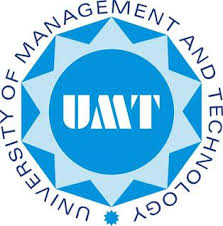
# Project Proposal



**Network Security**

**Topic: Smart Car Forensics**

**Proposed by**:

Moazzan Sabir(17010020006)

Ammar Khan (17010020010)

**Batch**: (10) BS\_CS

**Submitted to:** Sir Ayaz

**Abstract: -**

**Car forensic is one of the branches of digital forensics that is recently becoming more and more popular and important. Because of the accelerated growth of technology and its implementation in various industries, modern cars have additional features to raise the level of security, improve the driving experience, and now add the advanced option to connect the car to the internet. Vehicles are fast becoming another important source of digital evidence in a criminal investigation. Traditionally, when a vehicle is involved in a crime scene (e.g. drink driving), the investigators focus on the acquisition of DNA, fingerprints and other identifying materials, usually non digital in nature. However, modern day cars, particularly smart or driverless cars, store a wealth of digital information, such as recent destinations, favorite locations, routes, personal data such as call logs, contact lists, SMS messages, pictures, and videos.**

**Introduction: -**

Vehicles (also referred to as automotive) such as cars are not common sources of digital evidence traditionally. With the increased digitalization of our society, smart vehicles and driverless vehicles are becoming popular. Such vehicles have digital devices (e.g. digital multimedia systems, GPS systems, and Internet connectivity) integrated or built-in. For example, a driver is able to download his/her favorite music or view the status updates from his/her friends on Facebook, etc. via the built-in Wi-Fi in the car. In other words, modern-day vehicles store a range of (digital) information, driving-related data (e.g. recent destinations, favorite locations, routes), personal data (e.g. call logs, contact lists, SMS messages, pictures, and videos), and other communication data. Predictably, modern-day vehicles will be an important source of evidence in a digital forensic investigation, and vehicle system forensics is an emerging research area. Therefore, we describe challenges related to vehicle system forensics. We also discuss locations of different systems in a vehicle, where user data could potentially be located. Such information would facilitate forensic acquisition. As a new research area, Digital Forensics is a subject in rapid development. Cyber security for ICT (Information Communications Technology) gets more and more attention. Another focal point will be the cars onboard systems which will explain what security features can be found on car systems, and how they can be manipulated with. The next thing that will be explained is the digital evidence that can be found in a car during a forensic investigation and how the car’s systems can be accessed to find as much evidence as possible. An Electronic Control Unit (ECU) is a microcontroller that controls the operations of a car. In modern cars, there can be around seventy ECUs that control the overall operations of the vehicle. Each ECU is responsible for different operations, such as body control, engine control and telematics. A telematics unit for example, provides connectivity (Wi-Fi or cellular network) to the car, through which the car is able to communicate with the outside world. The different ECUs are connected within a car through networks such as Local Interconnect Network. For digital automotive forensics, the two main and commonly used features are the Event Data Recorder (EDR) and the insurance black box that works together with a telematics unit.

**Related Literature: -**

Vehicle system forensics is an emerging area of research, possibly due to the regency of smart and driverless vehicles as well as the supporting infrastructures such as smart cities, smart nations and Internet of Things. For example, researchers from the University of Tulsa researched on the security (vulnerability identification) and forensic aspects of automotive security. They explained the fundamentals of Controller Area Network bus (CAN-bus) and how to do perform reverse engineering on the signals. A device named TIB was designed to facilitate simulation of a vehicle so that a user can attach an Engine Control Unit (ECU). TIB also has an instrument cluster and a simulated anti-lock braking system. It is not clear, however, if their device allows connection to a digital multimedia system. In addition, their device may not be compatible with ECUs due to the different standard used in U.S. and Europe.

**Methodology: -**

Commonly, amid vehicle legal examination, the EDR, the infotainment unit and other ECUs are analyzed . In this proposition, the versatile application, Exchange, will be the reinforcement information for the EDR and other related information that might be of intrigued for forensics. Our proposition is based on the EVITA extend [9], which proposed an inserted Equipment Security Module (HSM) in the ECU to guarantee secure communications for on-board system. As proposed within the EVITA extend, each ECU has its claim HSM. This recommends that any hub communicating through the CAN transport is required to have get to authorization in arrange to send or get messages. In our proposal, the versatile gadget acts as a communicating hub through the CAN transport, and so requires get to authorization. To conduct a symptomatic on the car, the portable gadget is connected to the OBD-II harbor by means of Wi-Fi or Bluetooth. Once connected, the portable gadget will be confirmed, to determine whether it is approved to recover the requested data. Once verified, the versatile gadget is connected to the CAN transport, and able to get to the specified data. The primary thought of the Exchange application is to read the DTCs (Demonstrative Transmission Code) and log them securely. The DTCs can be perused by the client of the DiaLOG application, and from there, the client is mindful of the car’s condition and state.

**Assumptions: -**

The assumptions of the proposed Dialog application are as follows: The mobile application is installed on a mobile device and the mobile device is available for investigation. The data is always automatically transmitted to the phone and later to the cloud. On the off chance that information isn't updated Cloud Portable application after a certain time, the proprietor will be informed. Finally, the cloud is safely overseen. A client is confirmed to access the cloud server, and as it were approved clients have access to the information. Be that as it may, indeed in the event that an assailant is able to get to the information within the cloud, our convention protects the judgment and secrecy of the information.

**The Dialog application: -**

A versatile gadget with the Discourse application can log the most recent vehicle operations. This information is transferred to the cloud when a appropriate arrange association is available. From this system, the legal examiners have the options to urge the information from three distinctive sources: the car EDR, the portable gadget or the cloud. The car owner (having the Exchange

application and get to to the forensic data) has control of what information to share with third parties. Certain information is obligatory to get a service and the car owner will got to allow get to to the benefit provider. However, he/she has the control of the transmitted data and can confirm the correctness of information. The proposed architecture shields the protection of the car owner/driver, in a way that's not conceivable with the current system that transmits information through the telematics unit. The keys for the versatile gadget are put away in a secure memory for example on a secure component, or the portable gadget could be supporting Trust Zone.

1. Authentication phase: In order to use the Dialog with the mobile device, the mobile device is required to be authenticated to the car. Only the authorized mobile device is given permission to access the data from the car, and most importantly to connect with the car’s internal network. An authorized device is divided into two different levels: basic or full authorization.
2. Demonstrative stage: In this stage, the portable device is associated to the vehicle through a Wi-Fi connection, via an on-board switch. The portable gadget ought to be authenticated to the vehicle to guarantee as it were authorized mobile gadgets are allowed to obtain the vehicle’s diagnostic information. On the off chance that verification is effective, the mobile device will send a symptomatic command to the ECU, and the versatile will get the coming about information. This operation is computerized once association is set up and verification is confirmed. This way, the driver is continuously mindful of his/her vehicle condition. Separated from that, the consistency of information can be kept up between the portable application and the vehicle.
3. Data logging: Data to be logged in the Dialog application are as follows:
4. DTCs: are the blunder codes related with the components within the vehicle. The most work of a diagnostic is to perused the DTCs and to resolve the associated problems of the vehicle concurring to the codes.
5. (ii) ECU substance is the firmware, application and data available in each ECU. To recover all the information in all the ECUs would be time devouring and require a expansive memory to store it all. The (concatenated) hashed esteem of each ECU can be put away to provide an astuteness check. Utilizing the design as proposed in the EVITA extend [9], the ace ECU contains all the hashed values of all the ECUs. Any changes in the substance of the ECUs, i.e. any type in operation to the streak, will alter the hashed esteem stored in the master ECU. Thus, the ace ECU is additionally alerted of the changes. The Discourse application information is also being upgraded in like manner.
6. Capacity to cloud: The client can exchange the data from the portable gadget to the cloud. For illustration, after each driving cycle, all information is exchanged to the cloud as a capacity reinforcement. At any required time, the information can be retrieved and dissected.
7. Amid forensics: Prerequisites amid forensics incorporate (i) Accessibility of versatile application information, (ii) Accessibility of ECU information, (iii) Realness, astuteness and rightness of information. The most recent symptomatic information put away in the versatile gadget is examined amid information collection. The ECU information, counting the EDR is additionally perused. Amid the forensic examination prepare, this information is compared to ensure its consistency.

**Conclusion: -**

In the present current world, the digitalization of ordinary things is developing to an ever increasing extent. This impact didn't sidestep the vehicle business. Present day vehicles are getting more digitalized, with each new model another component or update of the past infotainment or security framework is added to make the regular voyaging and driving more secure what's more, simpler for clients or drivers. Along these lines, the vehicles are having increasingly more code that keeps all the additional usefulness running, which at last gives space for blunders, and security oversight that programmers can use in malignant ways. In this manner, the part of advanced legal sciences of vehicles has created in these pasts not many years. Be that as it may, the primary explanation isn't just to recuperate the programmer assaults on cars - car forensic is mainly used to solve crimes by connecting the criminals or the suspects to crimes committed while using a car. Extracting data from embedded car systems is done because it contains security logs of the vehicle moments before an accident happened. There is also the data from the infotainment systems that is more interesting for car forensic in cases different than traffic disputes. That is because it contains all kind of data and logs from the vehicle and devices that the vehicle was connected to. Ultimately, the car is one of the best sources of information or digital evidence today. And can be very useful if the forensic investigator knows the where to look for evidence and is familiar with the methods for data acquisition from a vehicle.