



Michigan State Police

# ***Vehicle Forensics***

## ***Digital Evidence from Infotainment Systems***

GENIVI Virtual AMM

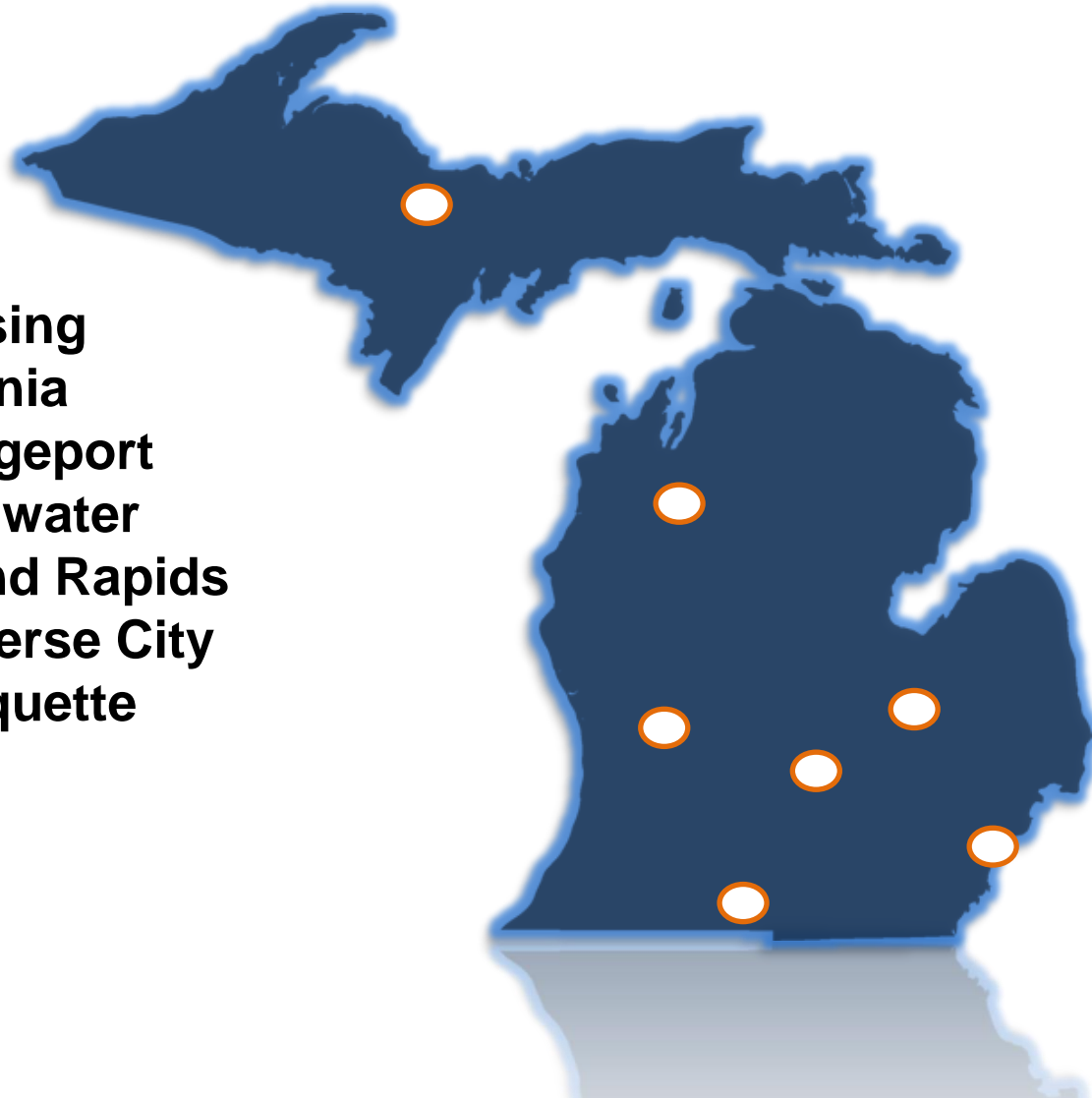
October 2020

D/F/Lt. Jim Ellis

Michigan State Police

# MSP Cyber Overview – Office Locations

Lansing  
Livonia  
Bridgeport  
Coldwater  
Grand Rapids  
Traverse City  
Marquette

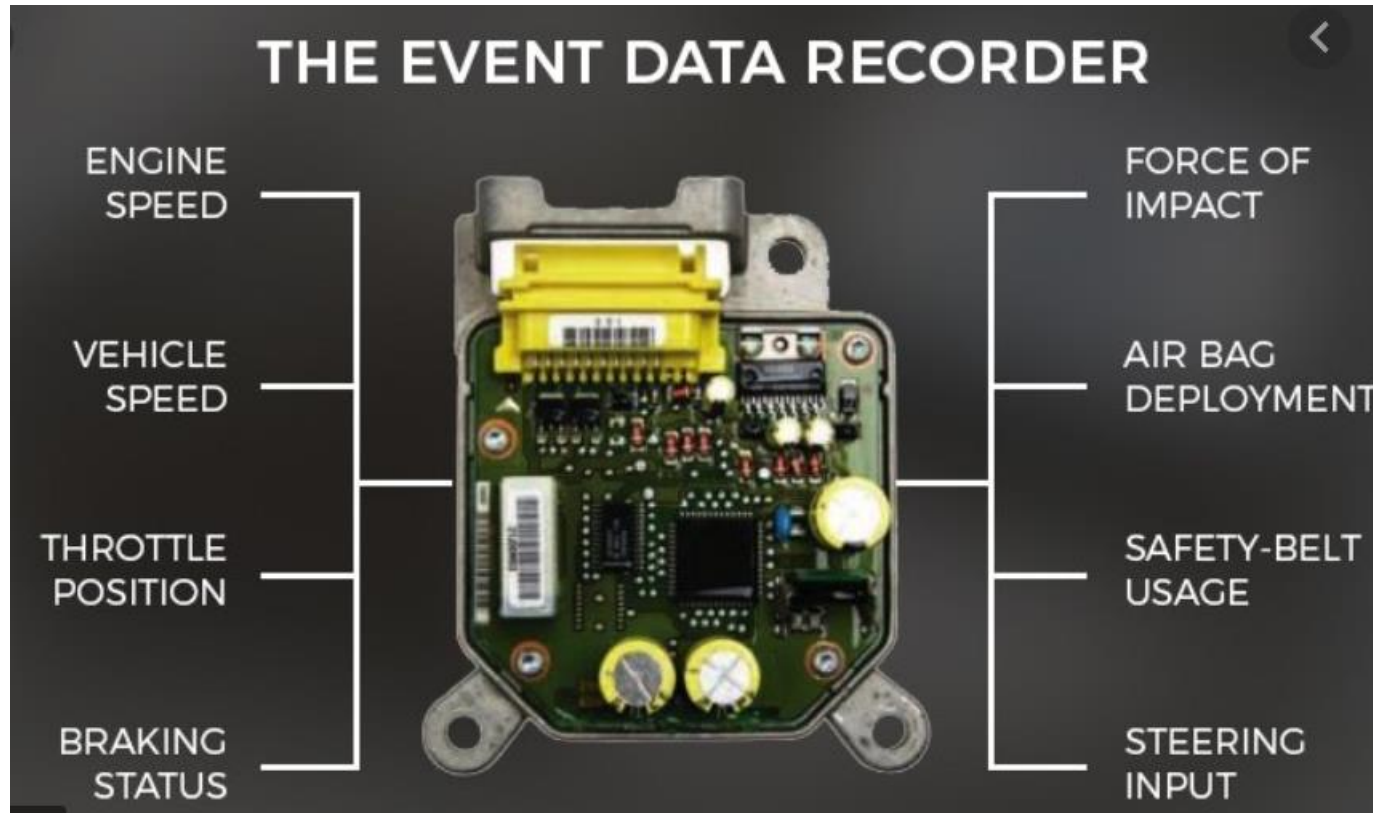


# Topics

- Infotainment & Telematics
- Recoverable Evidence
  - Vehicle Events
  - Driver Events
- Methods of Acquisition
- Case Examples
- Summary



# Event Data Recorder - EDR



The Original Black Box



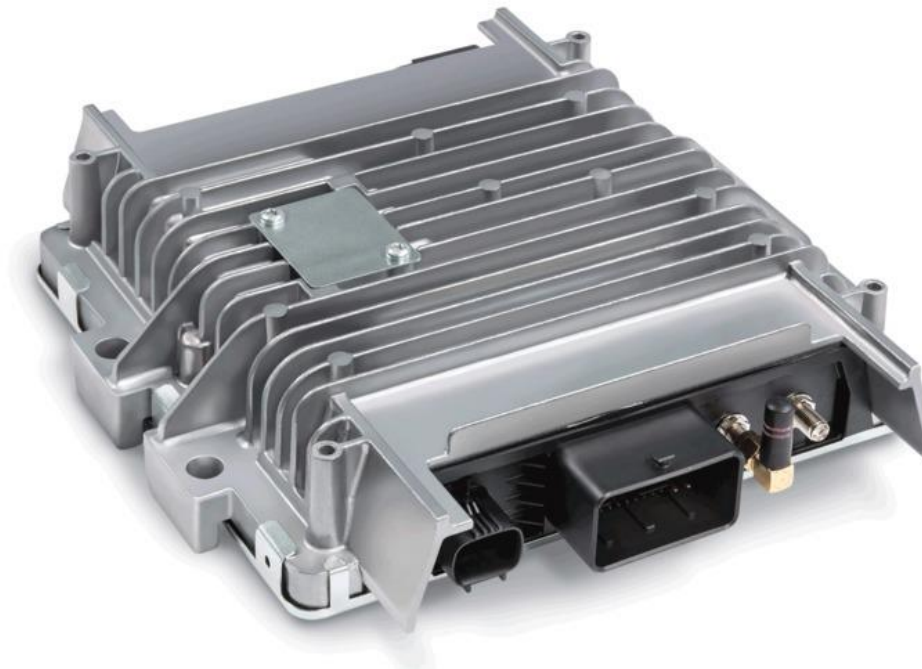
# Infotainment Systems

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

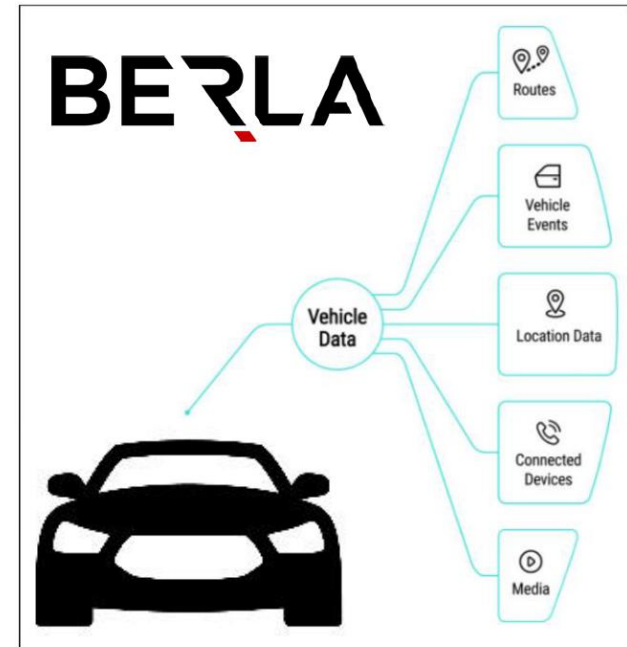


Image Source: [berla.co](http://berla.co)

*\* 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

The screenshot displays the iVe - Infotainment & Vehicle System Forensics software interface. The left pane shows a tree view of content categories, with 'Track Logs (27)' selected under the 'Navigation' folder. The main grid lists various LogicalTrack events with columns for Map, Name, Count, Flags, and Start Time. Below the grid is a map showing the acquired geo-referenced data as a blue route with green markers, covering the area around Odenton and Crofton, Maryland.

Map	Name	Count	Flags	Start Time
<input checked="" type="checkbox"/>	LogicalTrack0017 SatTS	26	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0018 SatTS	9	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0019	10	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0020	94	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0021	68	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0022	1	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0023 SatTS	69	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0025	1	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0027	1	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0029	1	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0031	34	None	04/28/2014
<input checked="" type="checkbox"/>	LogicalTrack0032 SatTS	265	None	04/28/2014





# 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



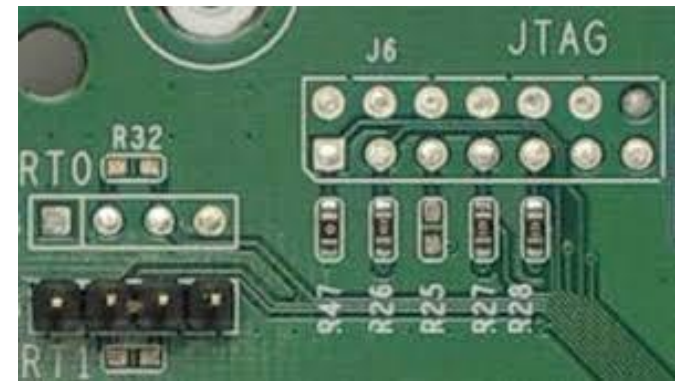
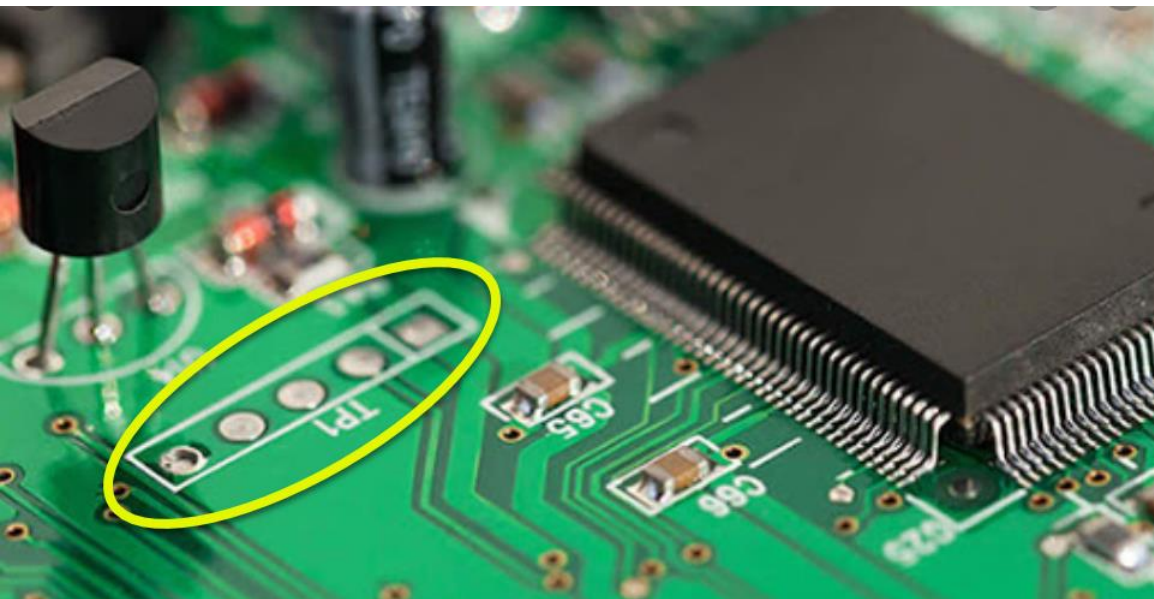
# Advanced Retrieval Methods

- JTAG
- ISP
- Chip-Off

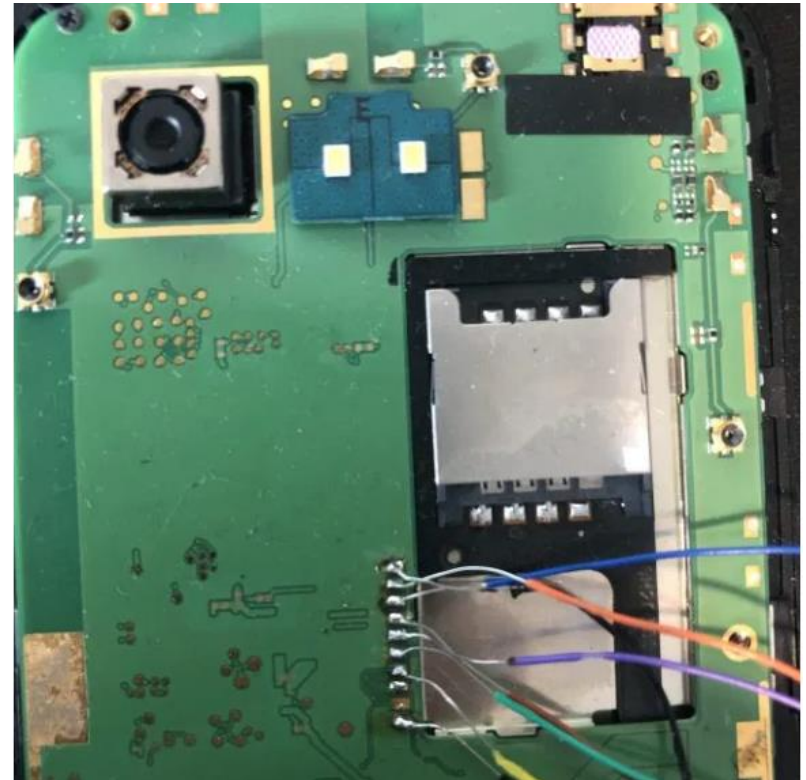
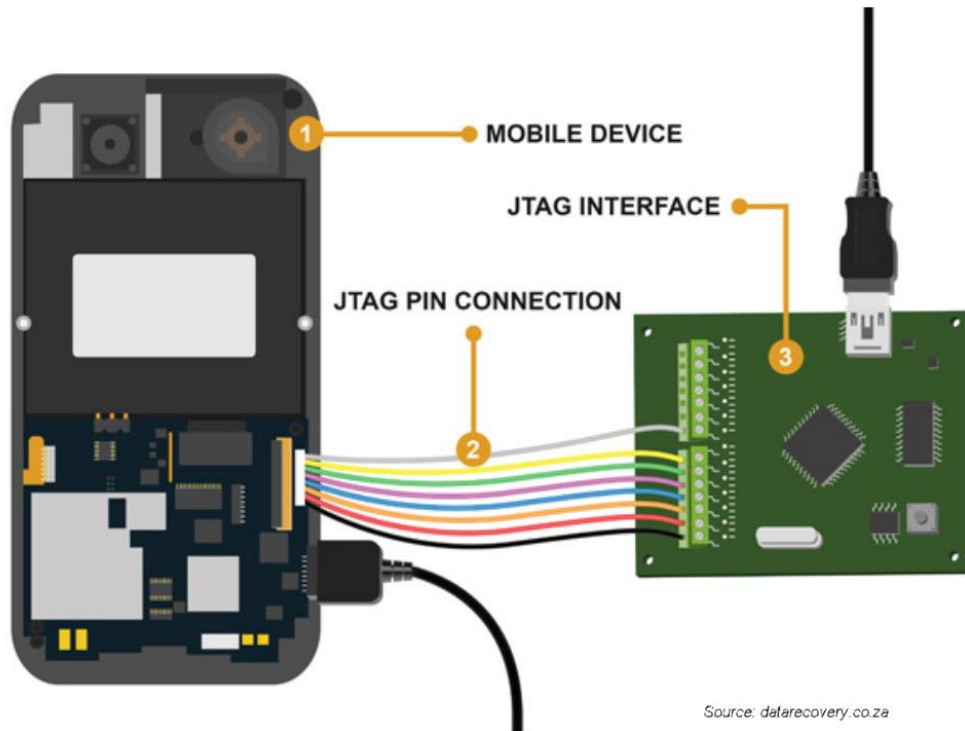


# JTAG TAPS

- Circuit Board Ports or Test Access Ports (TAPS)
- Communicate w/processor and memory

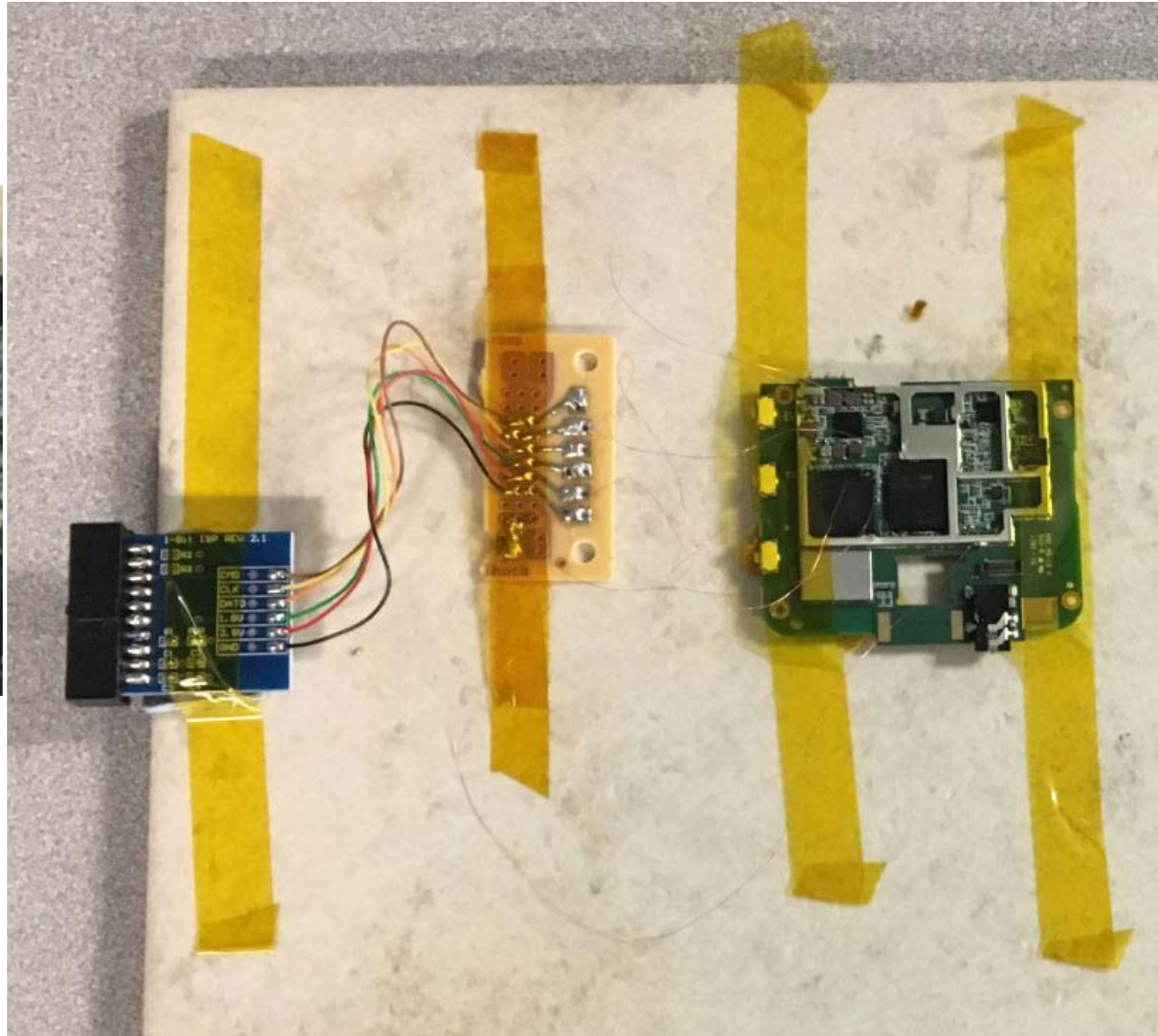
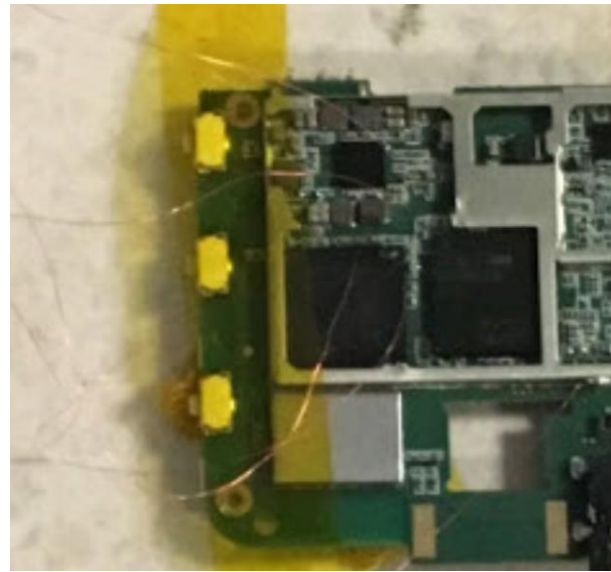


# JTAG Example

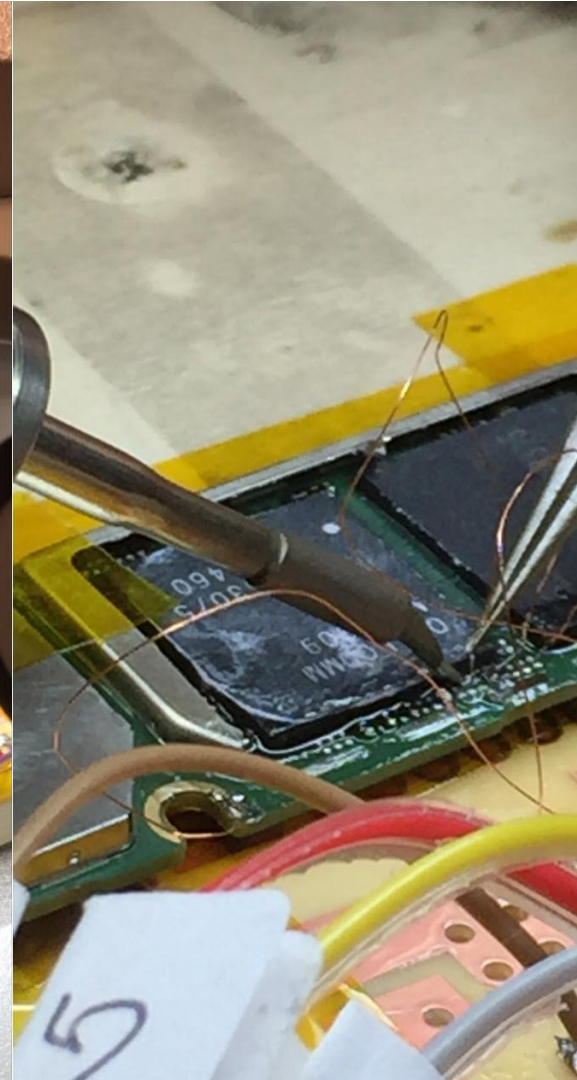
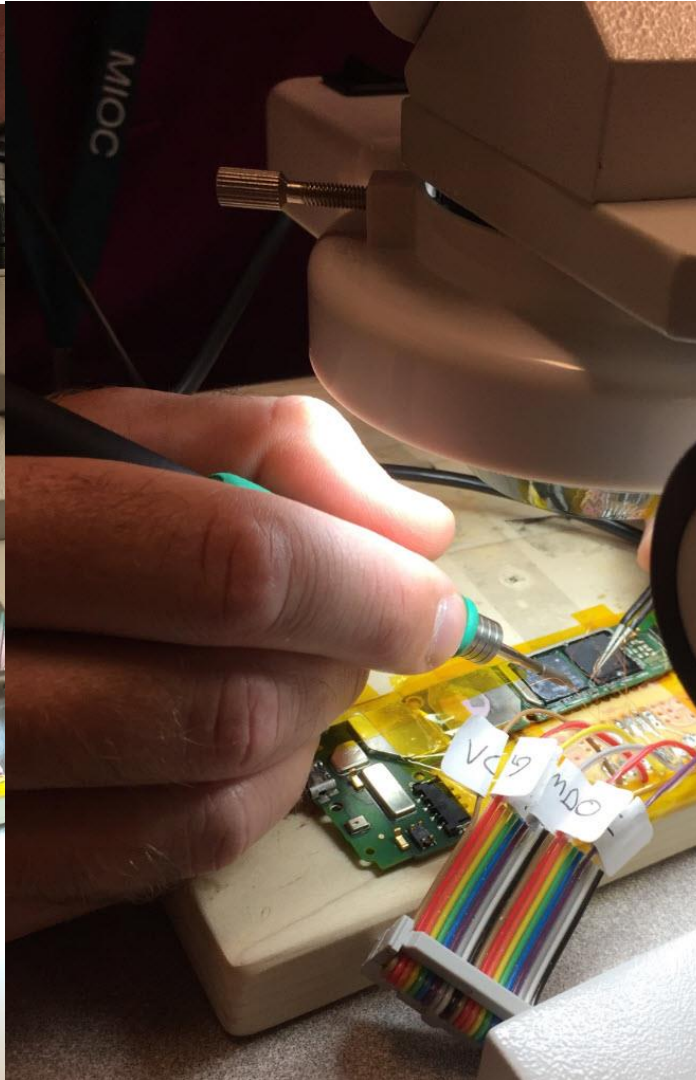
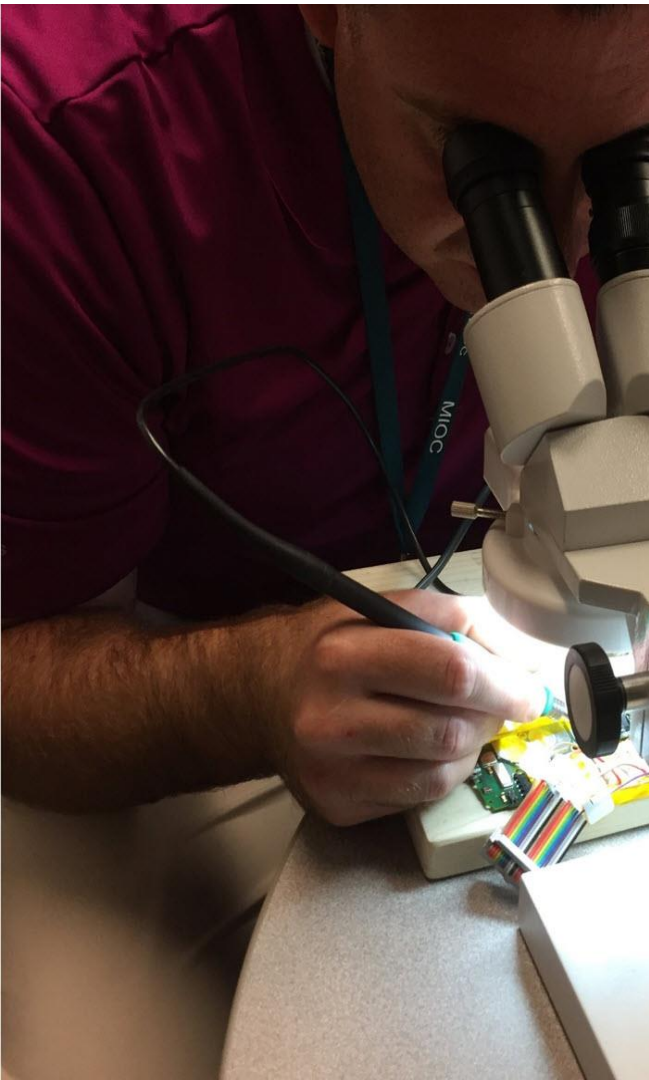




# ISP Example

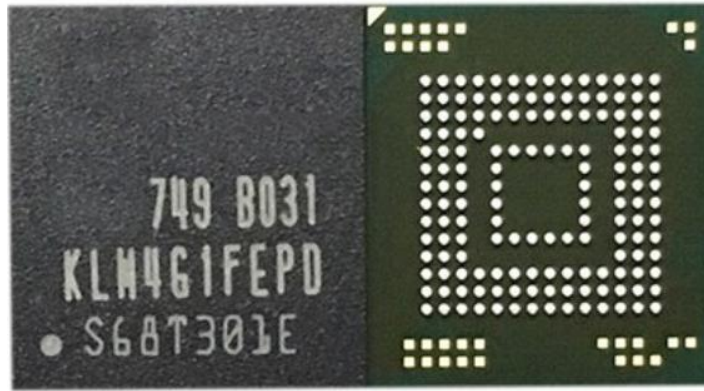


# ISP





# CHIP-OFF



# CHIP-OFF

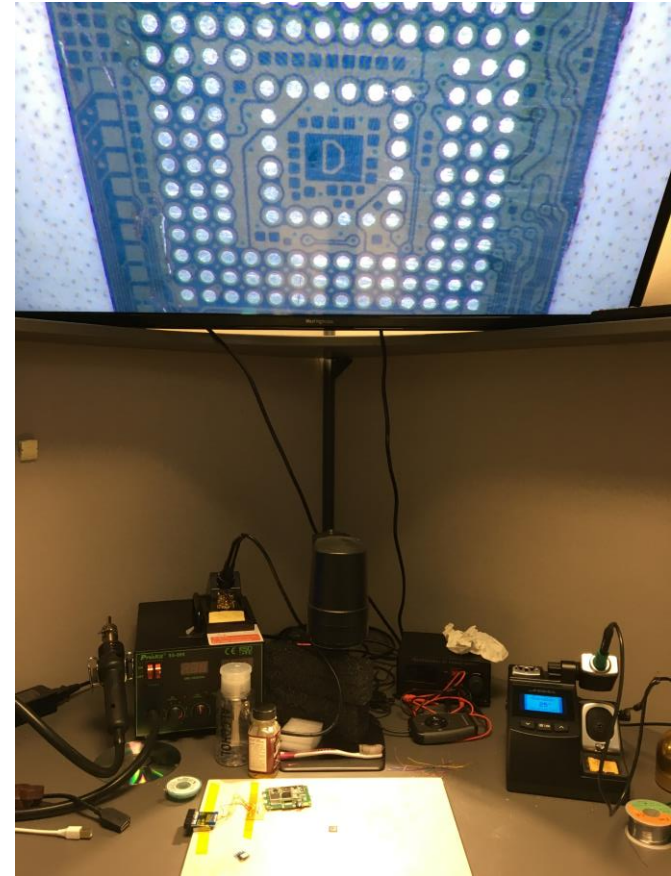
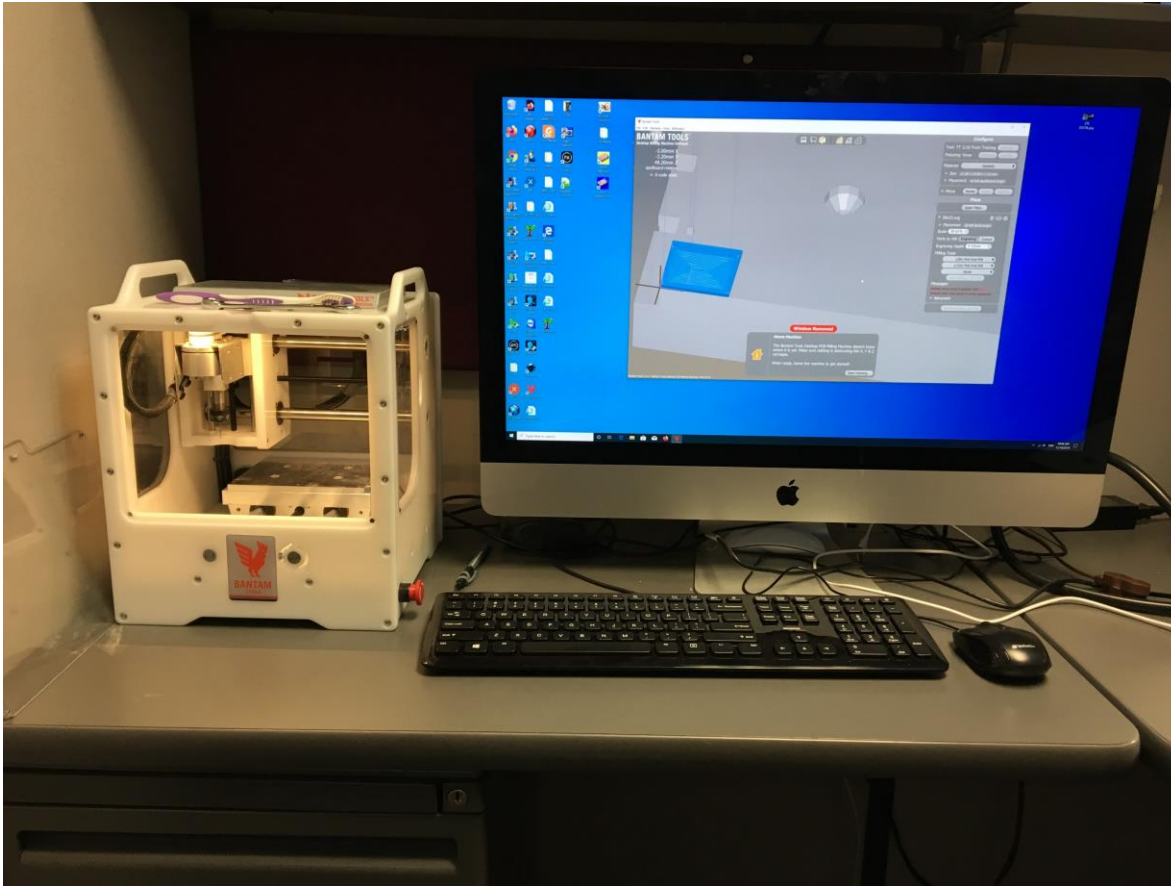
- Heat





# 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





# Michigan State Police

## Questions?

**D/F/Lt. Jim Ellis**

**MSP Cyber**

**[EllisJ3@michigan.gov](mailto:EllisJ3@michigan.gov)**

**Main 1-877-MI-CYBER**

[Michigan.gov/MSPCYBER](http://Michigan.gov/MSPCYBER)  
[MichiganICAC.com](http://MichiganICAC.com)  
[Michigan.gov/cybersecurity](http://Michigan.gov/cybersecurity)

Michigan Cyber Command Center (MC3)  
Computer Crimes Unit (CCU)  
Internet Crimes Against Children (ICAC)

