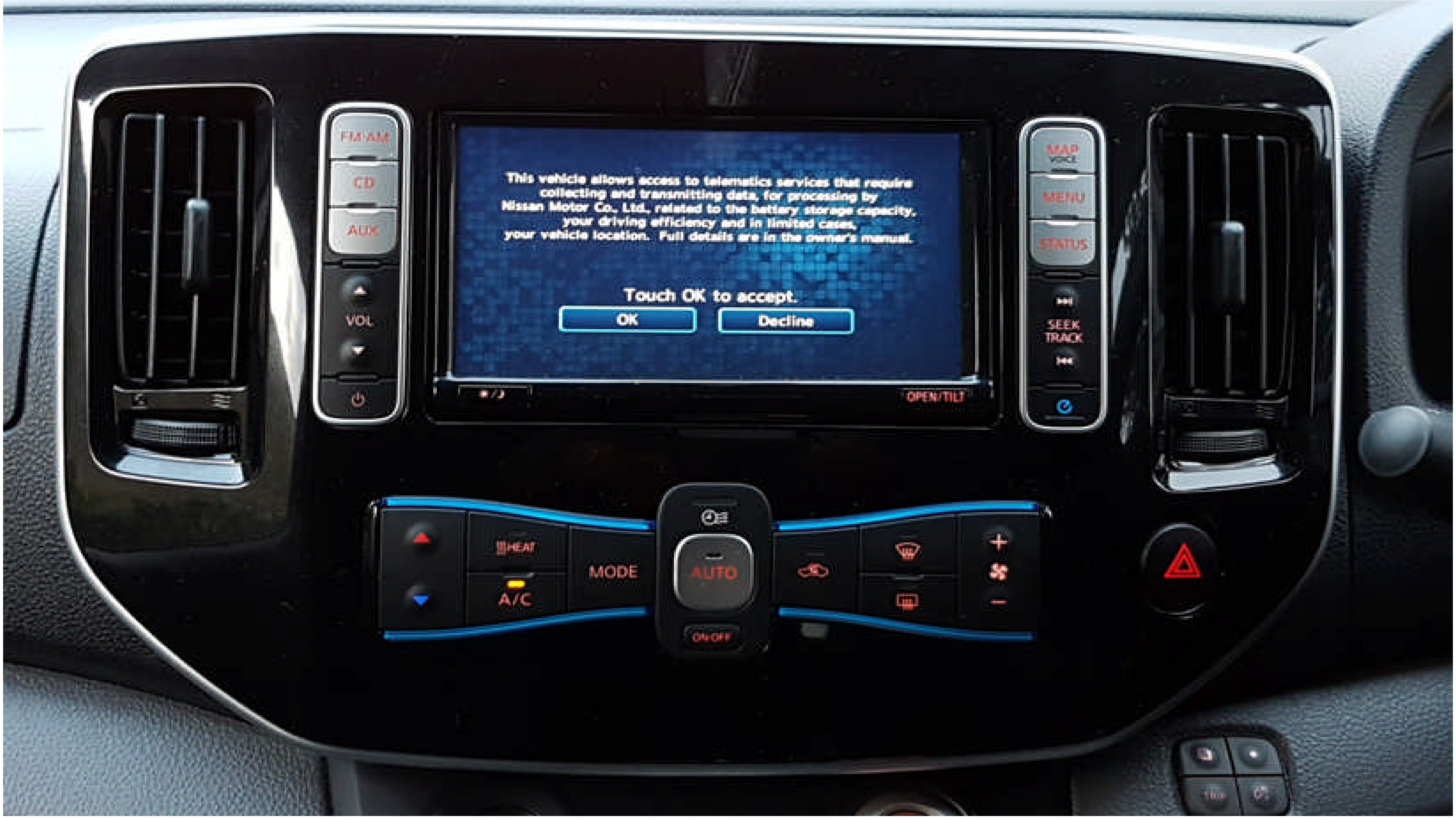


This vehicle allows access to telematics services that require
collecting and transmitting data, for processing by
Nissan Motor Co., Ltd., related to the battery storage capacity,
your driving efficiency and in limited cases,
your vehicle location. Full details are in the owner's manual.

Touch OK to accept.

PRIVACY IMPLICATIONS OF INTELLIGENT TRANSPORT SYSTEMS

Khalil El-Khatib
Rajen Akalu
Kushal Jaisingh

THE JOURNEY

- Technology is rapidly advancing in the transport sector

TODAY'S CONNECTED VEHICLES

- Modern vehicles
  - More than 50 networked computers:
    - Average new vehicle has 40 to 50 computers that run 20 million lines of software code, more than a Boeing 787 (KPMG)
  - Networks on wheels
- Infotainment and telematics systems generate, collect, and transmit lots of data to provide on-board features for a safe and comfortable ride!!!
- Contains potentially sensitive information about driver!

TODAY’S CONNECTED VEHICLES

- New vehicles have many sensors and have multiple options to connect to other types of networks
- Gather and generate lots of data to provide on-board features to consumers
  - Contains potentially sensitive information about consumers
  - Remotely accessible by automakers and infotainment/telematics service providers

BACKGROUND – INFOTAINMENT SYSTEMS

- Contain non-vehicular information
- Provide drivers convenient onboard functions when driving:
  - Hands free calling
  - Text messaging
  - Emailing
  - …

BACKGROUND – TELEMATICS SYSTEMS

- Contain vehicular information about vehicle’s internal systems
- Primarily used for vehicle diagnostics and emergency situations to automatically provide roadside assistance service providers pertinent information

VEHICLE IDENTIFICATION DATA INCLUDES

- Vehicle identification number (VIN)
- Subscriber identify module card number (SIM)
- Internet protocol address (IP)
- Radio frequency identification serial number (RFID)
  - Many vehicles are equipped with RFID tags for toll collection, and can be linked to vehicle owners' billing account information for their toll usage
  - Some vehicle keys contain embedded RFID tags for convenience and personalization of drivers' seat settings

- Can be used to reveal the identity of the owner of the vehicle

PERSONAL INFORMATION

- Personal information is “information about an identifiable individual”
- Includes identification data, personal communications data, biometric and health data, location data, driver behavior data, and miscellaneous infotainment data
- Driver behavior data and miscellaneous infotainment data aren’t considered personal information, but certainly have implications on one’s privacy

PERSONAL COMMUNICATIONS DATA

- Includes:
  - Voice calls
  - Text messages
  - Emails
  - Social networking information

PERSONAL COMMUNICATIONS DATA - METADATA

- Each personal communication event’s data is accompanied by its corresponding metadata including:
  - Event’s date
  - Time
  - Origin
  - Destination
  - Duration
  - …

BIOMETRIC & HEALTH DATA

- Some vehicles contain biometric authentication and health monitoring devices
- Information retrieved from these devices can also reveal the identities of drivers

DRIVER BEHAVIOR DATA

- Includes information regarding drivers’ driving habits such as vehicle speed, acceleration, direction, braking, cornering, ignition, steering, seat belts, and door locking
- Alone cannot be used to identify individuals
- Combined with vehicle identification data, could have major privacy implications

VEHICLE LOCATION DATA

- Includes recently visited destinations as well routes travelled
- Alone may not be able to reveal identities of individuals
- Combined with other data sources, major privacy implications arise as intimate details of individuals' private lives are portrayed

MISCELLANEOUS INFOTAINMENT DATA

- Includes personal contacts, calendar/planner schedules, search history, recently viewed content (photos, audio, video, websites), and any other data which may be synced from mobile devices
- Reveals a lot about individuals’ personal lives
- Can be used for profiling individuals based on their social associations, interests, and content preferences

DATA USAGE IN INFOTAINMENT AND TELEMATICS SYSTEMS

- Live agent assistance, including:
  - Automatic collision notification emergency assistance
  - Roadside assistance

- Remote monitoring and control, including:
  - Remote vehicle diagnostics
  - Fleet management
    - Can monitor vehicle location and routes travelled in real time including vehicle speed and driving violations
  - Usage-Based Insurance (UBI)
  - Automotive financing

DATA USAGE IN INFOTAINMENT AND TELEMATICS SYSTEMS

- Geo-fencing
  - Used in fleet management and automotive financing applications to confine vehicles to a specific predefined geographic boundary
  - If vehicle roams out of its boundary, predefined actions are executed such as:
    - Notify fleet manager or financier of boundary breach
    - Remotely disable vehicle
- Location-based advertising, including:
  - Vehicle-to-Retail (V2R) location-based advertising communications are targeting drivers
  - GM's "AtYourService" feature allows their business partners to notify OnStar subscribers of special offers

DATA USAGE IN INFOTAINMENT AND TELEMATICS SYSTEMS

- Distance-based road taxation
  - Provides drivers the option to either pay a high flat rate for unlimited driving on toll roads
  - Or a lower rate based on the GPS data collected by a voluntary dongle or mobile app which monitors the distance travelled on the toll roads
- Electronic tolling
  - Relies on roadside RFID scanners and Automatic License Plate Readers (ALPRs)
  - Scans vehicles' RFID tags and license plates as they pass through entry and exit nodes of toll roads to determine the amount owed

DATA USAGE IN INFOTAINMENT AND TELEMATICS SYSTEMS:

- Personal Connectedness and Infotainment, including:
  - Include hands-free communications via voice commands for drivers to safely engage in communications
  - Contacts, calendar data, and other information is automatically synced to the vehicle to provide infotainment services

THIRD PARTY INTERESTS

- Infotainment/telematics data has become a very hot commodity
- Many people are interested in purchasing this data for the valuable insights it can provide using data analytics

THIRD PARTY INTERESTS - TOMTOM

- TomTom was caught selling customer GPS data to ____ _______ ________for creating speed traps
- Dutch law enforcement

POTENTIAL PRIVACY VIOLATION- FORD

- Ford’s Global VP of Marketing said:
  - “We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing”
- He later clarified his statement by saying:
  - “We do not track our customers in their cars without their approval or consent”
- Despite his clarification, automakers still have the ability to track their customers’ vehicles and mine sensitive information

POTENTIAL PRIVACY VIOLATION – GM'S ONSTAR

- GM's OnStar service provides directions, roadside assistance, and concierge services to its subscribers
- Recently, GM added their new AtYourService feature to their existing OnStar service offerings

LET US FIND OURSELVES WHAT IS ON THESE SYSTEMS

- What is stored on these systems and how can it be used to determine information about its users?

TARGET SYSTEMS

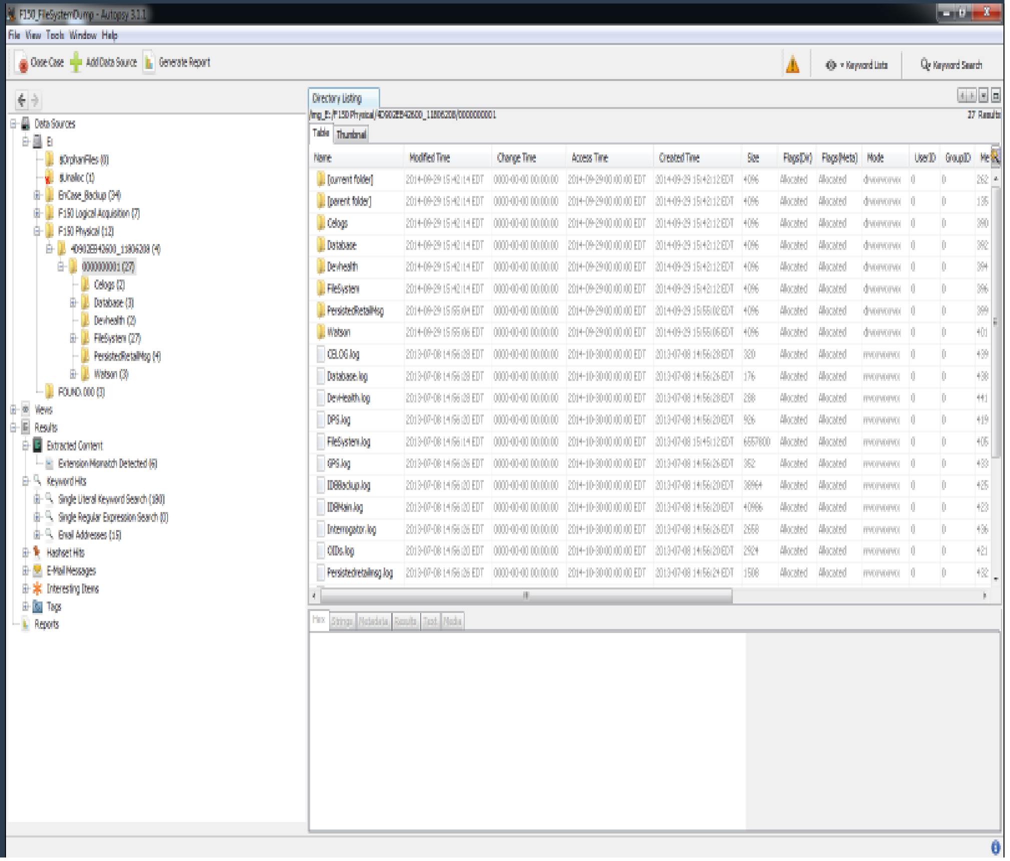
- Many car manufacturers
- Many different platforms: Ford SYNC, Dodge uConnect, GMC/Chevrolet OnStar/MyLink, etc)
- Different generations among same branded platforms (e.g. SYNC Gen1, Gen2)
- Windows, Linux/Android, QNX based systems
- Aftermarket systems → same case as above (Android more popular)

DATA ACQUISITION PROCESS

- Not as straightforward as initially thought…especially car manufacturer
- Not everyone is willing to let us take their vehicle apart for one main component
- Original Equipment Manufacturers (OEMs) are complicated to power up standalone but represent majority of market

FORD F150 TRUCK

- Based off this first dump, lots of relevant information stored!
- Logs upon logs upon logs
- GPS breadcrumbs
- Phonebook folder
- Web browsing folder (nothing in it but feature might not of been used)
- Etc.



```
Data Sources
  E:
    $OrphanFiles (0)
    $Unalloc (1)
    EnCase_Backup (34)
    F150 Logical Acquisition (7)
    F150 Physical (12)
      409028E42600_11806208 (4)
        0000000001 (27)
          Celogs (2)
          Database (3)
          Devhealth (2)
          FileSystem (27)
          PersistedRetailMsg (4)
          Watson (3)
    FOUND.000 (3)
Views
Results
  Extracted Content
    Extension Mismatch Detected (6)
  Keyword Hits
    Single Literal Keyword Search (180)
    Single Regular Expression Search (0)
    Email Addresses (15)
  Hashset Hits
  E-Mail Messages
  Interesting Items
  Tags
Reports
```

/img_E:/F150 Physical/409028E42600_11806208/0000000001

27 Results

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	Me
[current folder]	2014-09-29 15:42:14 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:42:12 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	262
[parent folder]	2014-09-29 15:42:14 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:42:12 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	135
Celogs	2014-09-29 15:42:14 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:42:12 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	390
Database	2014-09-29 15:42:14 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:42:12 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	392
Devhealth	2014-09-29 15:42:14 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:42:12 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	394
FileSystem	2014-09-29 15:42:14 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:42:12 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	396
PersistedRetailMsg	2014-09-29 15:55:04 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:55:02 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	399
Watson	2014-09-29 15:55:06 EDT	0000-00-00 00:00:00	2014-09-29 00:00:00 EDT	2014-09-29 15:55:06 EDT	4096	Allocated	Allocated	d/drwxrwxrwx	0	0	401
CELOG.log	2013-07-08 14:56:28 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:28 EDT	320	Allocated	Allocated	r/rrwxrwxrwx	0	0	439
Database.log	2013-07-08 14:56:28 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:26 EDT	176	Allocated	Allocated	r/rrwxrwxrwx	0	0	438
DevHealth.log	2013-07-08 14:56:28 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:28 EDT	288	Allocated	Allocated	r/rrwxrwxrwx	0	0	441
DPS.log	2013-07-08 14:56:20 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:20 EDT	926	Allocated	Allocated	r/rrwxrwxrwx	0	0	419
FileSystem.log	2013-07-08 14:56:14 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 15:45:12 EDT	6557800	Allocated	Allocated	r/rrwxrwxrwx	0	0	405
GPS.log	2013-07-08 14:56:26 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:26 EDT	352	Allocated	Allocated	r/rrwxrwxrwx	0	0	433
IDBBackup.log	2013-07-08 14:56:20 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:20 EDT	38964	Allocated	Allocated	r/rrwxrwxrwx	0	0	425
IDBMain.log	2013-07-08 14:56:20 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:20 EDT	40966	Allocated	Allocated	r/rrwxrwxrwx	0	0	423
Interrogator.log	2013-07-08 14:56:26 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:26 EDT	2658	Allocated	Allocated	r/rrwxrwxrwx	0	0	436
OIDs.log	2013-07-08 14:56:20 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:20 EDT	2924	Allocated	Allocated	r/rrwxrwxrwx	0	0	421
Persistedretailmsg.log	2013-07-08 14:56:26 EDT	0000-00-00 00:00:00	2014-10-30 00:00:00 EDT	2013-07-08 14:56:24 EDT	1508	Allocated	Allocated	r/rrwxrwxrwx	0	0	432

MORE HARDWARE

- At this point, need to do more investigation
- Plan: acquire more infotainment systems
- Contacted junkyards and dealerships
- Turns out powering up the system standalone isn’t as straightforward as aftermarket systems… entire wire harnesses, vehicle fuse box and Body Control Module (BCM) needed
- Process of acquiring and wiring up one Ford SYNC platform took almost a moth (trial and error and finding out components were missing before it could work)

CF397
CD
RADIO
SIRIUS
AUX
PHONE
OK
INFO
MENU
ON/OFF
PASS
AIRBAG
OFF

Alright, now that we have some hardware, how are we extracting the data??!?

BERLA IVE

- iVe (forensic software specifically for OEMs used in conjunction with hardware extraction)
- Supports BMW, Buick, Cadillac, Chevrolet, Chrysler, Dodge, FIAT, Ford, GMC, HUMMER, Jeep, Lincoln, Maserati, Mercury, Pontiac, Ram, SRT, Saturn, and Toyota (generally 2008 and up)
- Only one problem… licence is ridiculously expensive

IN THE MEANTIME…

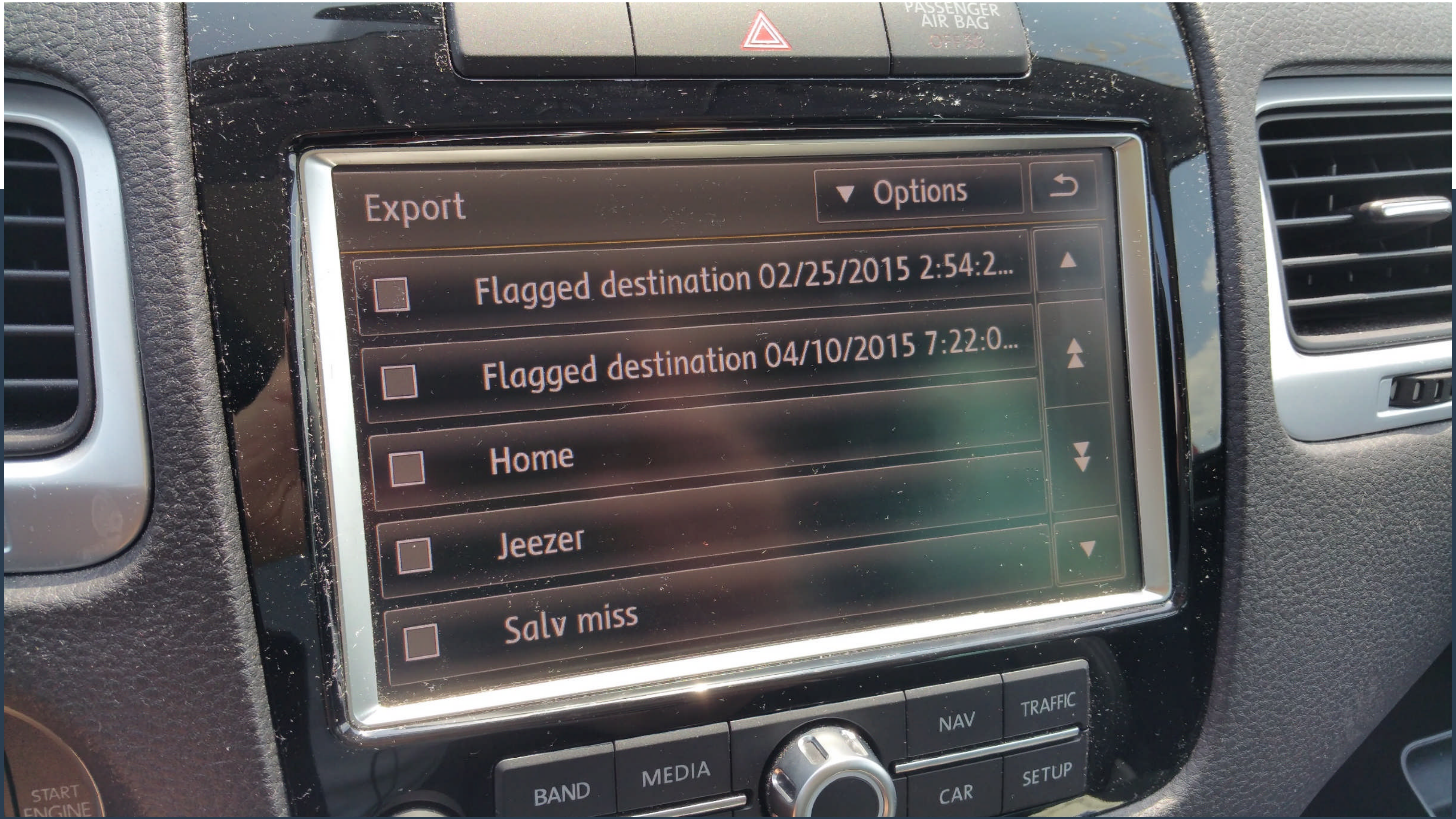
- Curious about what could be found on vehicles through simple user interactions
- OWASCO Volkswagen/Audi dealership willing to helps us with second hand vehicles on lot
- Are users aware of what they could be leaving behind?

VEHICLES

- 2013 VW Passat (no GPS, just basic infotainment)
- 2014 VW Touareg (higher end infotainment with GPS)
- 2012 Audi Q5 (higher end infotainment with GPS)
- 2014 Audi Q7 (higher end infotainment with GPS)

OBSERVATIONS

- Bluetooth device lists (profiles)
- Phone contacts
- Profile information (name, device info, # of imported contacts)
- Navigation info and addresses still stored including exact coordinates
- Can export contacts/GPS information to SD/USB (any that were imported, depending on system)



Export

▼ Options

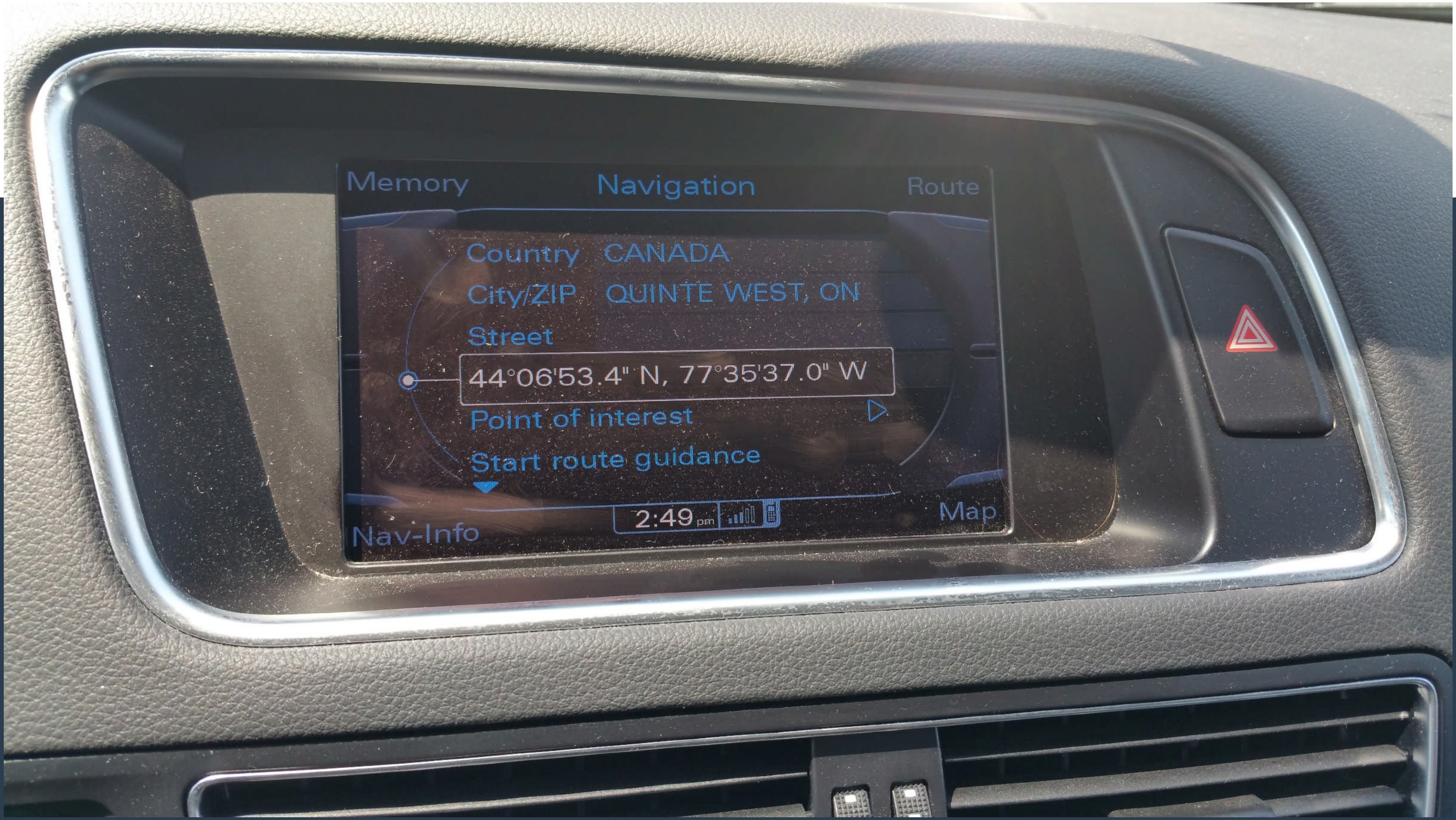
□ Flagged destination 02/25/2015 2:54:2...

□ Flagged destination 04/10/2015 7:22:0...

□ Home

□ Jeezer

□ Salv miss



Country CANADA

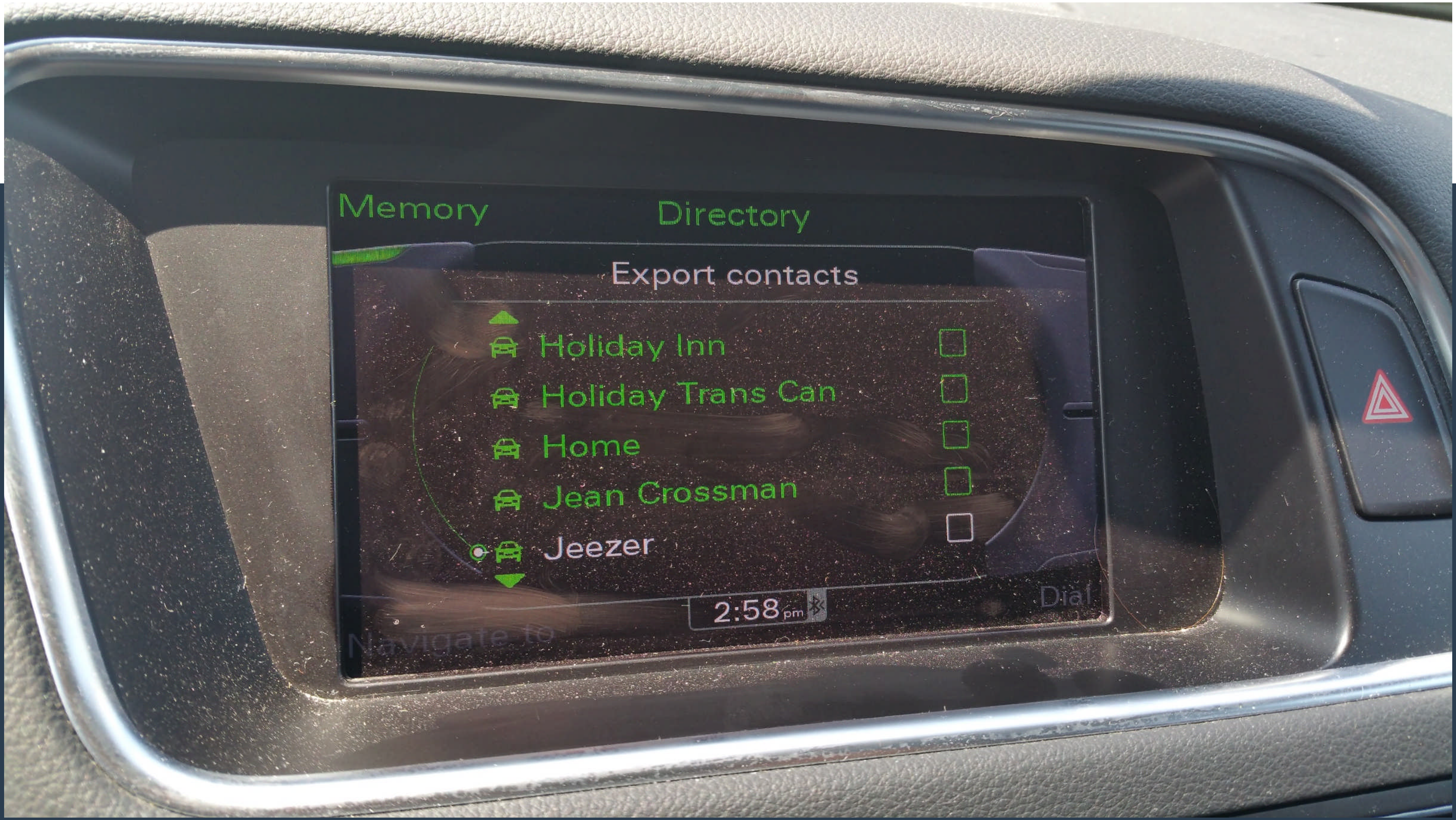
City/ZIP QUINTE WEST, ON

Street

44°06'53.4" N, 77°35'37.0" W

Point of interest

Start route guidance

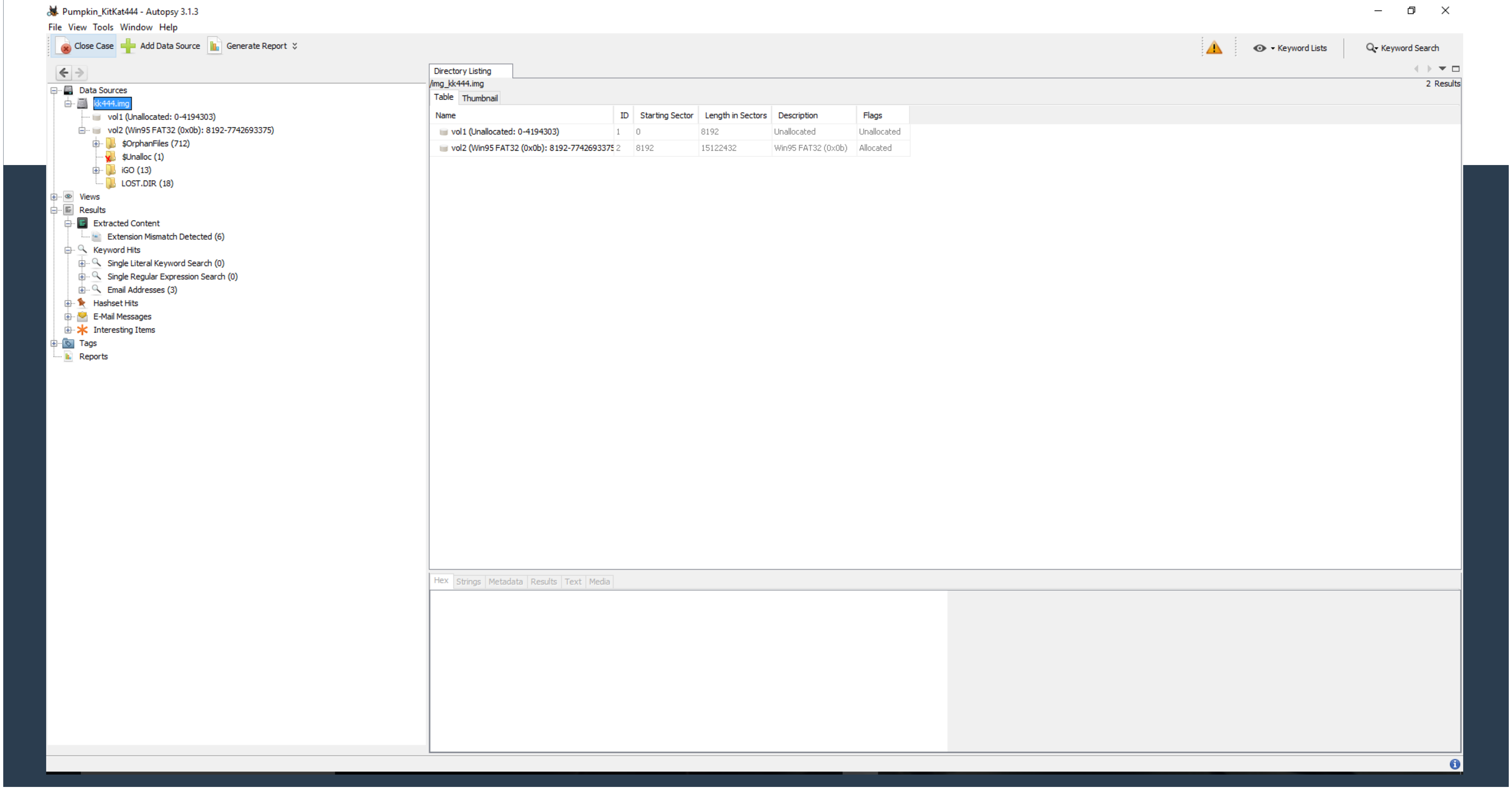

Memory
Directory
Export contacts
Holiday Inn □
Holiday Trans Can □
Home □
Jean Crossman □
Jeezer □
2:58 pm
Dial
Navigate to

EVEN MORE HARDWARE (AFTERMARKET)

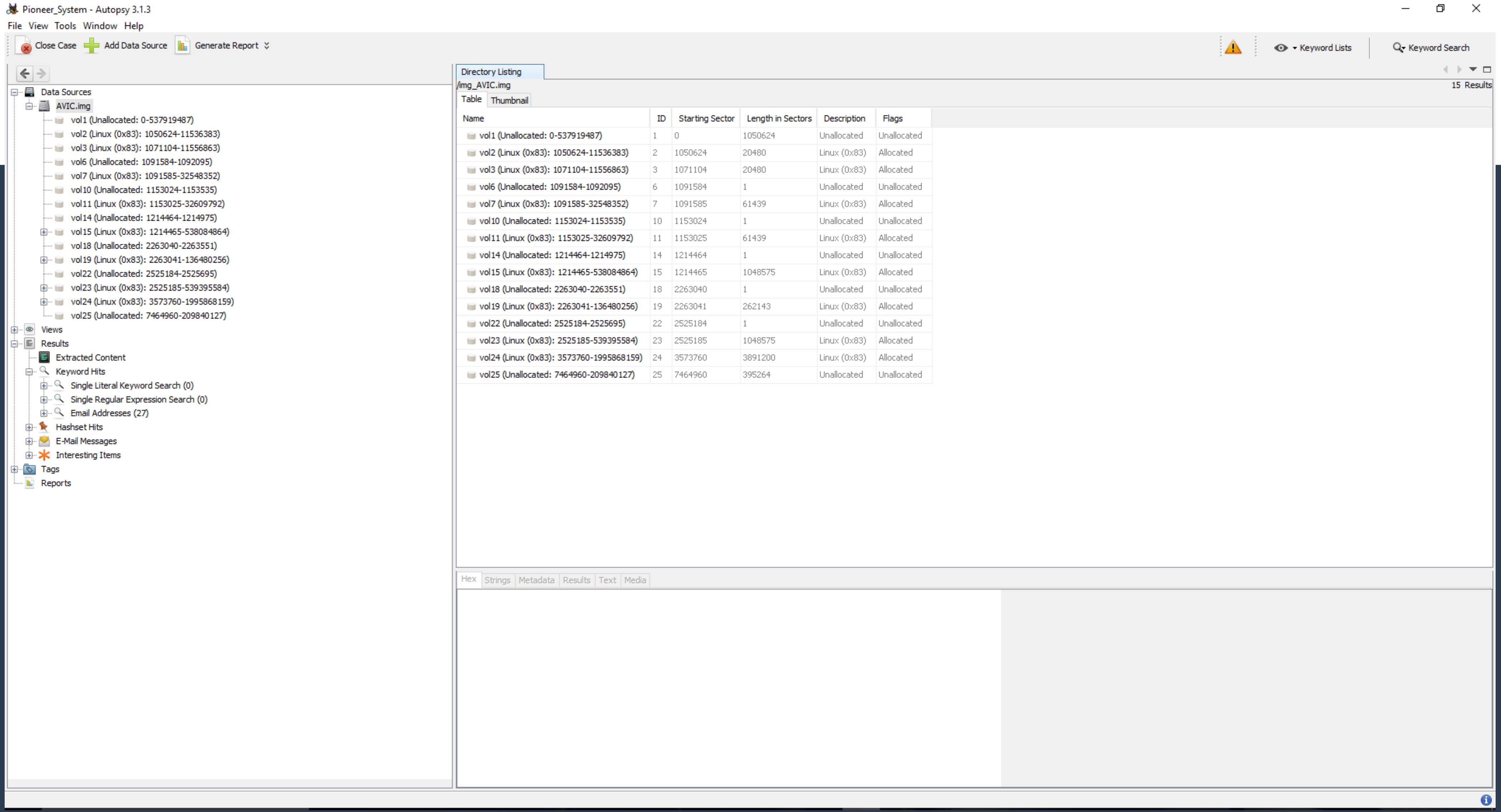
- Decided to acquire aftermarket systems as they’re still relevant in the market
- Windows CE 6 based infotainment (OUKU brand)
- Android Kitkat 4.4.4 infotainment (Pumpkin brand)
- Android variant with Android Auto and Apple Carplay (Pioneer brand)

DATA EXTRACTION PROCESS

- Basically, these were using commonly available operating systems so much more straightforward
- Gain SU and enable debugging mode or even better, get a terminal session going (especially for Android)
- Once complete, dd all the sectors into an .img file
- For Windows CE, replace GPS.exe shortcut with another .exe (explorer.exe in this case then full admin rights)



Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-4194303)	1	0	8192	Unallocated	Unallocated
vol2 (Win95 FAT32 (0x0b): 8192-774269337	2	8192	15122432	Win95 FAT32 (0x0b)	Allocated

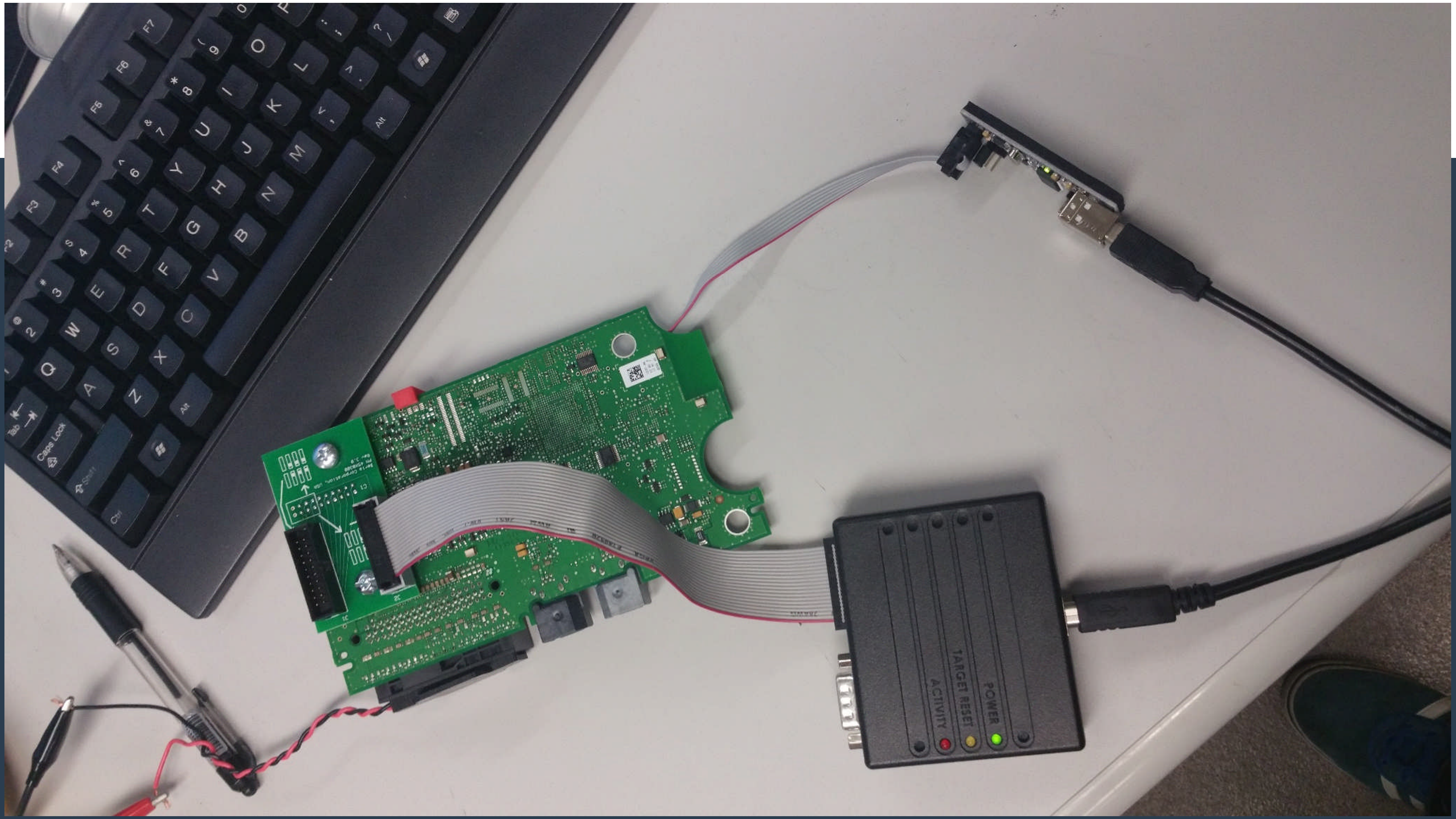


```
Data Sources
  AVIC.img
    vol1 (Unallocated: 0-537919487)
    vol2 (Linux (0x83): 1050624-11536383)
    vol3 (Linux (0x83): 1071104-11556863)
    vol6 (Unallocated: 1091584-1092095)
    vol7 (Linux (0x83): 1091585-32548352)
    vol10 (Unallocated: 1153024-1153535)
    vol11 (Linux (0x83): 1153025-32609792)
    vol14 (Unallocated: 1214464-1214975)
    vol15 (Linux (0x83): 1214465-538084864)
    vol18 (Unallocated: 2263040-2263551)
    vol19 (Linux (0x83): 2263041-136480256)
    vol22 (Unallocated: 2525184-2525695)
    vol23 (Linux (0x83): 2525185-539395584)
    vol24 (Linux (0x83): 3573760-1995868159)
    vol25 (Unallocated: 7464960-209840127)
Views
Results
  Extracted Content
  Keyword Hits
    Single Literal Keyword Search (0)
    Single Regular Expression Search (0)
    Email Addresses (27)
  Hashset Hits
  E-Mail Messages
  Interesting Items
Tags
Reports
```

/img_AVIC.img

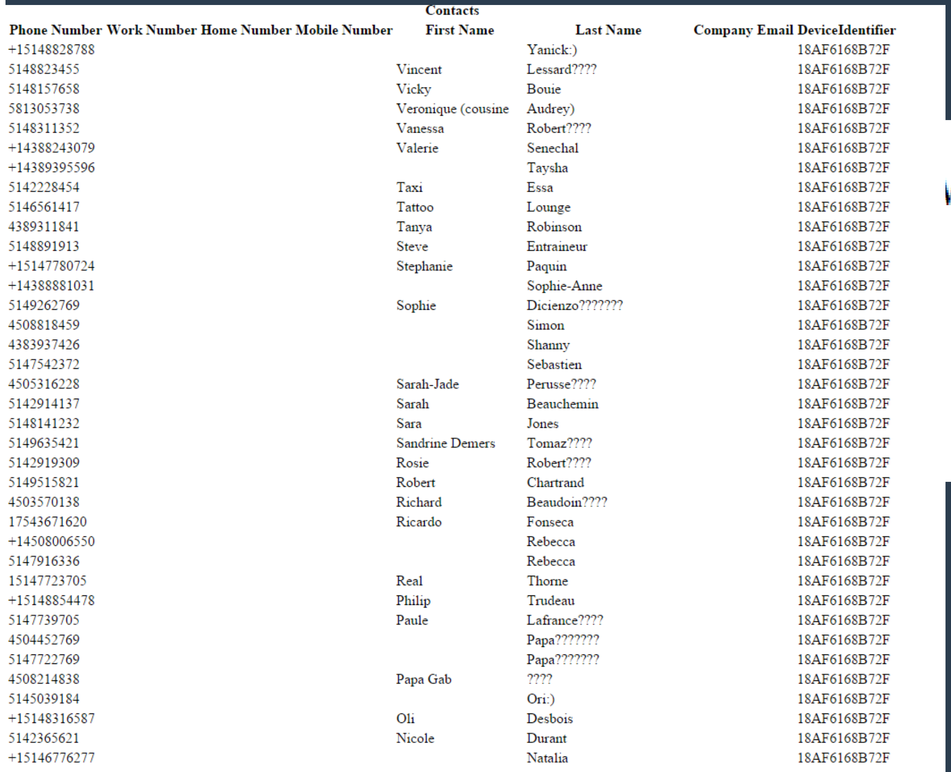
15 Results

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-537919487)	1	0	1050624	Unallocated	Unallocated
vol2 (Linux (0x83): 1050624-11536383)	2	1050624	20480	Linux (0x83)	Allocated
vol3 (Linux (0x83): 1071104-11556863)	3	1071104	20480	Linux (0x83)	Allocated
vol6 (Unallocated: 1091584-1092095)	6	1091584	1	Unallocated	Unallocated
vol7 (Linux (0x83): 1091585-32548352)	7	1091585	61439	Linux (0x83)	Allocated
vol10 (Unallocated: 1153024-1153535)	10	1153024	1	Unallocated	Unallocated
vol11 (Linux (0x83): 1153025-32609792)	11	1153025	61439	Linux (0x83)	Allocated
vol14 (Unallocated: 1214464-1214975)	14	1214464	1	Unallocated	Unallocated
vol15 (Linux (0x83): 1214465-538084864)	15	1214465	1048575	Linux (0x83)	Allocated
vol18 (Unallocated: 2263040-2263551)	18	2263040	1	Unallocated	Unallocated
vol19 (Linux (0x83): 2263041-136480256)	19	2263041	262143	Linux (0x83)	Allocated
vol22 (Unallocated: 2525184-2525695)	22	2525184	1	Unallocated	Unallocated
vol23 (Linux (0x83): 2525185-539395584)	23	2525185	1048575	Linux (0x83)	Allocated
vol24 (Linux (0x83): 3573760-1995868159)	24	3573760	3891200	Linux (0x83)	Allocated
vol25 (Unallocated: 7464960-209840127)	25	7464960	395264	Unallocated	Unallocated


POWER
TARGET RESET
ACTIVITY

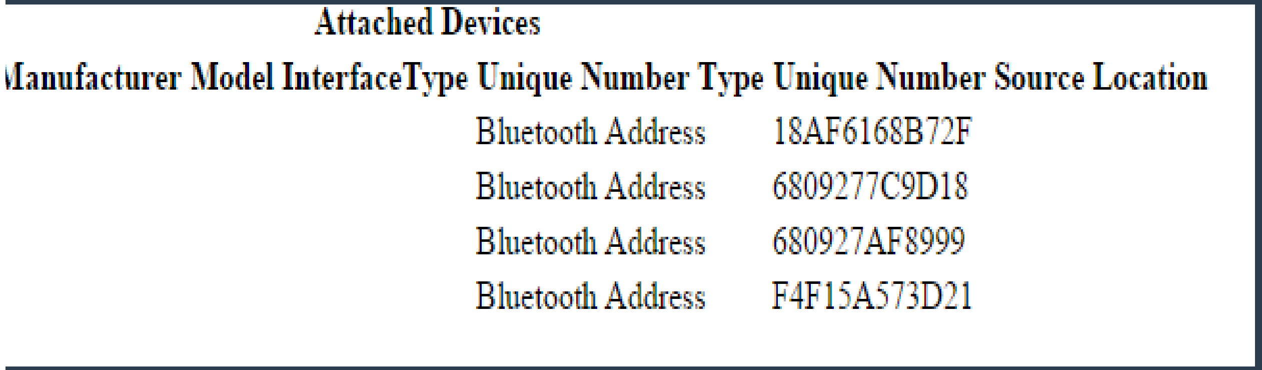
FORD SYNC

- Ford SYNC infotainments seem to keep all contacts, phone profiles as well as Bluetooth addresses and filesystem items



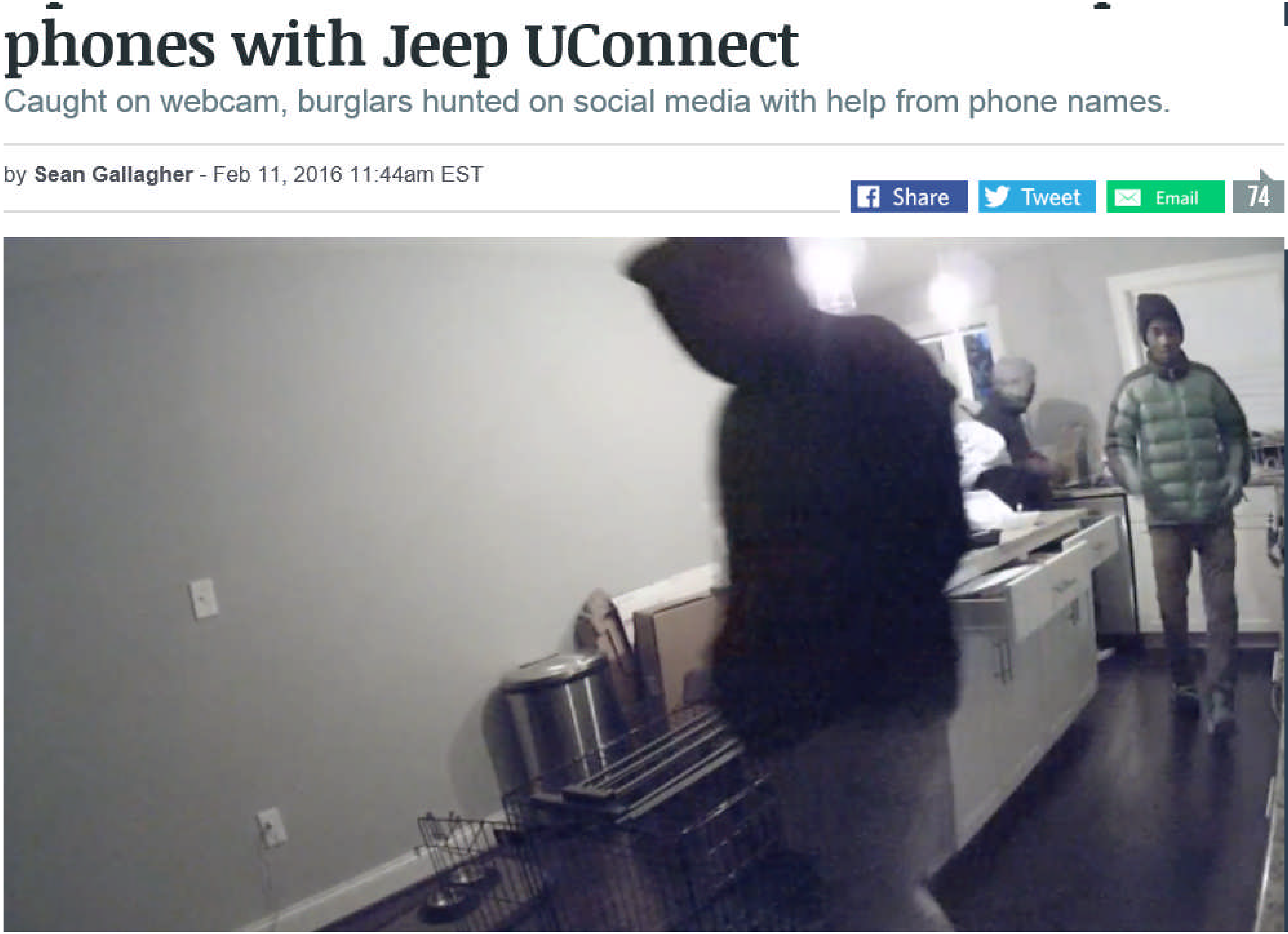
Contacts

Phone Number	Work Number	Home Number	Mobile Number	First Name	Last Name	Company	Email	DeviceIdentifier
+15148828788					Yanick:)			18AF6168B72F
5148823455				Vincent	Lessard????			18AF6168B72F
5148157658				Vicky	Bouie			18AF6168B72F
5813053738				Veronique (cousine	Audrey)			18AF6168B72F
5148311352				Vanessa	Robert????			18AF6168B72F
+14388243079				Valerie	Senechal			18AF6168B72F
+14389395596					Taysha			18AF6168B72F
5142228454				Taxi	Essa			18AF6168B72F
5146561417				Tattoo	Lounge			18AF6168B72F
4389311841				Tanya	Robinson			18AF6168B72F
5148891913				Steve	Entraineur			18AF6168B72F
+15147780724				Stephanie	Paquin			18AF6168B72F
+14388881031					Sophie-Anne			18AF6168B72F
5149262769				Sophie	Dicienzo???????			18AF6168B72F
4508818459					Simon			18AF6168B72F
4383937426					Shanny			18AF6168B72F
5147542372					Sebastien			18AF6168B72F
4505316228				Sarah-Jade	Perusse????			18AF6168B72F
5142914137				Sarah	Beauchemin			18AF6168B72F
5148141232				Sara	Jones			18AF6168B72F
5149635421				Sandrine Demers	Tomaz????			18AF6168B72F
5142919309				Rosie	Robert????			18AF6168B72F
5149515821				Robert	Chartrand			18AF6168B72F
4503570138				Richard	Beaudoin????			18AF6168B72F
17543671620				Ricardo	Fonseca			18AF6168B72F
+14508006550					Rebecca			18AF6168B72F
5147916336					Rebecca			18AF6168B72F
15147723705				Real	Thorne			18AF6168B72F
+15148854478				Philip	Trudeau			18AF6168B72F
5147739705				Paule	Lafrance????			18AF6168B72F
4504452769					Papa???????			18AF6168B72F
5147722769					Papa???????			18AF6168B72F
4508214838				Papa Gab	????			18AF6168B72F
5145039184					Ori:)			18AF6168B72F
+15148316587				Oli	Desbois			18AF6168B72F
5142365621				Nicole	Durant			18AF6168B72F
+15146776277					Natalia			18AF6168B72F



Attached Devices

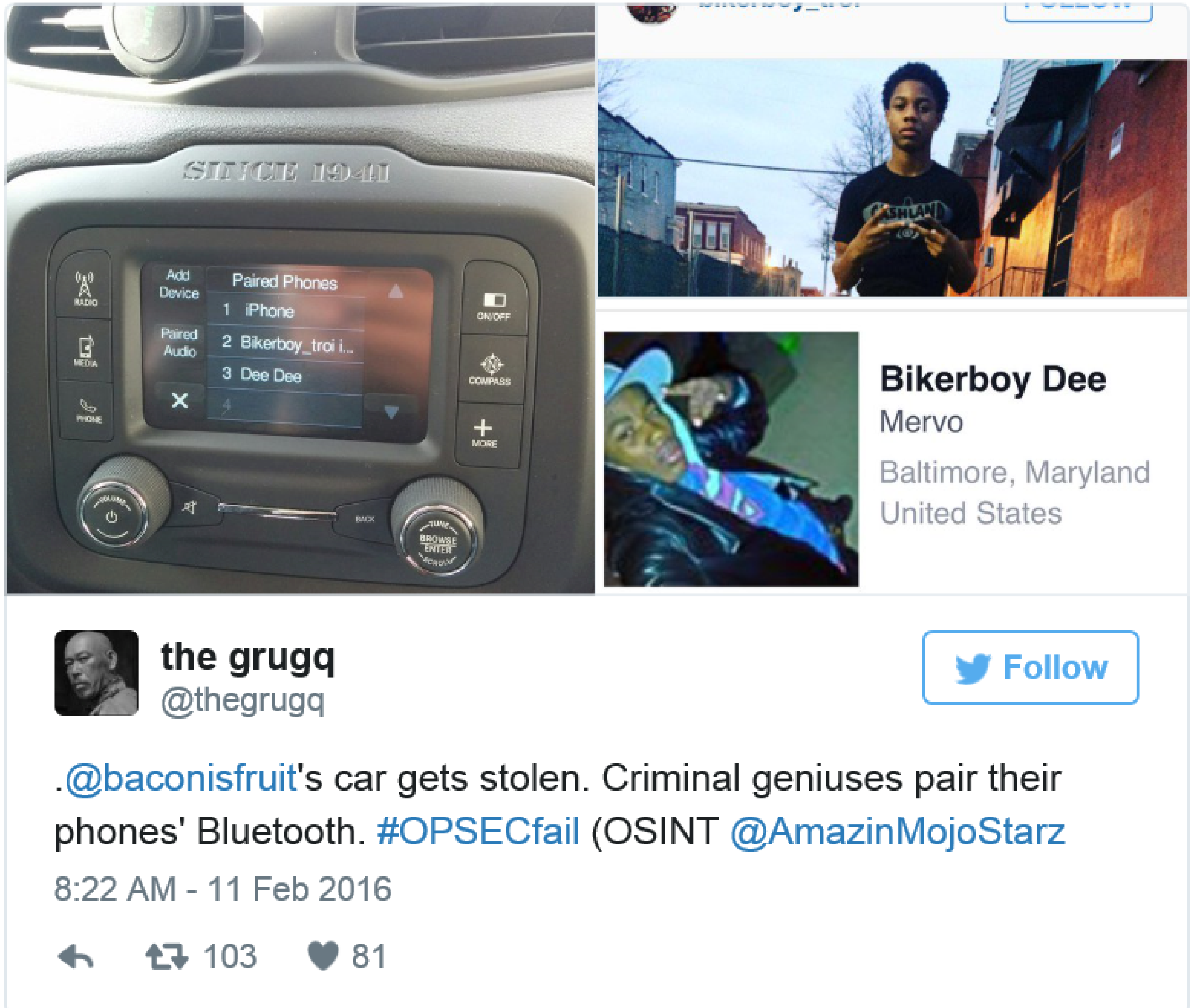
Ianufacturer	Model	InterfaceType	Unique Number Type	Unique Number	Source Location
			Bluetooth Address	18AF6168B72F	
			Bluetooth Address	6809277C9D18	
			Bluetooth Address	680927AF8999	
			Bluetooth Address	F4F15A573D21	



phones with Jeep UConnect

Caught on webcam, burglars hunted on social media with help from phone names.

by **Sean Gallagher** - Feb 11, 2016 11:44am EST



Bikerboy Dee
Mervo
Baltimore, Maryland
United States

the grugq
@thegrugq

Follow

.@baconisfruit's car gets stolen. Criminal geniuses pair their phones' Bluetooth. #OPSECfail (OSINT @AmazinMojoStarz

8:22 AM - 11 Feb 2016

103 81

LAWS, POLICIES, AND USERS

- Previous law and policy research has demonstrated a widespread disrespect for the privacy of customers by companies offering connected car services.

- Survey research indicates that drivers will be more comfortable with the use of connected systems if they have some measure of control over their privacy settings

LAWS, POLICIES, AND USERS

- Apart from PIPEDA, there are no laws enforced to limit the collection and use of customer information by automakers
- Customers must trust the policies and terms dictated by automakers and infotainment/telematics service providers

WHAT DID WE CONCLUDE?

- Privacy policies are a necessary but an insufficient form of privacy protection in the connected vehicle context.

Necessary because…

- Privacy regulation is based on the notion that the individual 'data subject' exercises control over their personal information
- It is also a consent driven model

Insufficient because…

- People do no read privacy policies
- People over value the immediate benefits obtained from revealing personal information and under estimate the cost of privacy loss
- Companies often use privacy policies to seem trustworthy while mitigating unethical data handling practices

Recommendations for Reform

- Design for Privacy
- Only collect data required to provide the original service advertised (not secondary purposes such as marketing).
- Only access and use the data collected for purposes involved with providing the advertised service.
- Do not share collected data with third-parties even if data is de-identified unless required for the service.

Recommendations for Reform

- Ensure “Terms and Conditions” and “Privacy Policy” documents clearly identify what data will be collected from both infotainment AND telematics systems, as well, define how the collected data will be used.
- Collected data should only be retained for the duration required by the service and then securely erased.
- Should a company choose to employ a less strict version of the policies recommended above which shares customer information with third-parties, customers should be provided the option to opt-out on the spot and their request should be processed immediately; preventing customer information to be shared starting from the time their service begins.

ADDITIONAL PRIVACY RECOMMENDATIONS FOR CAR DEALERS AND RENTAL COMPANIES

- Ensure any existing data from both the infotainment AND telematics system is cleared prior to selling/renting the vehicle.
- Employ vehicle inspection reports to verify that the data has been cleared.

INDEPENDENT CREDENTIALING AUTHORITY

- Trusted by customers, manufacturers, system operators, service providers
- Created by statute.

Establish rules for:

- Initialization – Vehicle set-up
- Operation – Major mode of operation

QUESTIONS?