Department of Commerce

Division of State Fire Marshal

Promoting prosperity by protecting what matters most

VEHICLE FORENSICS: UNDERNEATH THE HOOD

Presented by: Brad Barkhurst
Forensic Specialist Supervisor
Ohio Fire Marshal Forensic Lab
Certified Berla Examiner
HTCIA Salt Fork Conference
May 22, 2025

Department of Commerce
Division of State Fire Marshal

WHAT IS VEHICLE FORENSICS?

- Digital vehicle forensics is a branch of digital forensics that involves recovering digital evidence or data stored in a vehicle's modules, networks, and messages sent across operating systems. The purpose of digital vehicle forensics is to provide evidence for criminal cases, root cause analysis and accident investigations.

-https://www.salvationdata.com/knowledge/what-is-digital-vehicle-forensics/

WHAT IS A GOOD SOURCE OF BEST PRACTICES?

- SWGDE.org
  - 2022-01-13 SWGDE Best Practices for Vehicle Infotainment and Telematics Systems_v3.0

- Provides information on safety concerns, evidence seizure and preserving data from vehicle infotainment and telematic systems. (This would often be viewed in the center console of a vehicle.)
- Provides information on data acquisition and analysis.
- What type of artifacts can be found during an analysis.

WHAT TRAINING IS AVAILABLE?

- Berla is the largest provider for vehicle forensics tools and training.
- Website: berla.co
- Based in Maryland
- They provide software and hardware kit called iVe.
- They provide in person and on location training. It is very hands on so it can't be done online. Most of the resources for this presentation are from the Berla workbook and app.

3 MAIN STEPS FOR A VEHICLE FORENSICS INVESTIGATION:

1) Identify

- What do you look at to identify the vehicle?

  -Make, model, VIN and trim.

  -This information can be entered into the Berla mobile app to see if the vehicle is even supported.

3 MAIN STEPS FOR A VEHICLE FORENSICS INVESTIGATION:

1) Identify continued…

- What type of data can be obtained? Depends (typically, cars pre-2008 don't provide much data.) This could be track logs, velocity logs, wifi connections, phone contacts, vehicle data, photos, audio recordings etc. What type of data for a specific vehicle can be found in the Berla app before doing the analysis.

- What is the vehicle's electronic control unit (ECU). Two types:
    1) Infotainment System - Person operates eg. Center console.
    2) Telematic System - Internal that person does not operate. Eg. OBD2 port.

3 MAIN STEPS FOR A VEHICLE FORENSICS INVESTIGATION:

2) Acquire

- Access the vehicle

  Typically: before opening the car door, take photos of vehicle, take photos of the vin # (by the front driverside window), take photos of the center console (may have to access the menu to find the version), turn off the vehicle if on, then disconnect the battery terminals.

- Extract the data

  This could be through the OBD2 port, USB port or vehicle module (blackbox.) Even key fobs and Onstar devices can hold data!

3 MAIN STEPS FOR A VEHICLE FORENSICS INVESTIGATION:

2) Acquire continued…

- Acquisition types:

  Physical (like a forensic image), logical , import (eg USB connection)

  If a module needs to be removed, once you get it out of the vehicle (It's a circuit board and housing), you still need to connect to it. That is a whole other process that we'll go into.

3 MAIN STEPS FOR A VEHICLE FORENSICS INVESTIGATION:

3) Analyze

- Once the data is acquired, the Berla iVe software is used to analyze it. The Berla analysis software is kind of like the FTK or Cellebrite for the vehicle forensics world.
- There are different artifacts you can search for depending on your investigation.
- Berla iVe software can save a case and generate a report. This can be imported into other tools to be read. I believe Cellebrite and Magnet can open Berla cases.

THINGS TO KEEP IN MIND AHEAD OF TIME:

- You will need to have the owner's consent or a search warrant to conduct the investigation.
- This process can sometimes take hours. Not only might you have to remove a vehicle module, but it also takes time to connect and extract the data. Don't forget, you have to put the module back too!
- It's good to have a garage in which you can work out of to protect yourself from the outside weather elements.

THINGS TO KEEP IN MIND AHEAD OF TIME:

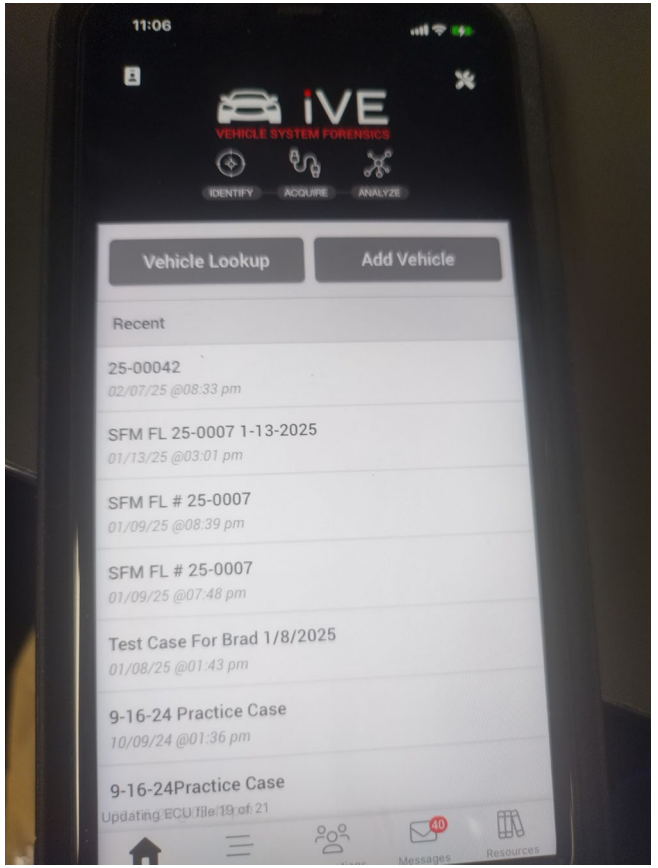
- There can be some nasty stuff in these vehicles, so you may need protective equipment.
- Before going out to a scene, get the make, model, trim and vin number ahead of time. No point in going somewhere if the vehicle is not supported!
- Bring a flashlight or headlamp, you may be crawling underneath stuff.

LET’S WORK A PRACTICE CASE:

- For my training, I was tasked with obtaining data from a 2019 Ford Focus. Let’s walk through this practice case:

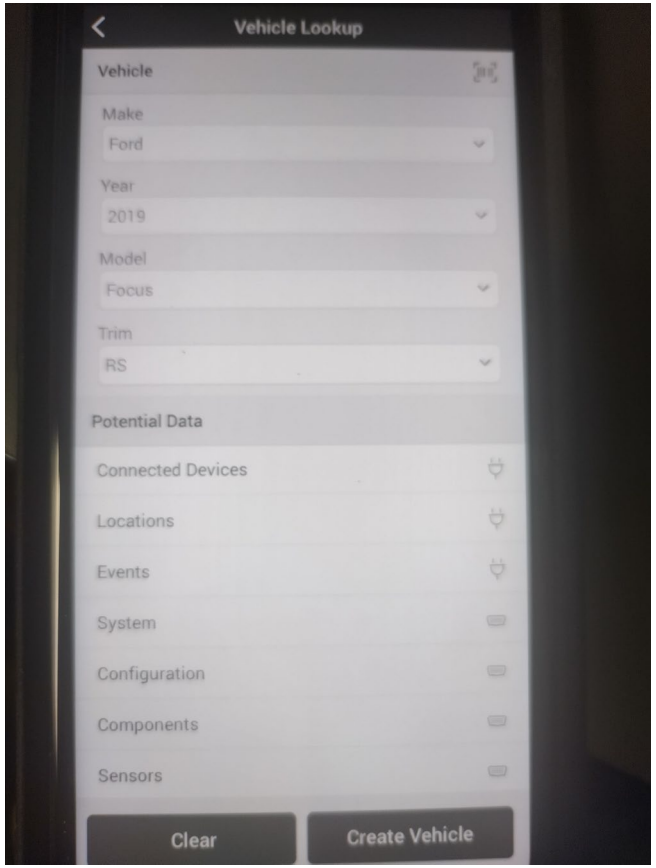
LET’S WORK A PRACTICE CASE:

- I took photos of the vehicle from all sides. I took a photo of the VIN #.
- I then added the vehicle in the Berla app.



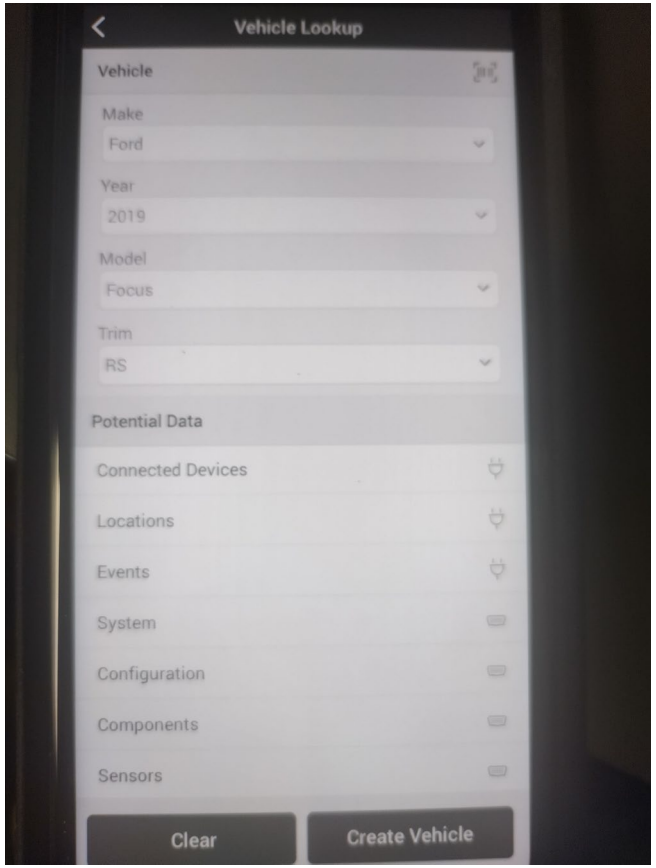
LET'S WORK A PRACTICE CASE:

- I type in the make, model and trim info into the app.



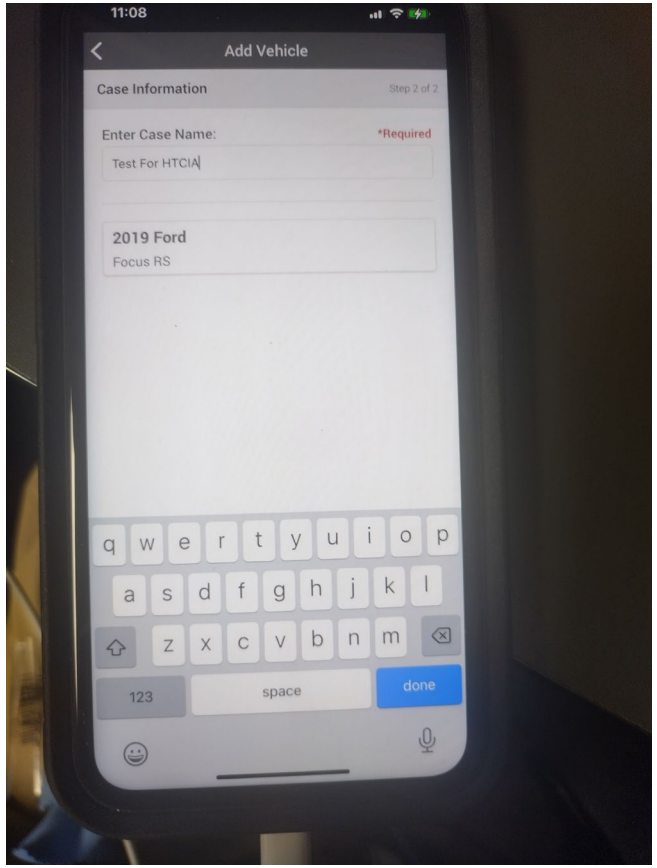
LET’S WORK A PRACTICE CASE:

- It will show me if the vehicle is vehicle is supported and the potential data that can be obtained.



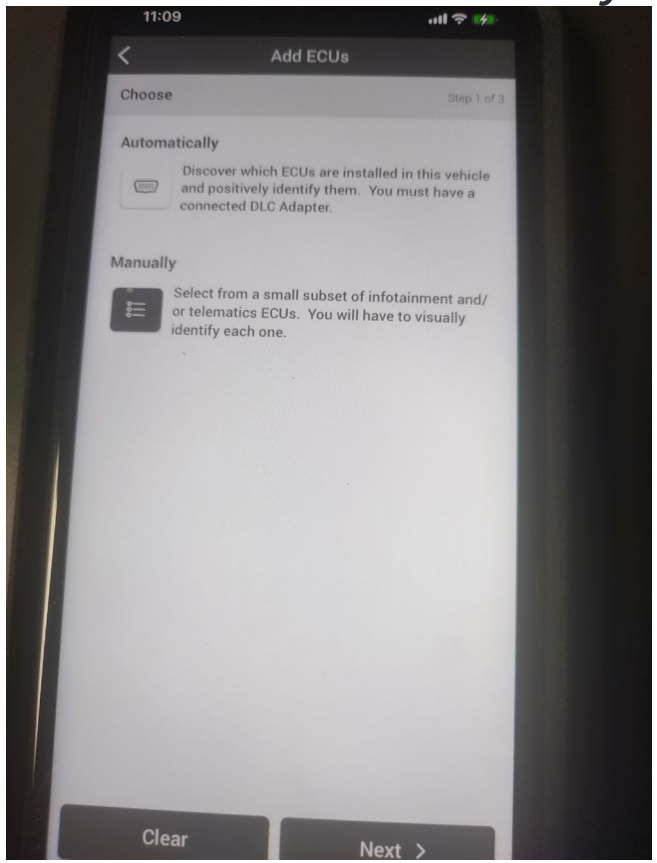
LET’S WORK A PRACTICE CASE:

- I type in my case number and brings up the vehicle info:



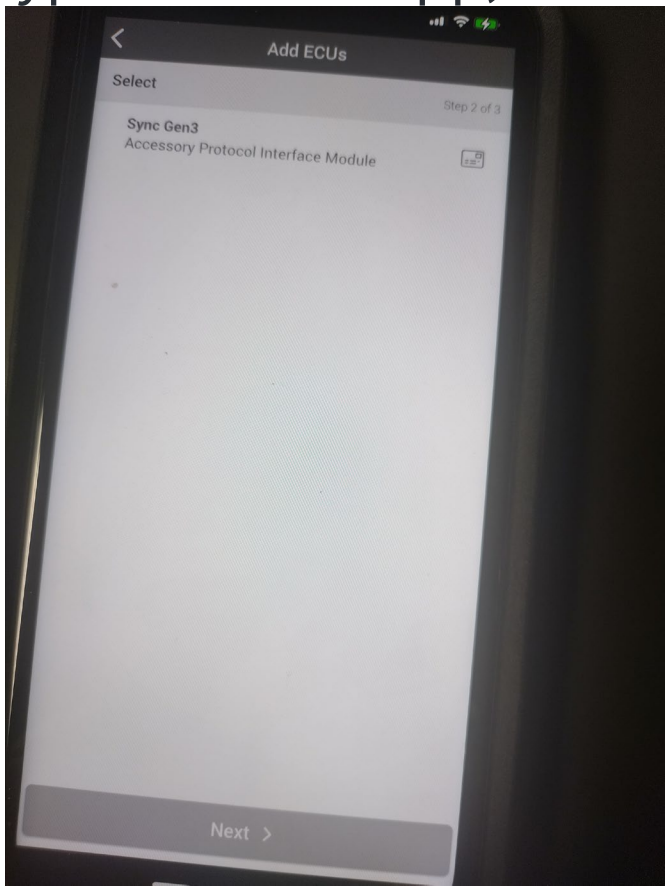
LET'S WORK A PRACTICE CASE:

- It allows me to add the electronic control unit info automatically or manually. I'll do the manual way:



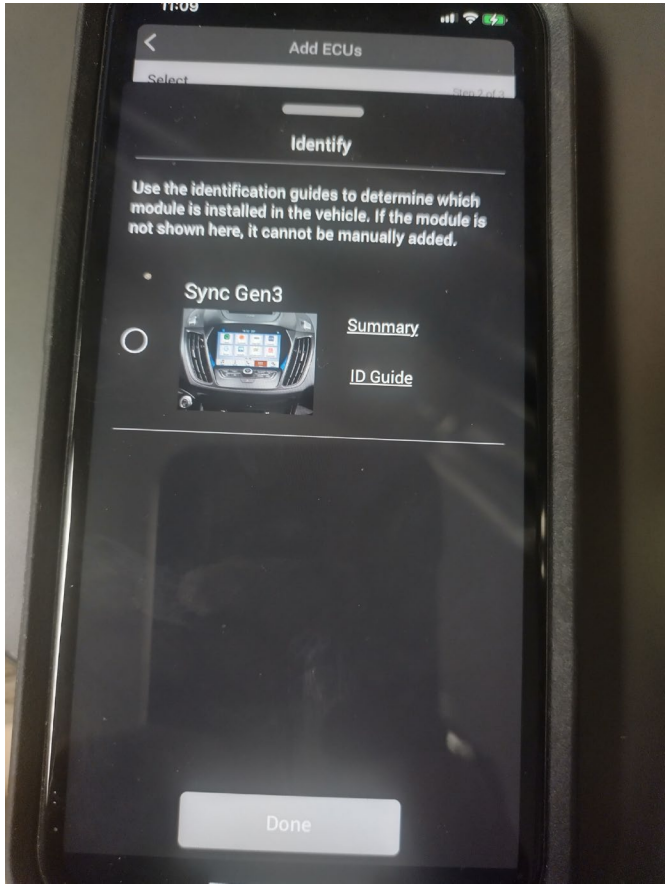
LET’S WORK A PRACTICE CASE:

- Based on the make, model, trin and vin # typed into the app, it is telling me that I will be working on a Ford Sync Gen3 ECU.



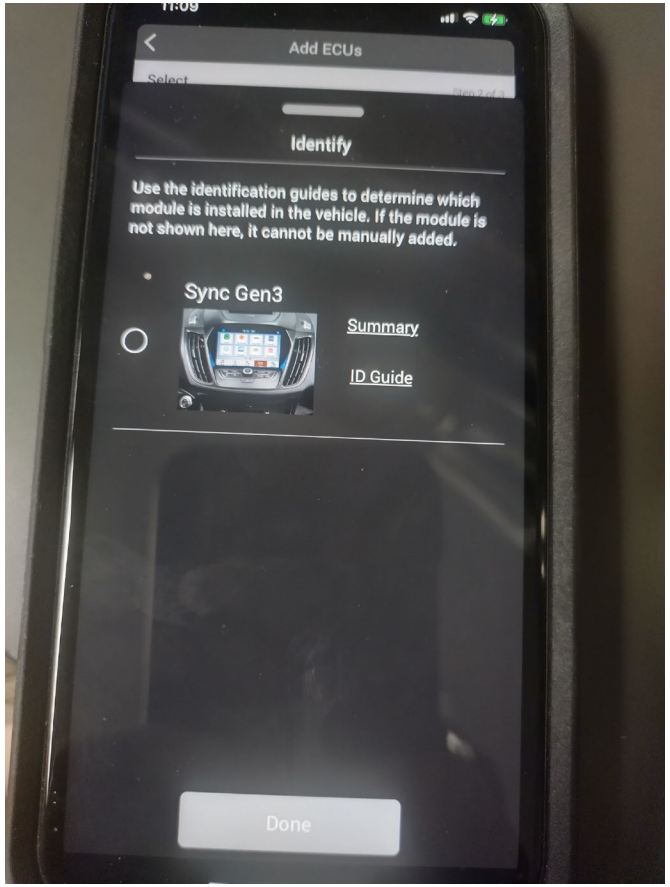
LET'S WORK A PRACTICE CASE:

- The ECU can be verified with the center console photo provided in the Berla app. Sometimes, the vehicle will need to be powered on and you may need to go into the console menu to obtain console version information.



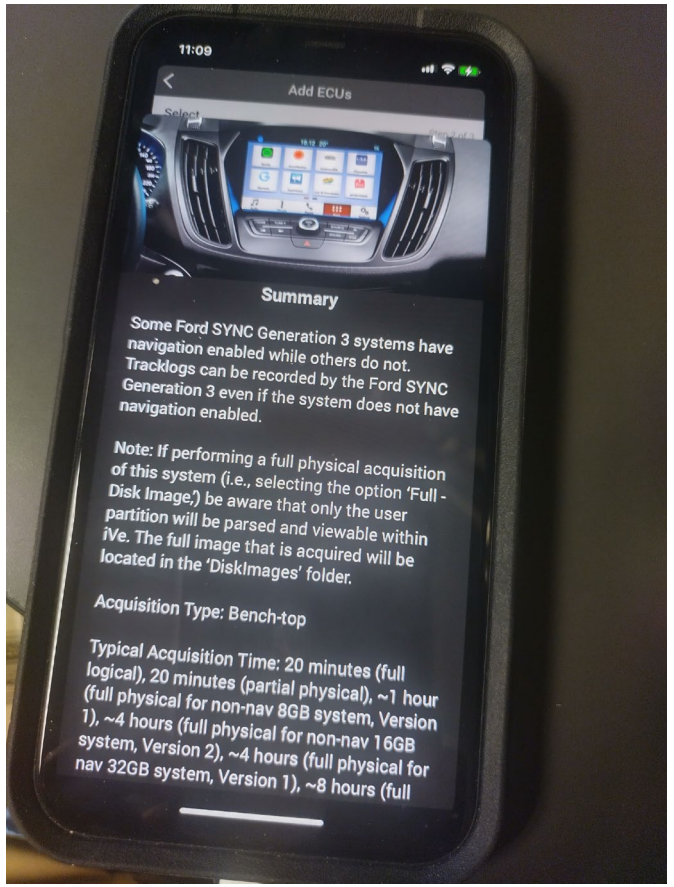
LET'S WORK A PRACTICE CASE:

- Even if the app says the vehicle is not supported, it is a good idea to contact Berla customer support to verify this information. There be an update soon to come out or the data might be able to be obtained via a chip off.



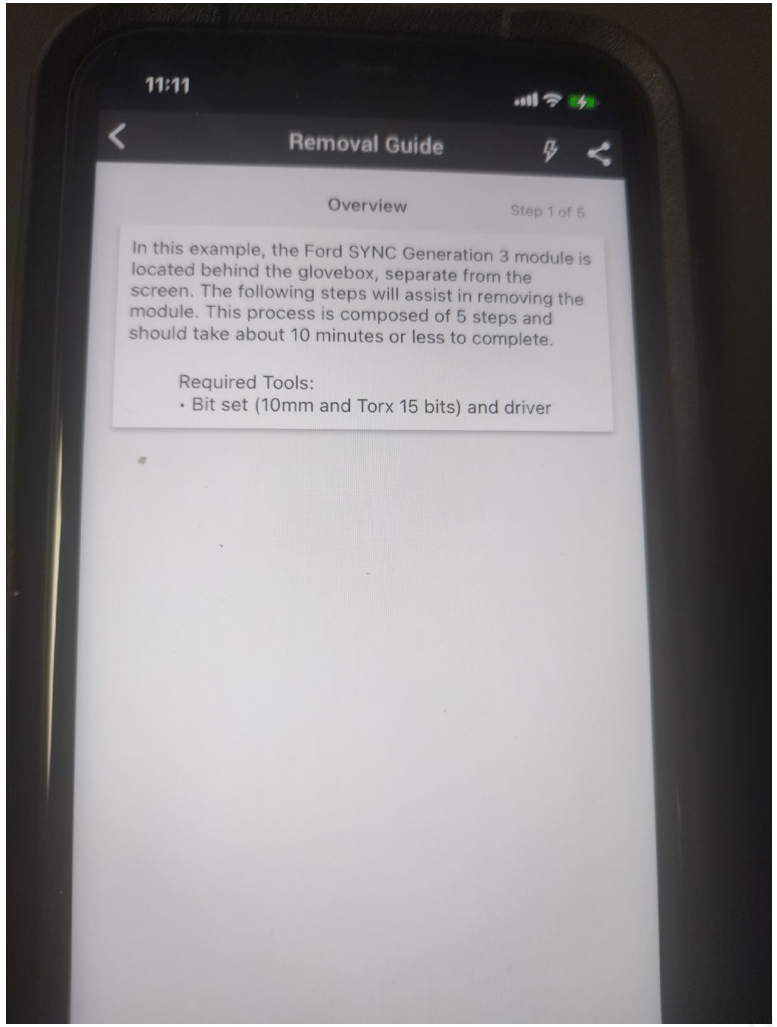
LET'S WORK A PRACTICE CASE:

- The Berla app will tell you what data is potentially available and how long the acquisition might take. It shows this vehicle may take over 4 hours and it did!



LET'S WORK A PRACTICE CASE:

- The Berla app will then tell you where the module is located and what tools you will need. You will need a wrench and bit kit. There are pry tools included in the Berla hardware kit. You'll need these to pry apart the vehicle interior.



LET'S WORK A PRACTICE CASE:

- Also, you will need a telescoping magnetic pickup pole. I dropped quite bits/nuts. This can be an issue if they fall down into the engine area. I almost had that happen when I loosened the battery connectors. So be careful!

Next up is the vehicle interior, pried apart!

LET’S WORK A PRACTICE CASE:

LET'S WORK A PRACTICE CASE:

- This is the area we need to get into!

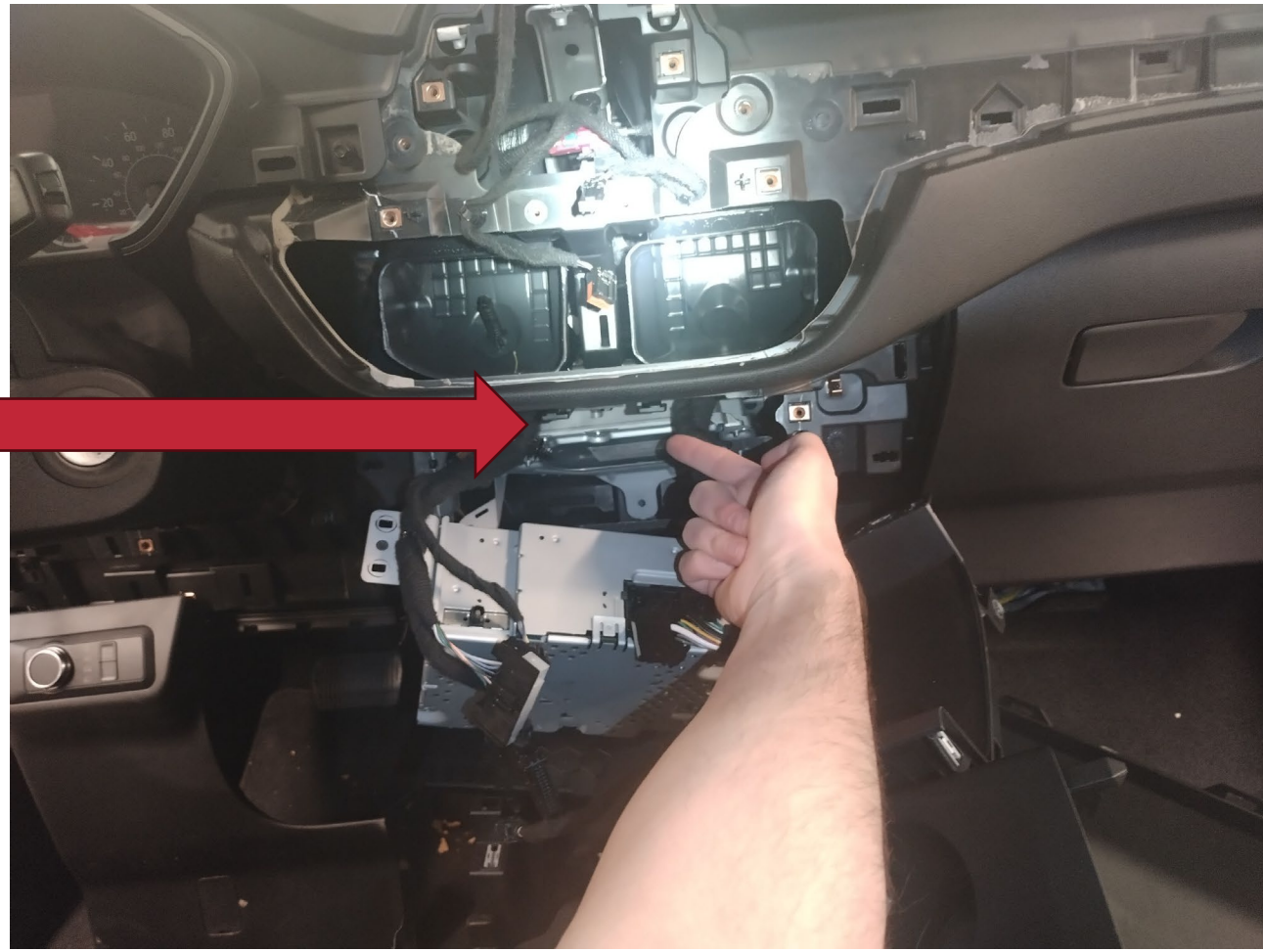
Behind this is the module.

We'll need to get this piece out of the way.

LET'S WORK A PRACTICE CASE:

- With that metal piece removed,

we can see the module!

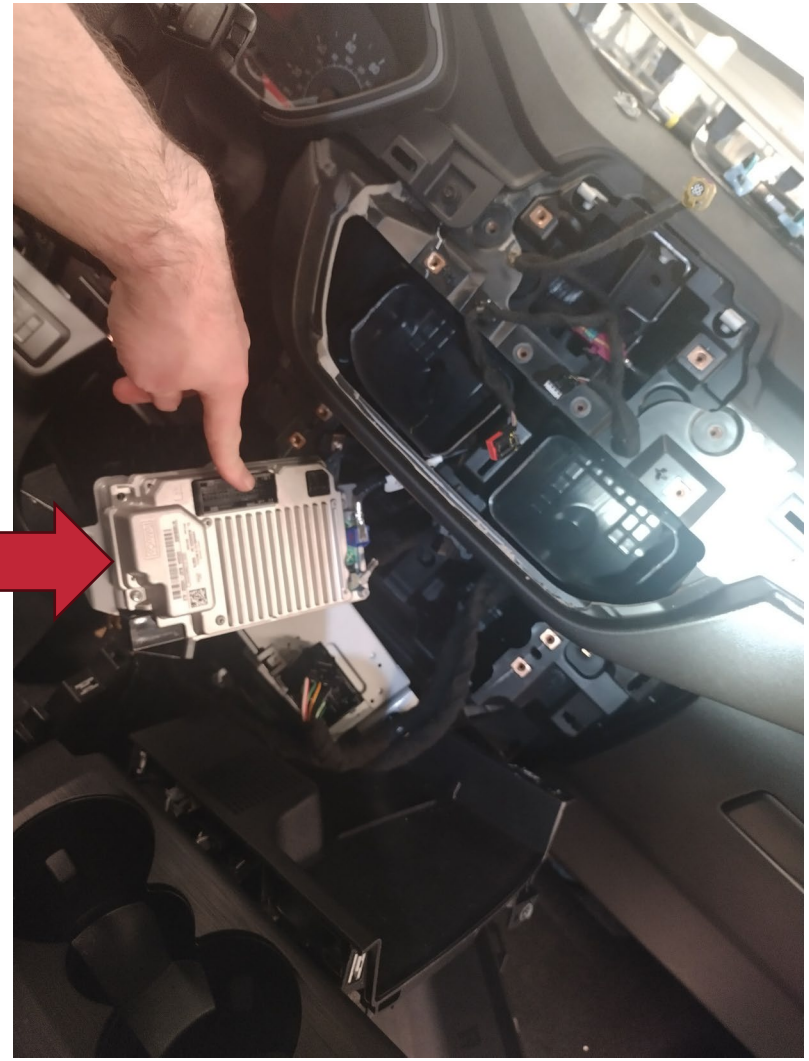


LET'S WORK A PRACTICE CASE:

- We then pull the module out and disconnect its connectors.

It was a pain, literally and figuratively!

The app removal instructions are not always perfect.



LET'S WORK A PRACTICE CASE:

- Once it is out, this is what it looks like:

- This becomes the piece of evidence we seize and take to the lab.

LET'S WORK A PRACTICE CASE:

- Here is what the module circuit board looks like out of the housing.
- The board I am working on is on the right.
- The Berla app provides removal instructions for the board and how to connect to it.
- This is done in the lab.

LET'S WORK A PRACTICE CASE:

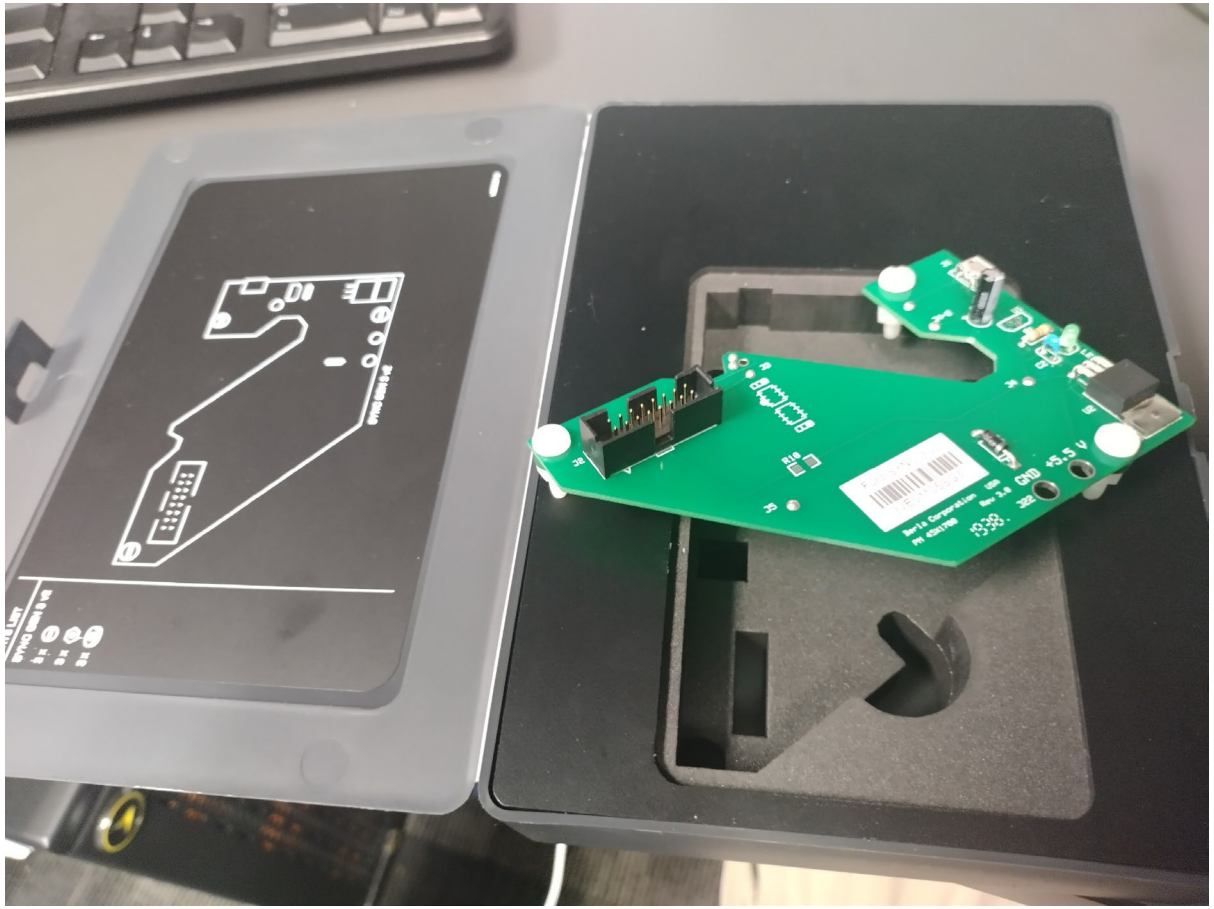
- The Berla hardware kit comes with a a connecting circuit board called a DIB. (Device interface board).
- The kit has several dibs for different types of vehicles.
- There are three types of dibs for Ford vehicles alone!

LET’S WORK A PRACTICE CASE:

- For this practice case, we are going to use the Ford Sync Gen 3 Version 2 dib.

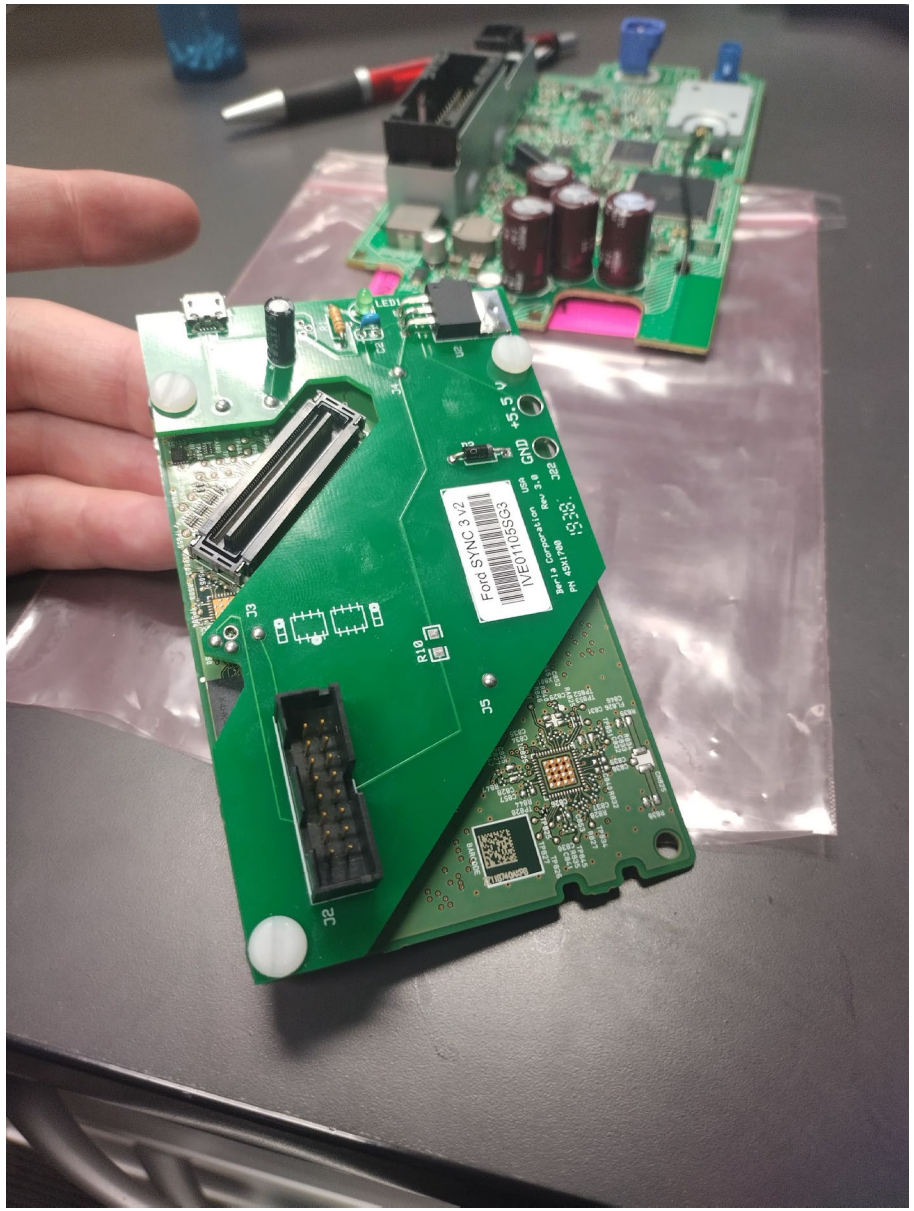
LET'S WORK A PRACTICE CASE:

- Notice the white plastic pieces on the sides. These are screws and nuts that you place between the vehicle module circuit board and dib to connect to each other.
- Sometimes you even have to rub off suader on the vehicle board to have an open electrical connection. The software will prompt you to test the connection.



LET’S WORK A PRACTICE CASE:

- Here is what it looks like when the two boards are connected.



LET’S WORK A PRACTICE CASE:

- We now have to power on the dib which is done through this cable and little black box supplied by Berla.

LET’S WORK A PRACTICE CASE:

- From the black box you hook up

This connector (basically an ethernet connector that goes to USB).

LET’S WORK A PRACTICE CASE:

- From there you can connect your USB connector to your computer where the Berla software extracts the data and it can be analyzed.
- There is a dongle that is needed In order to run the software.

LET'S WORK A PRACTICE CASE:

- When the Berla software can't parse the data, the chip from the board may need to come off the module board where the raw data can be obtained. This is known as a chip off.

Photo of SFM chip off equipment:

LET’S WORK A PRACTICE CASE:

- This should be done as a last resort since the module will be rendered useless if the chip is removed.
- Also, you will still need to know how to interpret that raw data in a hex viewer.
- Berla recently started doing classes on chip-offs.

LET'S WORK A PRACTICE CASE:

- Vehicle forensic analysis can make or break an investigation.
- SFM investigators have been able to track an arsonist's vehicle movements and find fires around where the vehicle has been.
- The fun part is having to put the vehicle back together!

QUESTIONS?

COM.OHIO.GOV

Forensic Lab “Laborghini”

Department of Commerce
Division of State Fire Marshal