated to a specific mobile device

2013 Ford Focus SYNC Generation II – Physical Acquisition



Canned SMS data found in extraction (potential for user generated one)



Some emails that were extracted

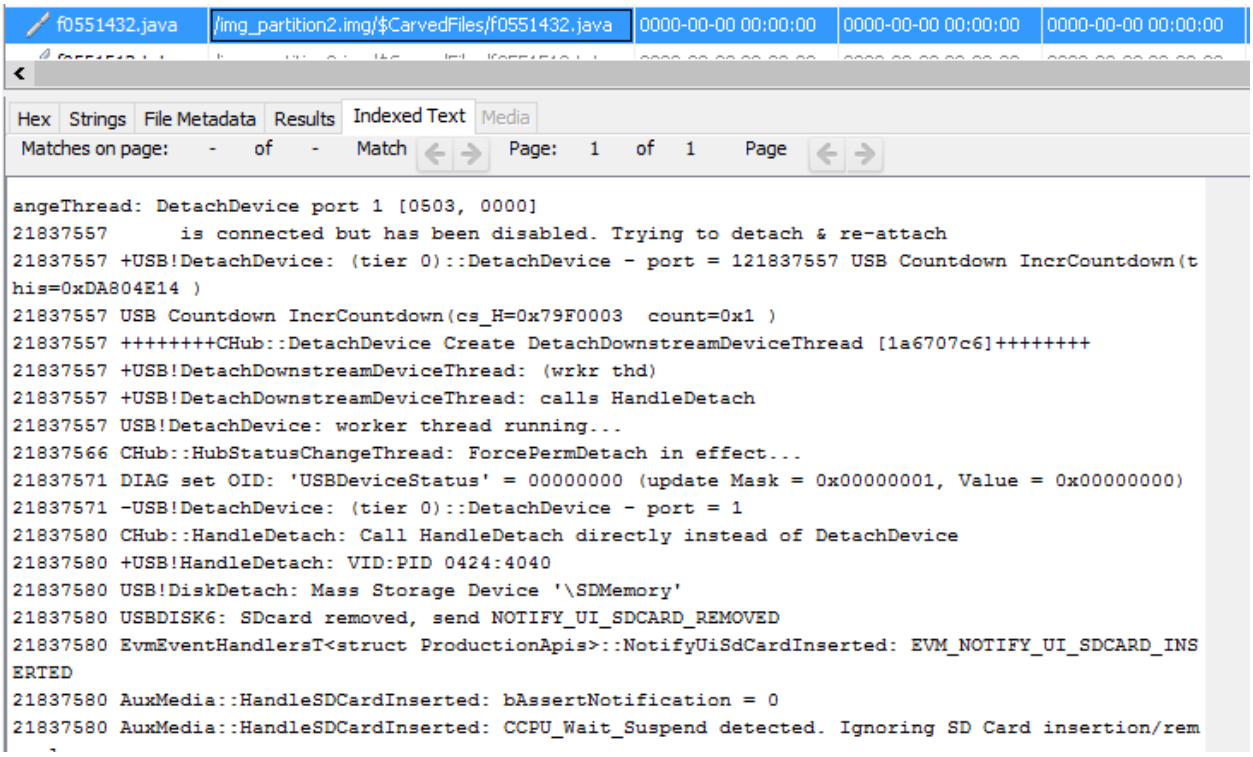
ENTEREDVIN	1FADP3F21DL356099
VEHICLEYEAR	2013
VEHICLEMANUFACTURER	Ford
VEHICLEMODEL	Focus
VEHICLETRIMLEVEL	SE
VEHICLEECU	Sync Gen2
ACQUISITION SUMMARY	

Back to Top

ATTACHED DEVICES

DEVICE NAME	DEVICE TYPE	MANUFACTURER	MODEL	INTERFACETYPE	UNIQUE NUMBER TYPE	UNIQUE NUMBER	SOURCE LOCATION
Kenny	Phone-5				Serial Number	C39H8UM[redacted]	
Jeremy iPhone	Phone-3				Bluetooth Address	00004F8F[redacted]	
					Bluetooth Address	54724F8F[redacted]	
					Bluetooth Address	54724F8F[redacted]	
					Bluetooth Address	54724F8F[redacted]	
Kenny					Serial Number	C39H8UM[redacted]	

iVe report of system information and connected devices



System events showing USB device being detached

CONTACTS

PHONE NUMBER	WORK NUMBER	HOME NUMBER	MOBILE NUMBER	FIRST NAME	LAST NAME	COMPANY	EMAIL	DEVICEIDENTIFIER
		7056849[redacted]			[redacted] self Storage			54724F8FD[redacted]
		+17053263[redacted]	7053212[redacted]	Agnes	[redacted]			54724F8FD[redacted]
	7056895[redacted]			Alan	[redacted]			54724F8F[redacted]
	1800306136339[redacted]		3474978[redacted]	Alex	[redacted]			54724F8F[redacted]
	7055647[redacted]	7055232[redacted]		Alexander	[redacted]			54724F8F[redacted]
				Andrea	[redacted]			54724F8F[redacted]
		4169017[redacted]		Andrea	[redacted]			54724F8F[redacted]

iVe report of all contact information and associated device

ID	DATE / TIME	LATITUDE	LONGITUDE	DISTANCE	BEARING
TRACK: RECOVERED0001					
1	1/2/2013 3:32:53 AM	42.33016	-83.14341		
2	1/2/2013 3:32:54 AM	42.33016	-83.14341		0°
3	1/2/2013 3:32:57 AM	42.33016	-83.14341		0°
4	1/2/2013 3:32:58 AM	42.33016	-83.14341		0°
5	1/2/2013 3:32:59 AM	42.33016	-83.14341		0°
6	1/2/2013 3:33:00 AM	42.33016	-83.14341		0°
7	1/2/2013 3:33:01 AM	42.33016	-83.14341		0°
8	1/2/2013 3:33:02 AM	42.33016	-83.14341		0°
9	1/2/2013 3:33:04 AM	42.33014	-83.14342	1.84 m	193°
10	1/2/2013 3:33:05 AM	42.33012	-83.14342	0.43 m	270°
11	1/2/2013 3:33:06 AM	42.33012	-83.14344	3.58 m	180°
12	1/2/2013 3:33:07 AM	42.3301	-83.14344	0.43 m	270°
13	1/2/2013 3:33:08 AM	42.3301	-83.14345	1.79 m	180°
14	1/2/2013 3:33:09 AM	42.33009	-83.14347	3.59 m	183°
15	1/2/2013 3:33:10 AM	42.33009	-83.14348	1.79 m	180°
16	1/2/2013 3:33:11 AM	42.33009	-83.14348		0°
17	1/2/2013 3:33:12 AM	42.33008	-83.1435	3.59 m	183°

iVe report of GPS coordinates/breadcrumbs on infotainment system

Door	Passenger door was opened at 2013-01-16 02:25:05	opened	1/16/2013 2:25:05 AM	42.35349	-83.04628
Door	Passenger door was opened at 2013-01-15 02:16:05	opened	1/15/2013 2:16:05 AM	42.50874	-82.92712
Door	Driver door was opened at 2013-01-15 02:16:08	opened	1/15/2013 2:16:08 AM	42.50874	-82.92714
Door	Passenger door was closed at 2013-01-15 02:16:25	closed	1/15/2013 2:16:25 AM	42.50874	-82.92714
Door	Passenger door was opened at 2013-01-15 02:16:33	opened	1/15/2013 2:16:33 AM	42.50874	-82.92714
Door	Driver door was closed at 2013-01-15 02:16:19	closed	1/15/2013 2:16:19 AM	42.50874	-82.92714

Back to Top

REBOOT EVENTS

EVENT TYPE	IDENTIFIER	ACTION	DATE TIME	LATITUDE	LONGITUDE	ALTITUDE
Reboot	Reboot Power Removed at 2013-01-14 19:15:55	Power Removed	1/14/2013 7:15:55 PM	44.58332	-79.43129	
Reboot	Reboot Power Removed at 2013-01-05 12:08:12	Power Removed	1/5/2013 12:08:12 PM	42.36334	-83.02525	
Reboot	Reboot Power Removed at 2013-01-18 05:25:54	Power Removed	1/18/2013 5:25:54 AM	44.58297	-79.43027	
Reboot	Reboot Power Removed at 2014-12-30 13:07:07	Power Removed	12/30/2014 1:07:07 PM	44.58251	-79.43099	
Reboot	Reboot Power Removed at 2013-01-04 20:45:43	Power Removed	1/4/2013 8:45:43 PM	42.34233	-83.07096	

Back to Top

USB EVENTS

EVENT TYPE	IDENTIFIER	ACTION	DATE TIME	LATITUDE	LONGITUDE	ALTITUDE
USB	USB Device Attached : Vendor:1060, ProductId:16448, Release:-1 at 2013-01-15 01:59:08	Device Attached	1/15/2013 1:59:08 AM	42.35351	-83.04632	
USB	USB Device Attached : Vendor:1060, ProductId:16448, Release:-1 at 2013-01-14 22:47:10	Device Attached	1/14/2013 10:47:10 PM	44.58251	-79.43099	
USB	USB Device Attached : Vendor:1060, ProductId:16448, Release:-1 at 2014-12-30 13:07:31	Device Attached	12/30/2014 1:07:31 PM	44.58251	-79.43099	
USB	USB Device Attached : Vendor:1060, ProductId:16448, Release:-1 at 2013-01-14 19:33:08	Device Attached	1/14/2013 7:33:08 PM	42.33061	-83.1431	
USB	USB Device Attached : Vendor:1060, ProductId:16448, Release:-1 at 2013-01-04 20:46:11	Device Attached	1/4/2013 8:46:11 PM	42.34233	-83.07096	

iVe report of various user interactions with vehicle and infotainment system

Phone	Phone disconnected at 2013-01-14 19:33:38	disconnected	1/14/2013 7:33:38 PM	42.33061	-83.1431
Phone	Phone disconnected at 2013-01-02 03:32:46	disconnected	1/2/2013 3:32:46 AM	42.33016	-83.14341
Phone	Phone disconnected at 2013-01-16 02:24:09	disconnected	1/16/2013 2:24:09 AM	42.35349	-83.04628
Phone	Phone disconnected at 2013-01-15 02:15:45	disconnected	1/15/2013 2:15:45 AM	42.50874	-82.92712

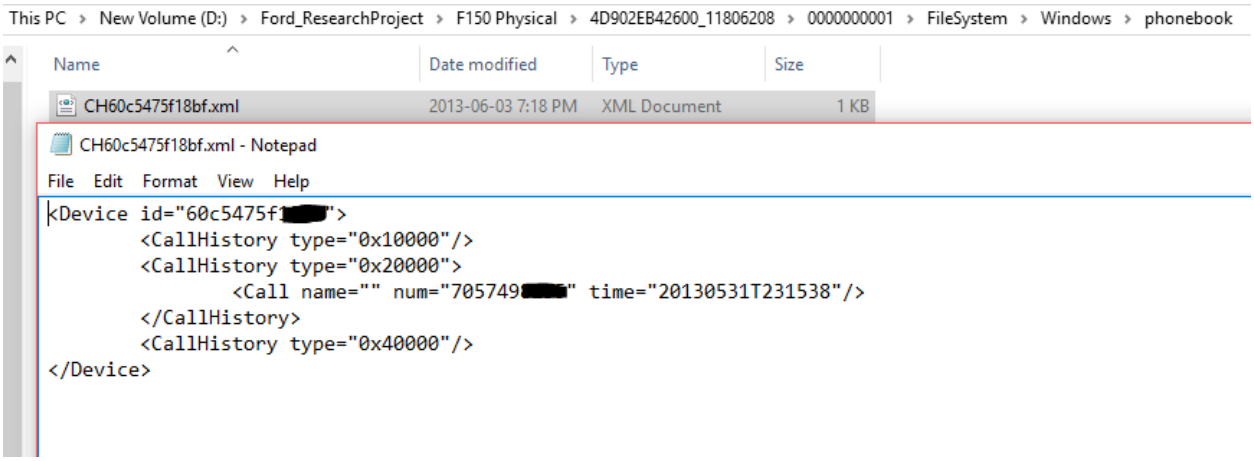
Back to Top

GEARSHIFT EVENTS

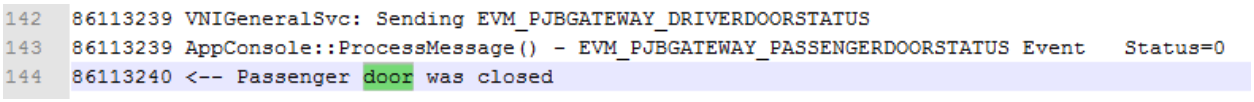
EVENT TYPE	IDENTIFIER	ACTION	DATE TIME	LATITUDE	LONGITUDE	ALTITUDE
GearShift	GearShift to Reverse at 2014-12-31 08:36:59	to Reverse	12/31/2014 8:36:59 AM	44.58295	-79.43032	
GearShift	GearShift to Park at 2014-12-31 08:37:03	to Park	12/31/2014 8:37:03 AM	44.58295	-79.43032	
GearShift	GearShift to Reverse at 2013-01-15 00:25:38	to Reverse	1/15/2013 12:25:38 AM	42.35353	-83.04633	
GearShift	GearShift to Drive at 2013-01-15 00:25:52	to Drive	1/15/2013 12:25:52 AM	42.35349	-83.04632	

iVe report of various events with vehicle and infotainment system

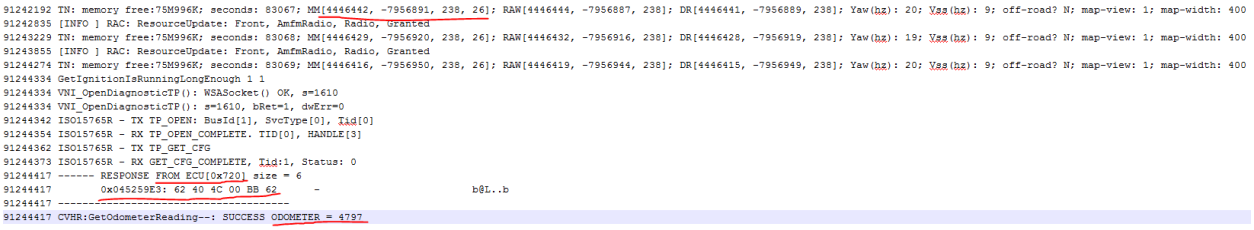
2013 Ford F-150 SYNC Generation II – Logical Acquisition



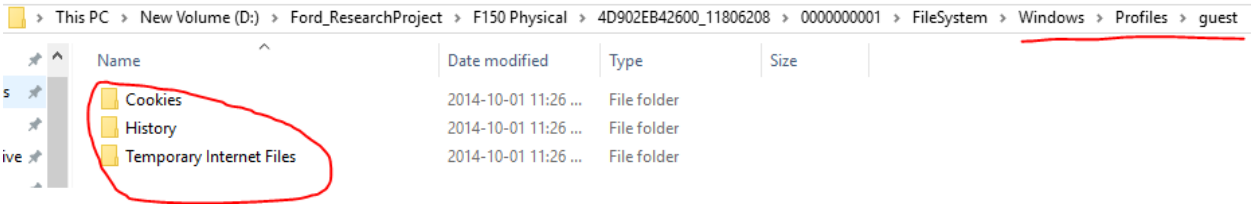
Device ID and contacted phone number found under call history XML file



Log of passenger door being closed



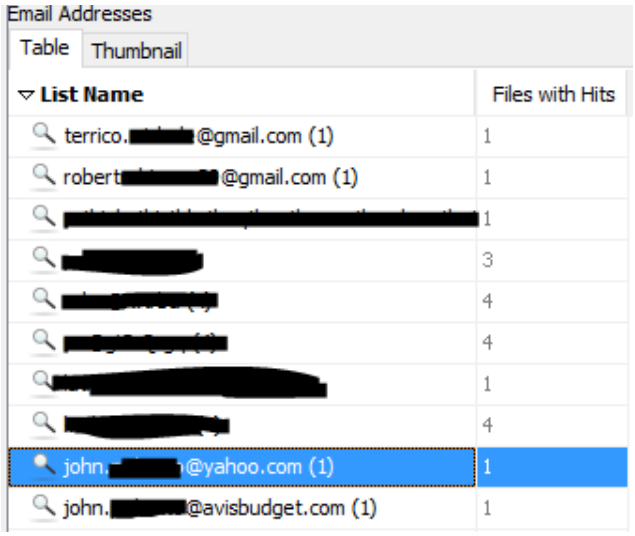
Various logged interactions such as odometer reading, GPS coordinates and ECU response



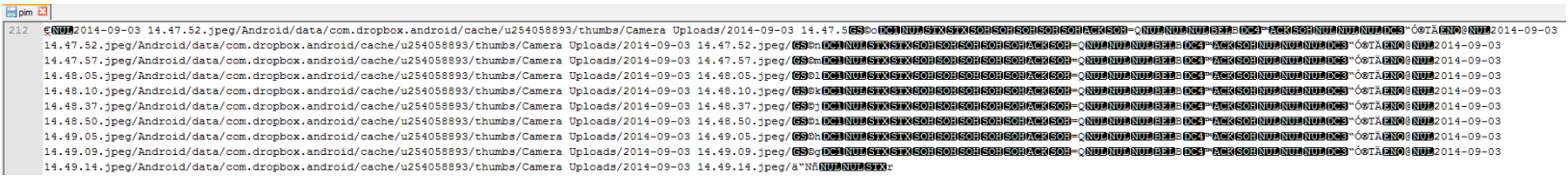
Potential Internet user history if feature is enabled and used

2013 Dodge Durango uConnect version 8.4 – Logical Acquisition

Test screenshot recovered



Emails found in extraction



Potential user activity

DEVICE NAME	DEVICE TYPE	MANUFACTURER	MODEL	INTERFACETYPE	UNIQUE NUMBER TYPE	UNIQUE NUMBER	SOURCE LOCATION
INTERNET						/dev/socket	
USB						D0B112F4C762620F086E1A17E0[redacted]	
Fox iPhone III	phone	APPLE	APPLE_IPHONE	Bluetooth	Bluetooth Address	54E43A23[redacted]	
Fox iPhone III						54:E4:3A:[redacted]	
Heather [redacted] iPhone						C0:63:94:[redacted]	
Heather [redacted] iPhone						C063945[redacted]	
Heather [redacted] iPhone						C39M77T[redacted]	
Chu Phone	phone	APPLE	APPLE_IPHONE	Bluetooth	Bluetooth Address	B8782E8[redacted]	

iVe report showing Bluetooth MAC addresses and other identifiers

TEXT MESSAGES (SMS)

DATE/TIME	TO	FROM	NAME	BODY	READ STATUS	DEVICEIDENTIFIER
9/14/2014 9:29:59 AM		4125892[redacted]		Ok	read	A49A5880[redacted]
9/14/2014 9:29:10 AM		4125892[redacted]		I just tried to call you he around you can't really talk?	read	A49A5880[redacted]
9/14/2014 9:25:34 AM		4125892[redacted]		OMG That's crazy I seen all the calls this morning I was like Damn I passed the fuk out I felt so bad why the funk does he do that to you	read	A49A5880[redacted]
9/14/2014 9:23:19 AM		4125892[redacted]		I got the biggest hangover and still spitting up	read	A49A5880[redacted]
9/14/2014 8:48:06 AM		4125892[redacted]		You ok	read	A49A5880[redacted]
9/14/2014 8:33:17 AM		4125892[redacted]		Call me I threw up and then passed out	read	A49A5880[redacted]

iVe report of SMS data and related device

CALL LOG ENTRIES

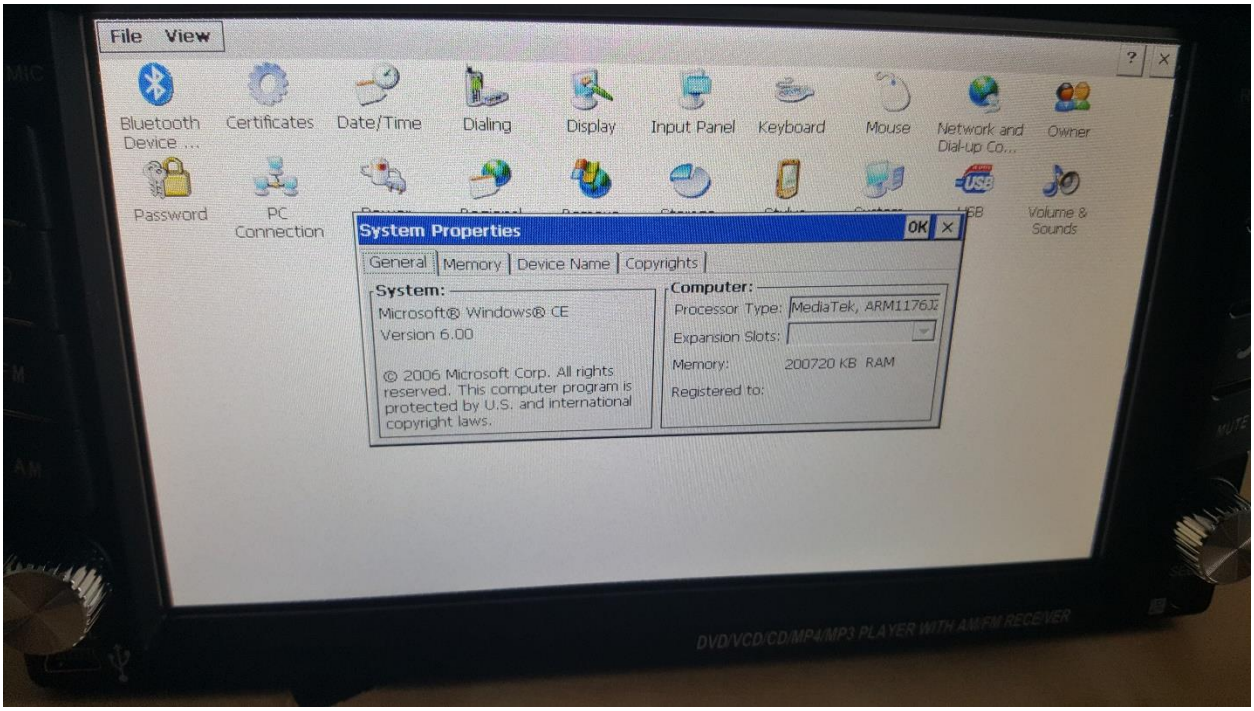
START TIME	PHONE NUMBER	CONTACT NAME	CALL TYPE	DEVICEIDENTIFIER
6/18/2014 11:58:32 AM	+1772216[redacted]			54E43A23[redacted]
6/15/2014 4:09:17 PM	0044126850[redacted]			54E43A23[redacted]
6/13/2014 5:37:24 PM	+447764684[redacted]	Emma [redacted]		54E43A23[redacted]
6/7/2014 5:26:30 PM	+17722169[redacted]			54E43A23[redacted]
6/7/2014 5:26:13 PM	7722169[redacted]			54E43A23[redacted]
6/7/2014 5:25:53 PM	+19542612[redacted]			54E43A23[redacted]

iVe report of call logs associated to a specific mobile device

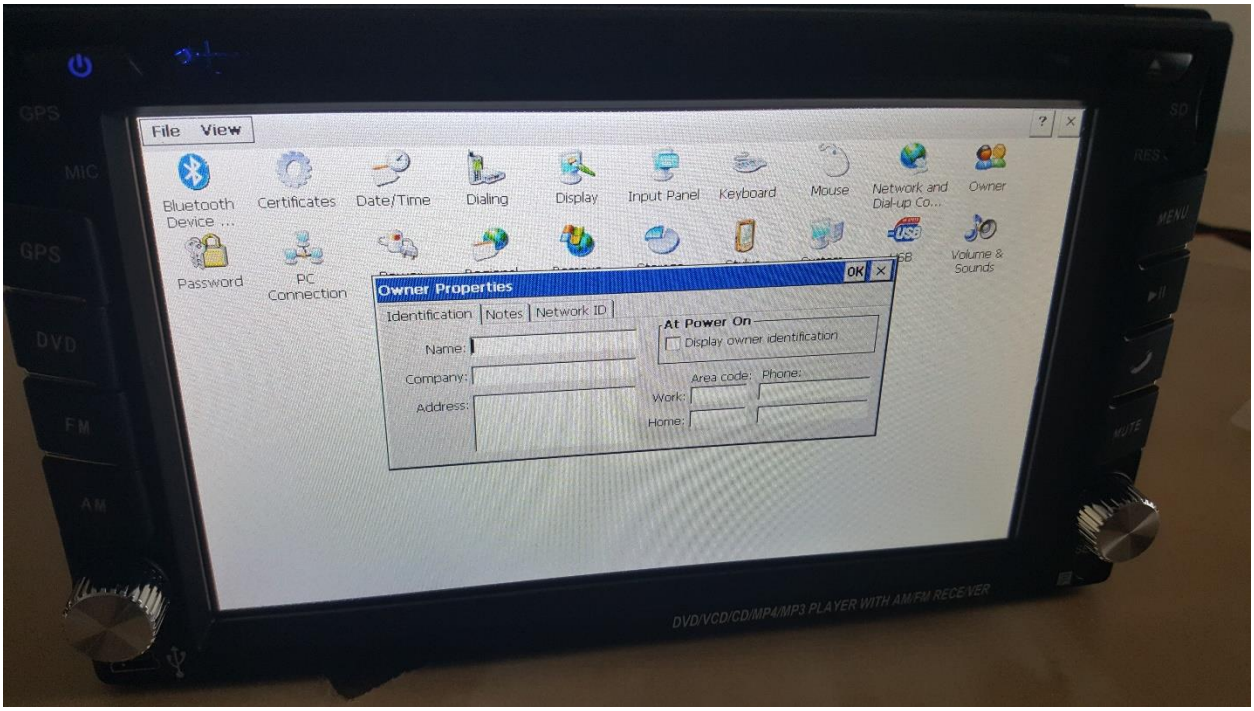
VEHICLEVIN	1C4RDHDG3EC537565
VEHICLEYEAR	2014
VEHICLEMANUFACTURER	Dodge
VEHICLEMODEL	Durango
VEHICLETRIMLEVEL	Limited
VEHICLEECU	uConnect 8.4A / 8.4AN

iVe report of system information

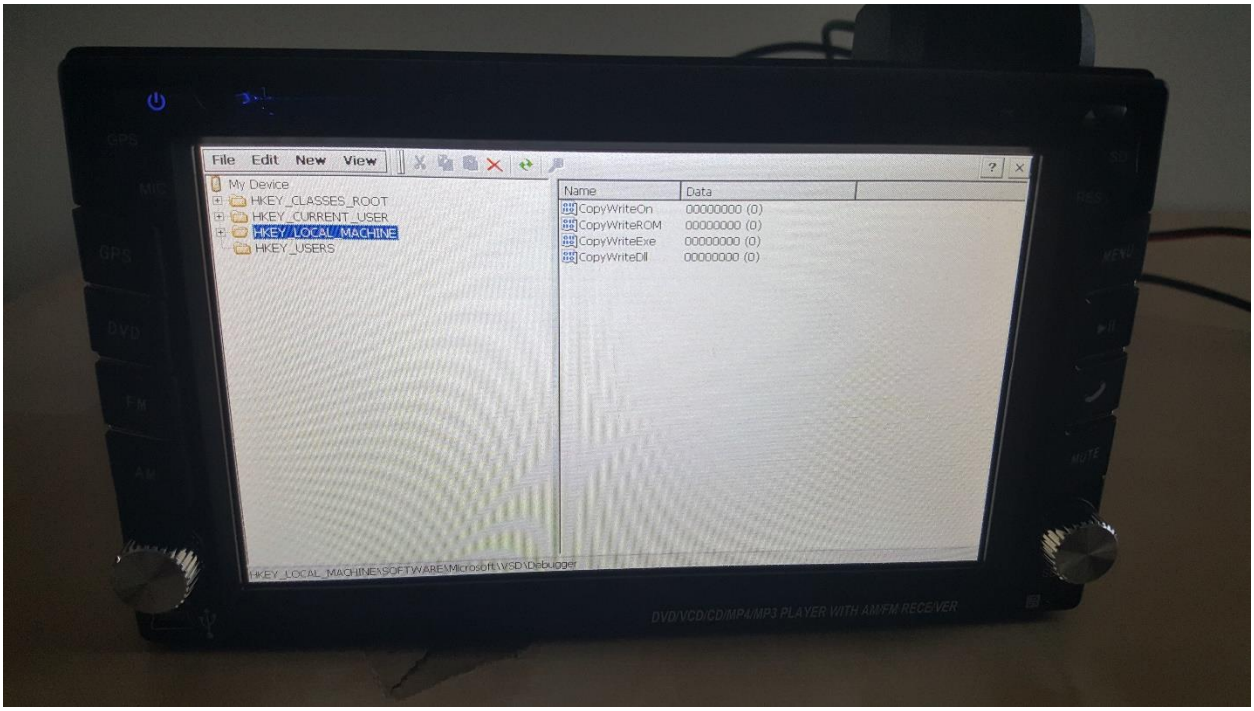
Ouku Windows CE – Logical Acquisition



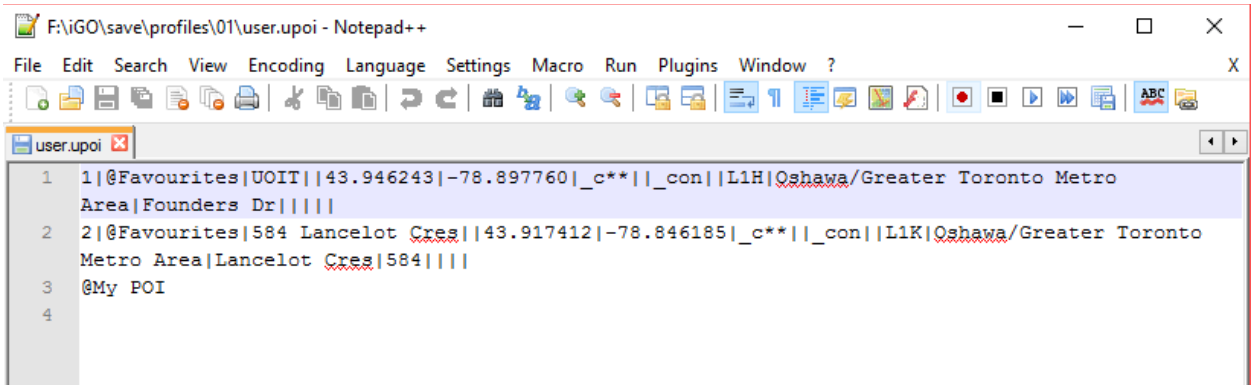
System Information



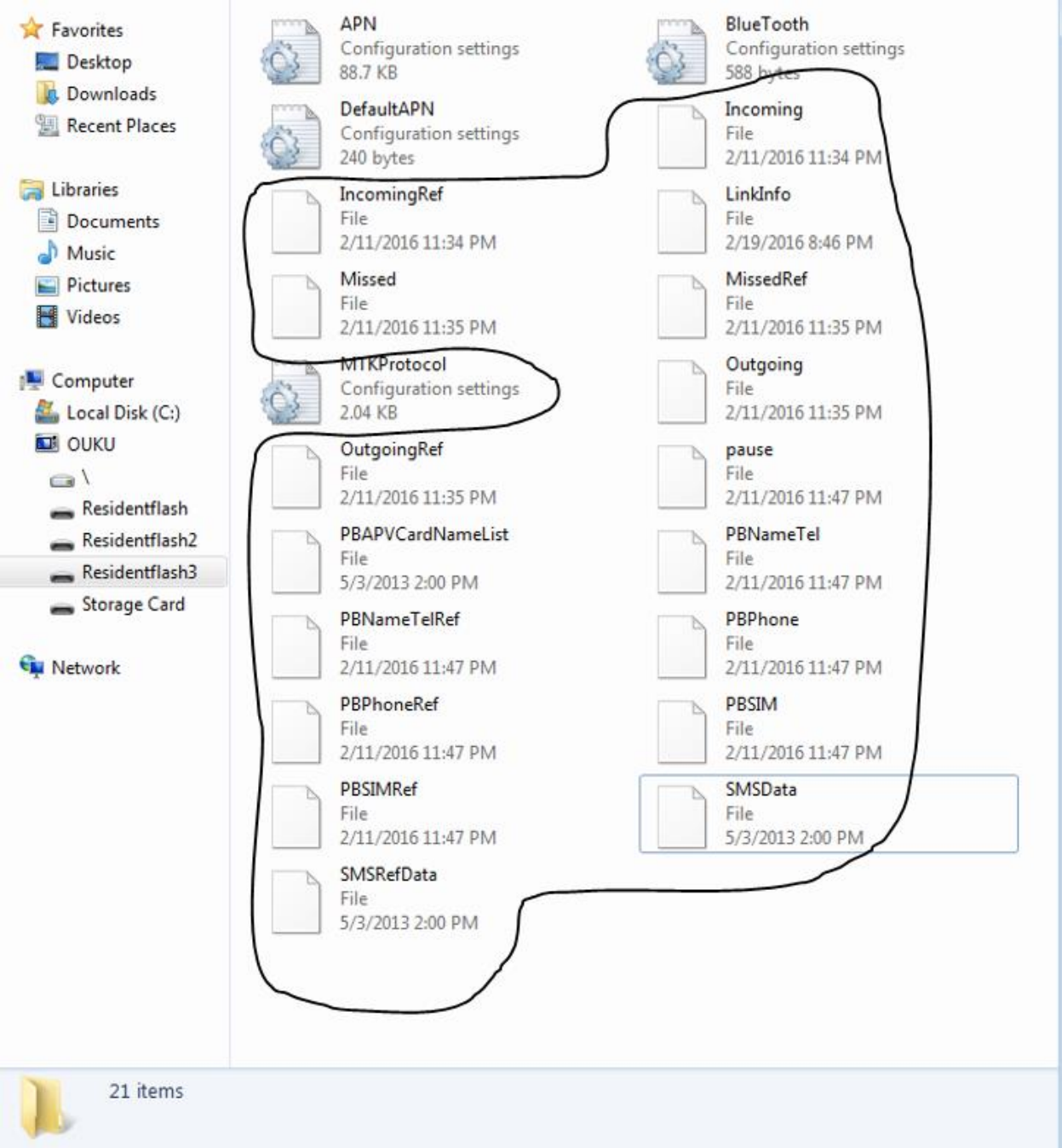
Potential owner information if set



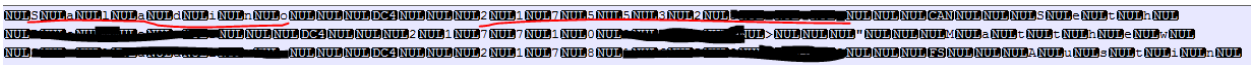
Device registry files can be viewed



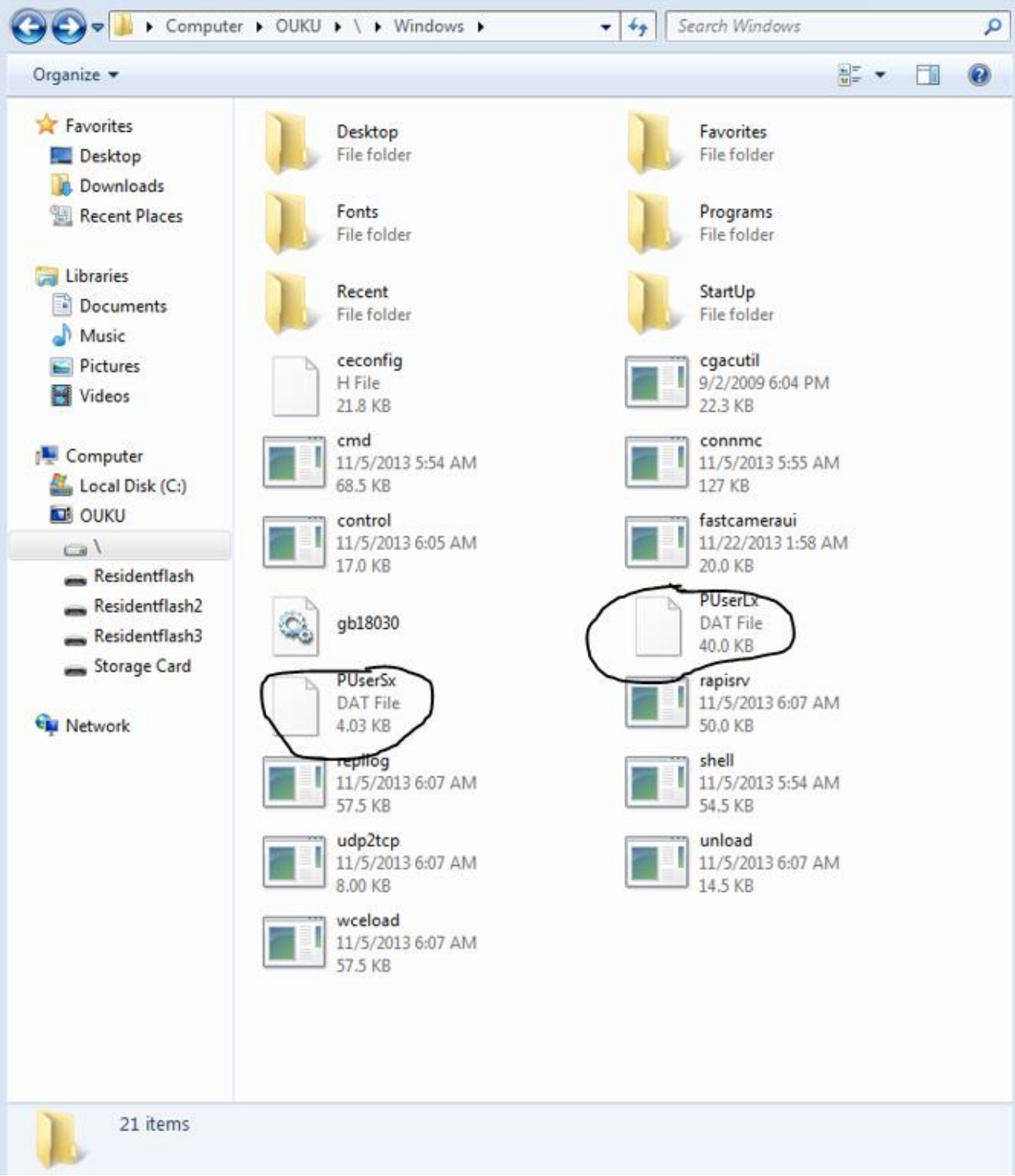
Favorited location information



Files containing contact and relative call logs information

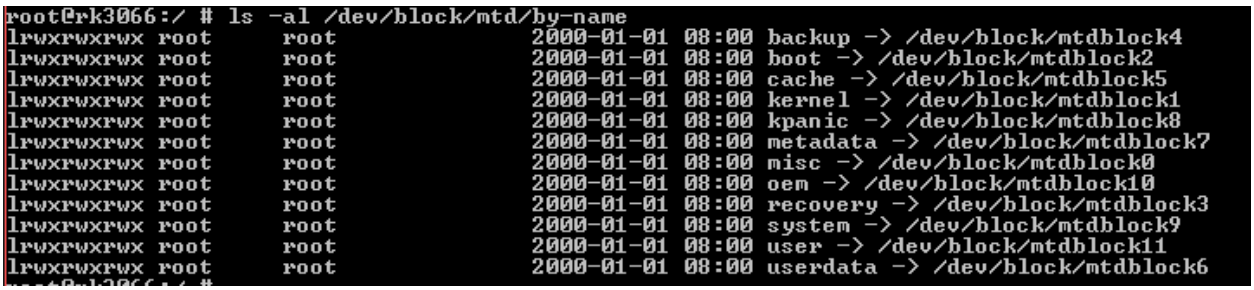


File showing contact names and associated phone numbers

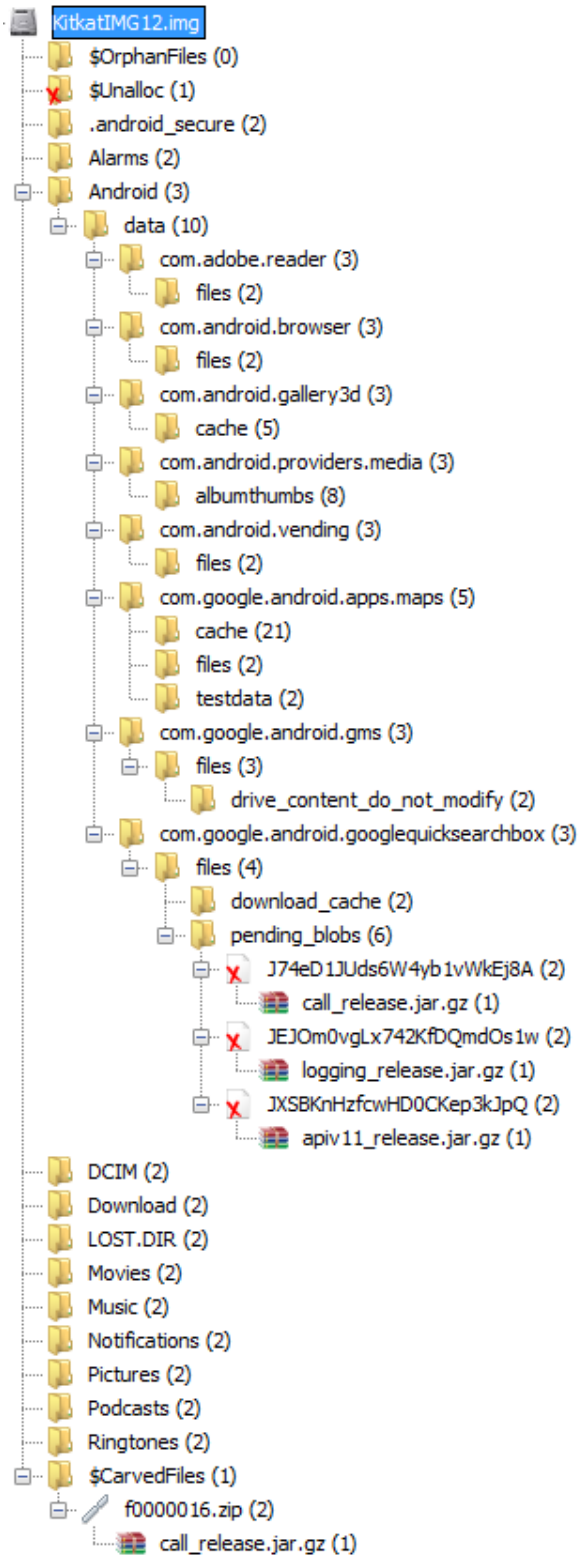


Potential user information but data is not in a readable format

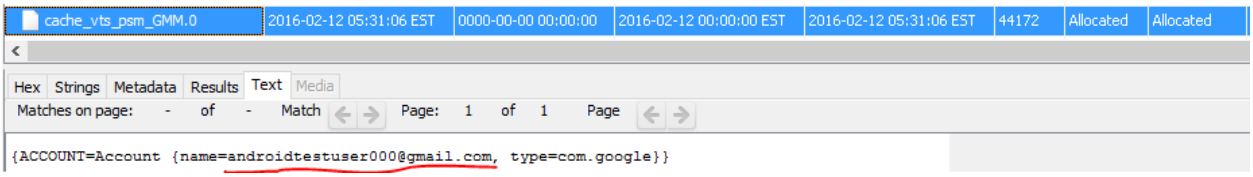
Pumpkin Android Kit-Kat 4.4.4 – Physical Acquisition



Acquired MTD blocks

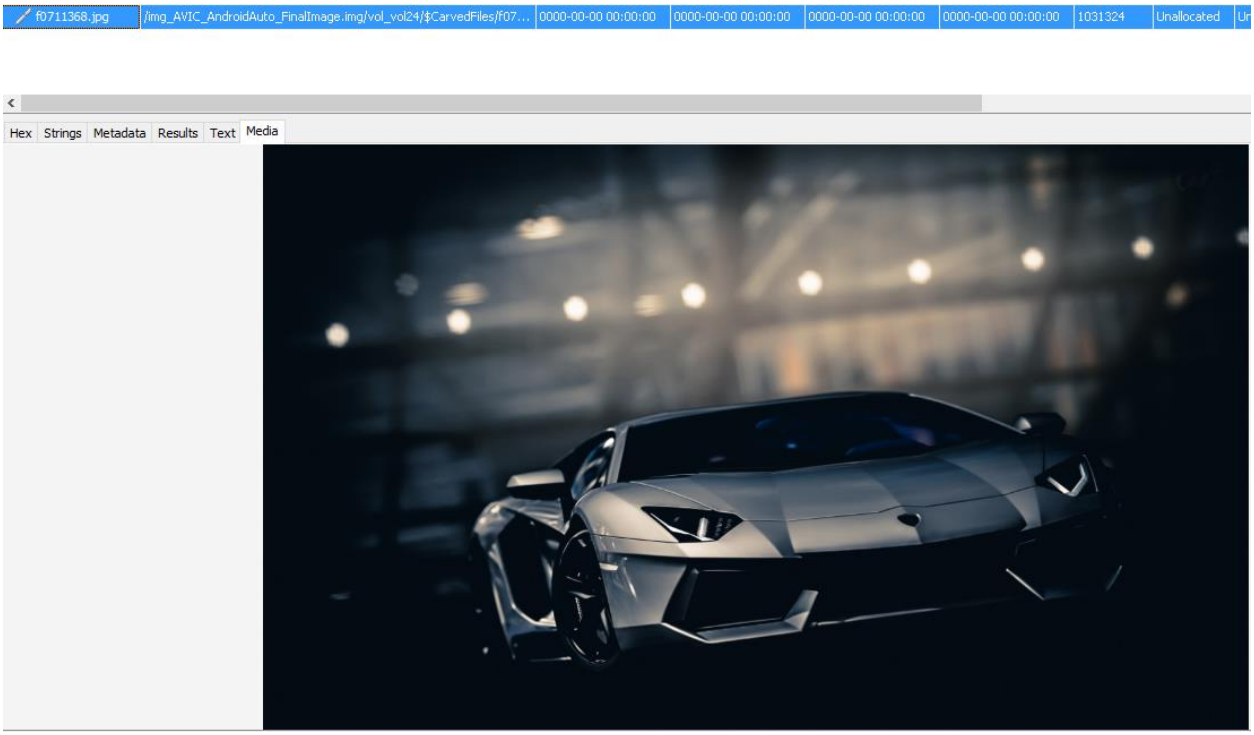


Available folders (limited data)

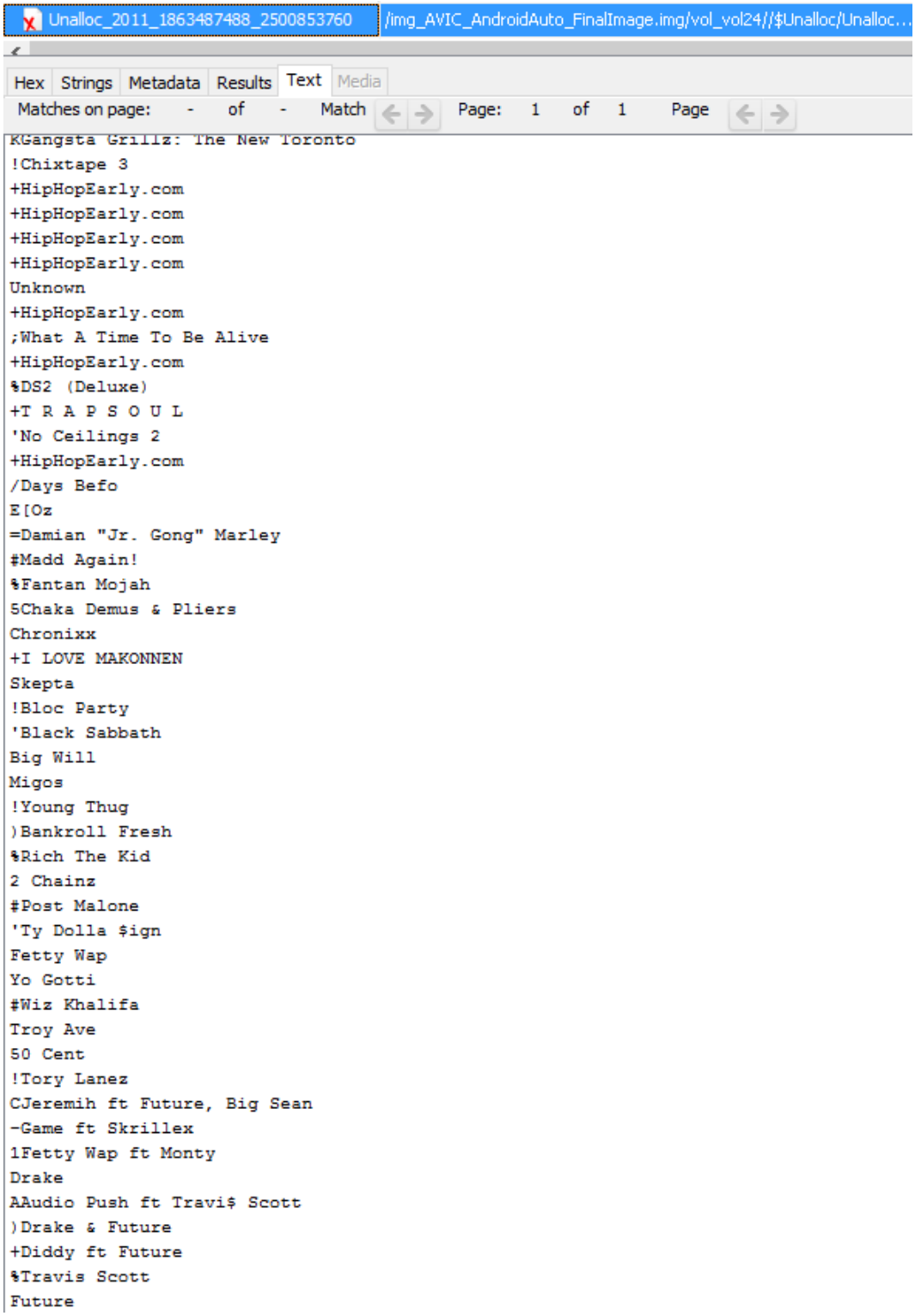


Test Google Play account located

Pioneer Android-based OS – Physical Acquisition



Recovered background image



Media playlist information


wmay@cisco.com

Table | Thumbnail

Source File	Keyword	Keyword Preview
NOTICE.txt	wmay@cisco.com	«wmay@cisco.com« * *
NOTICE_AVN.txt	wmay@cisco.com	«wmay@cisco.com« * *

Emails found in source files

Extra

Example of Ford SYNC module retrieval process

Entire Ford SYNC module

Ford SYNC storage module (JTAG acquisition done on board residing inside encasement)

Bibliography

[1] Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). *Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions*. In Information Security for South Africa, 2013 (pp. 1–8). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6641058

[2] Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

[3] Ashcroft, J., Daniels, D. J., Hart, S. V. (April, 2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (pp. 1–91). Retrieved January 29th, 2016, from http://ecrime.on.ca/intake/files/Forensic%20Examination%20of%20Digital%20Evidence%20-%20A%20Guide%20for%20Law%20Enforcement.pdf

[4] Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (No. NIST SP 800-101r1). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[5] Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. Digital Investigation, 10(4), 323–349. https://doi.org/10.1016/j.diin.2013.10.003

[6] Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. In *Proceedings of the Fourth Digital Forensic Research Workshop* (pp. 1–9). Retrieved January 29th, 2016, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.492&rep=rep1&type=pdf&embedded=true

[7] Cai, L., Zeng, K., Chen H. and Mohapatra, P. “Good neighbor: ad hoc pairing of nearby wireless devices by multiple antennas.” in NDSS, 2011.

[8] Canlar, E. S., Conti, M., Crispo, B., & Di Pietro, R. (2013). Windows Mobile LiveSD Forensics. Journal of Network and Computer Applications, 36(2), 677–684. https://doi.org/10.1016/j.jnca.2012.12.024

[9] Carney, J.J. Small Scale Digital Device Forensics–Evidence from Mobile Phones and GPS Units May Surprise You!.

[10] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T. “Comprehensive experimental analyses of automotive attack surfaces.” in USENIX Security Symposium, 2011.

[11] Chen, S.-W., Yang, C.-H., & Liu, C.-T. (2011). Design and Implementation of Live SD Acquisition Tool in Android Smart Phone (pp. 157–162). IEEE. https://doi.org/10.1109/ICGEC.2011.46

[12] Chung, E. (October 27th, 2014). Carmakers Ignore Hacking Risk, Security Expert Says. Retrieved June 5th, 2015 from http://www.cbc.ca/beta/news/technology/carmakers-ignore-hacking-risk-security-expert-says-1.2810847

[13] Cohen, T. 2011. Look At What My Car Can Do, DEFCON 19, Unpublished, 2011, [video presentation].

[14] Court of Appeal of Ontario. (February, 2013). *R. v. Fearon, 2013 ONCA 106 (CanLII)* (pp. 1– 27). Retrieved January 29th, 2016, from https://www.canlii.org/en/on/onca/doc/2013/2013onca106/2013onca106.pdf

[15] CTV Ottawa, (October 8th, 2013). Would You Put a Black Box on Your Car to Lower Insurance Rates? Retrieved on November 5th, 2014 from http://ottawa.ctvnews.ca/would-you-put-a-black-box-on-your-car-to-lower-insurance-rates-1.1489201

[16] Ertaul, L. and Mullapudi, S. "The security problems of Vehicular Ad Hoc Networks (VANETs) and proposed solutions in securing their operations." in ICWN, 2009, pp. 3–9.

[17] Everett, C. E., & McCoy, D. (n.d.). OCTANE: Open Car Testbed And Network Experiments Bringing Cyber-Physical Security Research to Researchers and Students. Retrieved from https://www.usenix.org/system/files/conference/cset13/cset13-everett.pdf

[18] Fox-Brewster, T. (March 25th, 2015). Former Tesla Intern Releases $60 Full Open Source Car Hacking Kit For The Masses. Retrieved June 5th, 2015 from http://www.forbes.com/sites/thomasbrewster/2015/03/25/hack-a-car-for-60-dollars/#467bbef01b03

[19] Garfinkel, S. L. (2010). *Digital forensics research: The next 10 years.* Digital Investigation, 7, S64–S73. http://doi.org/10.1016/j.diin.2010.05.009

[20] Glisson, W. B., Storer, T., & Buchanan-Wollaston, J. (2013). An empirical comparison of data recovered from mobile forensic toolkits. Digital Investigation, 10(1), 44–55. https://doi.org/10.1016/j.diin.2013.03.004

[21] Glisson, W. B., Storer, T., Mayall, G., Moug, I., & Grispos, G. (2011). Electronic retention: what does your mobile phone reveal about you? International Journal of Information Security, 10(6), 337–349. https://doi.org/10.1007/s10207-011-0144-3

[22] Gonzales, A. R., Schofield, R. B. Hagy, D.W. (January, 2007). *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (pp. 1 – 81). Retrieved January 29th, 2016, from

http://ecrime.on.ca/intake/files/Digital%20Evidence%20in%20the%20Courtroom%20-%20A%20Guide%20for%20Law%20Enforcement%20and%20Prosecutors.pdf

[23] Gonzales, A. R., Schofield, R. B. Hagy, D.W. (January, 2007). *Investigations involving the Internet and Computer Networks* (pp. 1 – 137). Retrieved from January 29th, 2016, http://ecrime.on.ca/intake/files/Investigations%20Involving%20the%20Internet%20and%20Computer%20Networks.pdf

[24] Greenberg, A. (21st of July, 2015). Hackers Remotely Kill a Jeep on the Highway – With Me in it. Retrieved October 3rd, 2015 from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[25] Grispos, G., Storer, T., & Glisson, W. B. (2011). A comparison of forensic evidence recovery techniques for a windows mobile smart phone. Digital Investigation, 8(1), 23–36. https://doi.org/10.1016/j.diin.2011.05.016

[26] Guo, H., Ahmed, D.T., and Saddik, A. E. 2013. Web services for VANET: a service oriented architecture for infotainment system based on mashup using open APIs, InProceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications (DIVANet '13). ACM, New York, NY, USA, 61-68.

[27] Hannay, P. 2013. Geo Forensics: Classes of Locational Data Sources for Embedded Devices. International Journal of Engineering and Technology, pp. 262–265, 2013.

[28] He, J., Wan, X., Liu, G., Huang, N. and Zhao, B. 2013. On the Application of Digital Forensics in Different Scenarios. Sponsored by IEEE Louisville chapter, pp. 1-5

[29] IEEE Standards Association, “IEEE guide for wireless Access in vehicular environments (WAVE) architecture,” 2013.

[30] Illera, A. G. and Vidal, J. V. 2013. Dude, WTF In My Car, DEFCON 21, Unpublished, 2013, [video presentation].

[31] Jovanovic, Z. and Redd, I. D. D. (2012). Android forensics techniques. International Academy of Design and Technology. Retrieved from http://www.bulleproof.com/Papers/Android%20Forensics%20Techniques.pdf

[32] Kang, M., S., Lee, S., B. and Gligor, V., D. “The crossfire attack”. in IEEE Symposium on Security and Privacy, 2013.

[33] Kopylova, Y., Farkas, C. and Xu, W. 2011. Accurate accident reconstruction in VANET. In Data and Applications Security and Privacy XXV, Springer, 2011, pp. 271–279.

[34] Kramer, J. A. (2013). DroidSpotter: A Forensic Tool for Android Location Data Collection and Analysis. Retrieved from http://lib.dr.iastate.edu/etd/13407/

[35] LeMere, B. 2013. Vehicle System Forensics, CEIC Orlando, Unpublished, [slide presentation].

[36] Lessard, J., & Kessler, G. (2010). Android Forensics: Simplifying Cell Phone Examinations. Retrieved from http://ro.ecu.edu.au/ecuworks/6479/

[37] Lin, C., Wu, G., Xia, F. and Yao, L. “Enhancing efficiency of node compromise attacks in Vehicular Ad hoc Networks using connected dominating set,” Mobile Networks and Applications, vol. 18, no. 6, pp. 908–922, Dec. 2013.

[38] Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P-H. and Shen, X. “Security in Vehicular Ad Hoc Networks.” Communications Magazine, IEEE, vol. 46, no. 4, pp. 88–95, 2008.

[39] Maaroufi, S. and S. Pierre S. 2014. Vehicular social systems: an overview and a performance case study. In Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications (DIVANet '14). ACM, New York, NY, USA, 17-24. DOI: http://dx.doi.org/10.1145/2656346.2656352

[40] Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic analysis of instant messenger applications on android devices. arXiv Preprint arXiv:1304.4915. Retrieved from http://arxiv.org/abs/1304.4915

[41] Markey, E. [Staff of United States Senator of Massachusetts] (July 21st, 2015). Tracking & Hacking: Security & Privacy Gaps Put American Drivers At Risk. Retrieved the October 3rd, 2015 from https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

[42] Mearian, L. (December 12th, 2014). Ford Dumps Microsoft for QNX, Unleashes New Functions in Sync v3. Retrieved October 3rd, 2015 from http://www.computerworld.com/article/2859373/ford-dumps-microsoft-for-qnx-unleashes-new-functions-in-sync-v3.html

[43] Mejri, M. N. and Ben-Othman, J. 2014. Entropy as a new metric for denial of service attack detection in vehicular ad-hoc networks," In Proceedings of the 17th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems (MSWiM '14). ACM, New York, NY, USA, 73-79.

[44] Miller, C. and Valasek, C. (post 2012). Adventures in Automotive Networks and Control Units. Unpublished.

[45] Mukasey, M. B., Sedwick, J. L., Hagy, D. W. (April, 2008). *Electronic crime scene investigation: a guide for first responders.* (pp. 1–74). Retrieved January 29th, 2016, from http://ecrime.on.ca/intake/files/Electronic%20Crime%20Scene%20Investigation%20-%20A%20Guide%20for%20First%20Responders%20-%20Second%20Edition.pdf

[46] Mutanga, M. B., Mudali, P., Dlamini, I. Z., Ndlovu, L., Xulu, S. S., Adigun, M. O., (May, 2010). *Challenges of Evidence Acquisition in Wireless Ad-Hoc Networks*. (pp. 1–8). IST- Africa (Conference), Cunningham, P., Cunningham, M., Institute of Electrical and Electronics Engineers, European Commission, Institute of Electrical and Electronics Engineers, Computer Society of South Africa. (2010). 2010 IST-Africa 19-21 May 2010, Durban, South Africa. Danvers, MA: IIMC International Information Management Corp. Retrieved from http://ieeexplore.ieee.org/servlet/opac?punumber=5749993

[47] Ntantogian, C., Apostolopoulos, D., Marinakis, G., & Xenakis, C. (2014). Evaluating the privacy of Android mobile applications under forensic analysis. Computers & Security, 42, 66–76. https://doi.org/10.1016/j.cose.2014.01.004

[48] Ontario Provincial Police. (n.d.). *Analog/Digital Evidence Seizure Checklist* (pp.1). Retrieved January 29th, 2016, from http://ecrime.on.ca/intake/files/OPP%20Analog%20Digital%20Evidence%20Checklist.pdf

[49] Ontario Provincial Police. (May, 2014). *Articulation of Categories* (pp. 1–13). Retrieved January 29th, 2016, from http://e-crime.on.ca/intake/files/articulation_of_categories.pdf

[50] Ontario Provincial Police. (May, 2015). *Best Practices for Seizing Electronice Evidence* (pp. 1–24). Retrieved January 29th, 2016, from http://e-crime.on.ca/intake/files/BestPractices%20V3.pdf

[51] Ontario Provincial Police. (May, 2015). *Cellular Telephone Exhibit Handling Basics* (pp. 1– 13). Retrieved January 29th, 2016, from http://e-crime.on.ca/intake/files/2015_05_Cell_Phone_Handling_Basics.pdf

[52] Ontario Provincial Police. (n.d.). *Computer Seizure Checklist* (pp. 1–2). Retrieved January 29th, 2016, from http://ecrime.on.ca/intake/files/Computer%20Seizure%20Checklist.pdf

[53] Ontario Provincial Police. (February, 2016). *Consideration for iOS 8 and Above* (pp. 1–12). Retrieved February 15th, 2016, from http://ecrime.on.ca/intake/files/Considerations%20for%20iOS%208%20and%20above.pdf

[54] Ontario Provincial Police. (n.d.). *Relevant Computer/Cell Phone Case Law* (pp. 1–7) Retrieved January 29th, 2016, from http://e-crime.on.ca/intake/files/DCLR2014.pdf

[55] Ontario Provincial Police. (February, 2012). *Search Warrant Guidelines - Cell Phones* - (pp. 1–5) Retrieved January 29th, 2016, from http://e-crime.on.ca/intake/files/sw_guidelines_cell.pdf

[56] Ontario Provincial Police. (February, 2012). *Search Warrant Guidelines - Computers* - (pp. 1–5) Retrieved January 29th, 2016, from http://e-crime.on.ca/intake/files/sw_guidelines.pdf

[57] Ontario Provincial Police. (February, 2012). *Search Warrant Guidelines - GPS* - (pp. 1–3) Retrieved January 29th, 2016, from

http://e-crime.on.ca/intake/files/sw_guidelines_gps.pdf

[58] Park, Y., Lee, S., Kim, J., & Shon, T. (2014). *Applying Digital Forensics in Various Application Fields: Required Elements for Having Legal Force.* In IT Convergence and Security (ICITCS), 2014 International Conference on (pp. 1–4). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7021741

[59] Parno, B. and Perrig, A. "Challenges in securing vehicular networks." in Workshop on hot topics in networks (HotNets-IV), 2005, pp. 1–6.

[60] Quick, D., & Choo, K.-K. R. (2014). Google Drive: Forensic analysis of data remnants. Journal of Network and Computer Applications, 40, 179–193. https://doi.org/10.1016/j.jnca.2013.09.016

[61] Rafique, M., & Khan, M. N. A. (2013). *Exploring Static and Live Digital Forensics: Methods, Practices and Tools.* International Journal of Scientific & Engineering Research, 4(10), 1048–1056.

[62] Raghavan, S. (2013). *Digital forensic research: current state of the art*. CSI Transactions on ICT, 1(1), 91–114. http://doi.org/10.1007/s40012-012-0008-7

[63] Rawat, A., Sharma, S. and Sushil, R. "VANET: Security attacks and its possible solutions". Journal of Information & Operations Management, vol. 3, no. 1, 2012.

[64] Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1–12.

[65] Rizzo, C. and Brookson, C. "ETSI white paper No. 1 security for ICT – the Work of ETSI.," ETSI, 2014.

[66] Schaefer, T., Höfken, H., and Schuba,M. 2012. “Windows Phone 7 from a Digital Forensics’ Perspective,” in Digital Forensics and Cyber Crime, Springer, 2012, pp. 62–76.

[67] Seo, J., Lee, S., & Shon, T. (2013). *A study on memory dump analysis based on digital forensic tools.* Peer-to-Peer Networking and Applications, 8(4), 694–703. http://doi.org/10.1007/s12083-013-0217-3

[68] Smith, C. (2014). Car Hackers’ Handbook. Unpublished.

[69] The Associated Press (September 4th, 2013) Hackers Hijack Car Computers and Take the Wheel. Retrieved June 5th, 2015 from http://www.cbc.ca/news/technology/hackers-hijack-car-computers-and-take-the-wheel-1.1322678

[70] The Indian Express. (February, 2016). *Apple vs FBI battle over iPhone 5c: Here’s everything you need to know*. Retrieved February 28th, 2016, from http://indianexpress.com/article/technology/tech-news-technology/apple-fbi-iphone-5c-san-bernadino-case-all-you-need-to-know/

[71] Thilakarathna, Petander, K. H. , Mestre, J. and Seneviratne, A. 2012. Enabling mobile distributed social networking on smartphones, In Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, 2012, pp. 357–366.

[72] Vidas, T., Zhang, C., & Christin, N. (2011). Toward a general collection methodology for Android devices. Digital Investigation, 8, S14–S24. https://doi.org/10.1016/j.diin.2011.05.003

[73] Vömel, S., & Freiling, F. C. (2011). *A survey of main memory acquisition and analysis techniques for the windows operating system*. Digital Investigation, 8(1), 3–22. http://doi.org/10.1016/j.diin.2011.06.002

[74] Wall, M. 2014. Is your connected car spying on you?," bbc.com, November 4th, 2014. [Online]. Available: http://www.bbc.com/news/business-29566764. [Accessed: November 5th, 2014].

[75] Wei, Z., Yu, F. R., and Boukerche, A. 2014. Trust Based Security Enhancements For Vehicular Ad Hoc Networks. In Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications (DIVANet '14). ACM, New York, NY, USA, 103-109.

[76] Wundram, M., Freiling, F. C., & Moch, C. (2013). *Anti-forensics: The Next Step in Digital Forensics Tool Testing* (pp. 83–97). IEEE. http://doi.org/10.1109/IMF.2013.17

[77] Yoo, B., Park, J., Lim, S., Bang, J., & Lee, S. (2012). *A study on multimedia file carving method. Multimedia Tools and Applications,* 61(1), 243–261. http://doi.org/10.1007/s11042-010-0704-y

[78] Younes, M. B. and Boukerche, A. "Efficient traffic congestion detection protocol for next generation VANETs." Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 208-212.

[79] Yu, B., Xu, C-Z. and Xiao, B. "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[80] Zareen, M. S., Waqar, A., & Aslam, B. (2013). *Digital forensics: Latest challenges and response.* In Information Assurance (NCIA), 2013 2nd National Conference on (pp. 21–29). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6725320