Vehicle Forensics

Digital Evidence from Infotainment Systems

GENIVI Virtual AMM

October 2020

D/F/Lt. Jim Ellis

Michigan State Police
MSP Cyber Overview – Office Locations

Lansing
Livonia
Bridgeport
Coldwater
Grand Rapids
Traverse City
Marquette
Topics

• Infotainment & Telematics
• Recoverable Evidence
  • Vehicle Events
  • Driver Events
• Methods of Acquisition
• Case Examples
• Summary
Event Data Recorder - EDR

The Original Black Box
Infotainment Systems

Entertainment & Information Systems for Vehicle Occupants
Telematic Systems
Telecommunications & Informatics
Vehicle Tracking, Fleet Management, and More
What Data can be Extracted – Vehicle Events

- Vehicle Events – sampling*
  - Doors Opening/Closing
  - Acceleration/Deacceleration
  - Odometer Readings
  - Ignition Cycles
  - Speed Logs
  - Gear Shifts
  - Braking
  - Seat Belts
  - Cruise Control Usage
  - Wipers/Headlights On/Off
  - Passenger Air Bag Status On/Off

*Logged Events are dependent on Vehicle Year, Make, Model, Options
What Data can be Extracted – **Driver Events**

- Driver Events
- Connected Devices
- Call Logs
- Location & Navigation Data
- Emails
- SMS/MMS Messages
- Photos
- Social Media Data
- Contact Lists
- Bluetooth Connections
- WiFi Connections
Data (Evidence) Retrieval

- Software/Hardware capable of interrogating “The Box”
- Retrieval of Infotainment and Telematic system data
- Extraction and Analysis Tools
  - Non-Invasive
  - Invasive
  - Destructive
- Often Key Evidence or Only Evidence
- Patterns of Life
Advanced Retrieval Methods

- JTAG
- ISP
- Chip-Off
JTAG TAPS

• Circuit Board Ports or Test Access Ports (TAPS)
• Communicate w/processor and memory
ISP Example
CHIP-OFF

• Heat
CHIP-OFF

• Milling
Forensic Case Examples

• West Michigan Crime Spree – 2012 Ford, No Initial Evidence
• Submerged Device Found – 14 months
• Arson – Ford Navigation, 2010 Lincoln
• Motor Vehicle Theft – Ford Sync Gen 2, 2013 Ford F-150
• Missing/Homicide – Ford Sync Gen 3, 2018 Ford Escape
• Homicide – GM HMI, 2016 Chevy Silverado
• VCSA - Ford Sync Gen 3, 2019 Ford F-150
Summary

**Vehicle Events**
- Doors Opening/Closing
- Acceleration/Deacceleration
- Odometer Readings
- Ignition Cycles
- Speed Logs
- Gear Shifts
- Braking
- Seat Belts
- Cruise Control Usage
- Wipers/Headlights On/Off
- Passenger Air Bag Status On/Off

**Driver Events**
- Connected Devices
- Call Logs
- Location & Navigation Data
- Emails
- SMS/MMS Messages
- Photos
- Audio Commands
- Social Media Data
- Contact Lists
- Bluetooth Connections
- WiFi Connections
Questions?

D/F/Lt. Jim Ellis
MSP Cyber
EllisJ3@michigan.gov
Main 1-877-MI-CYBER