Automotive DoIP and Forensic Analysis for Automotive Systems

Christopher Corbett and Kevin Gomez Buquerin

Disclaimer

The opinions expressed in this presentation and on the following slides are solely those of the presenters and not necessarily those of the Audi AG.

Please note that we are not answering questions to products or strategies of the Audi AG.

Thank you.

Who are we

Christopher Corbett:

Phd-Student@ Ulm University
Incident Responder@ AUDI AG

✉ christopher.corbett@uni-ulm.de

🔗 www.ccorbett.de

Kevin Gomez Buquerin:

Phd-Student@ TH Ingolstadt
Incident Responder@ AUDI AG

✉ kgbuquerin@gmail.com

🐦 @kgbuquerin

🔗 www.github.com/kgbuquerin

What we are going to talk about

- Change in the automotive domain
- Motivation for this research
- What do ICS and automotive have in common
- Public awareness and research
- DoIP and UDS protocol
- Evaluation & Tooling
- Why automotive forensics?
- Definition of automotive forensics
- Implementation of our automotive forensics concept
- Gap analysis and opportunities
- Summary of the talk

The automotive domain is changing

UNECE
ISO21434
ISO26262

Complexity
of Automotive
Systems

Mobility
Services

Crime
Misuse

Security

Autonomous
Driving

Motivation for the research

Chris is into:

Embedded Systems
Automotive Security
Automotive Protocols
Testing
Forensic

+

Kevin is into:

Malware Analysis
Forensic
Reverse Engineering
Automotive Security

Protocol Analysis & Forensics @ State of the Art Automotive Systems

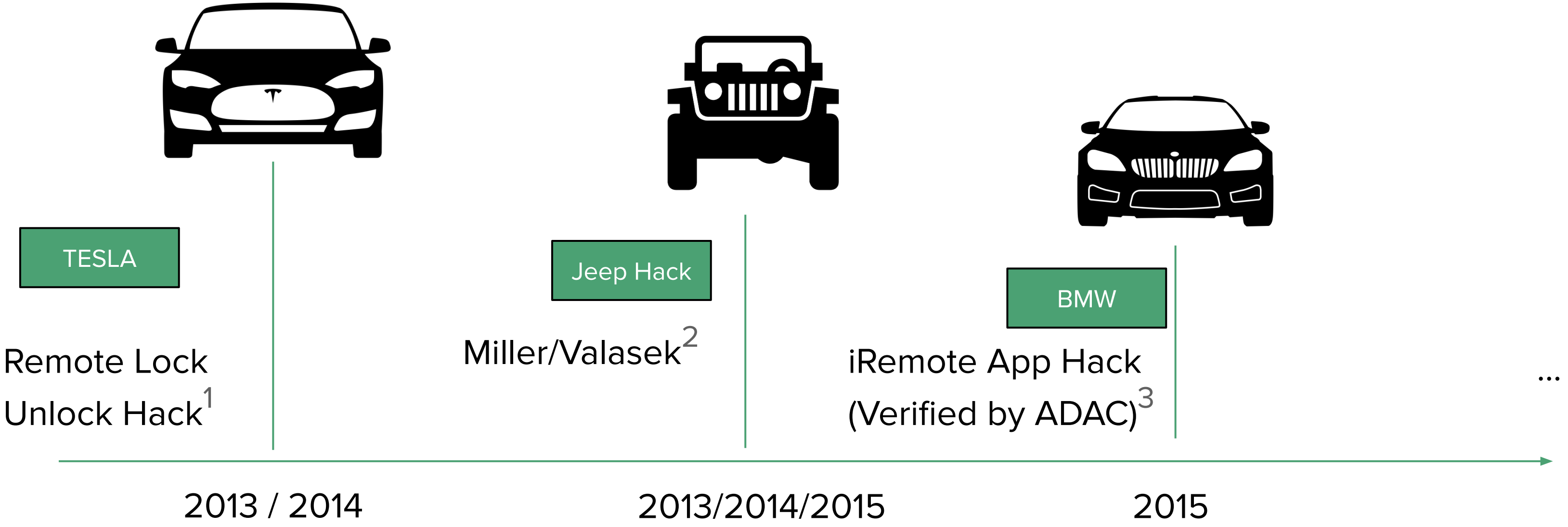
Detailed publications planned early 2020

- Forensic Readiness, Ethernet based Automotive Protocol Analysis and Information Gathering Possibilities

Comparison

ICS	Automotive
Systems run ~20/30+ years	Systems run ~20/30+ years
Patching is difficult due to certification sensitivity of the infrastructure	Patching is difficult due to safety clearance and distribution overhead
Mostly Windows and Linux based systems	10+ different operating systems
Interconnection via internet proofed to be a bad idea	Goal to interconnect all vehicles via internet
Standardized & proprietary protocols	Standardized & proprietary protocols
....	....

How it all started with public awareness and research



TESLA

Remote Lock
Unlock Hack[1]

2013 / 2014

Jeep Hack

Miller/Valasek[2]

2013/2014/2015

BMW

iRemote App Hack
(Verified by ADAC)[3]

2015

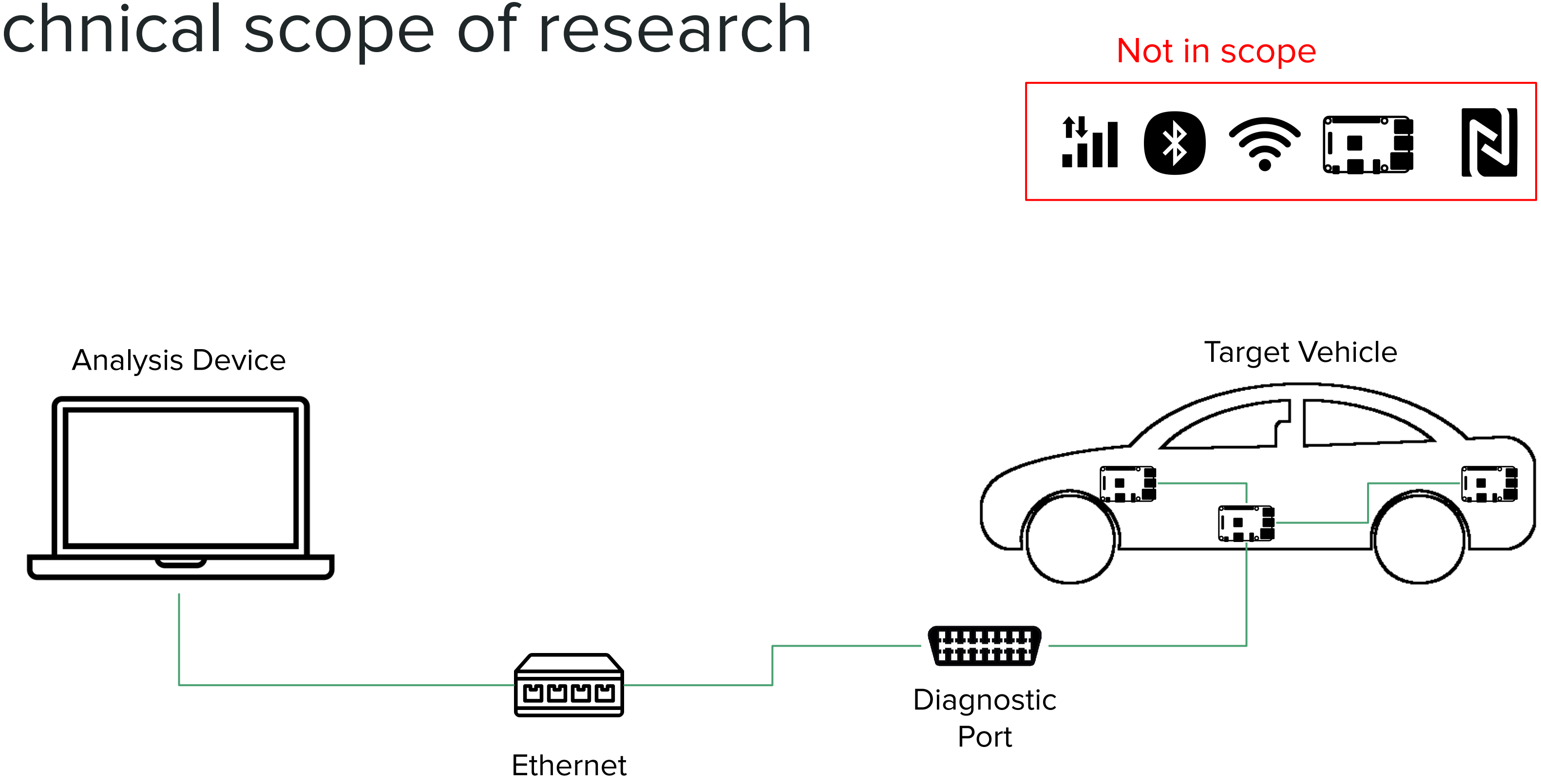
...

[1] https://www.spiegel.de/auto/aktuell/tesla-model-s-von-hackern-fremdgesteuert-a-982481.html

[2] http://illmatics.com/carhacking.html

[3] http://www.carnectiv.com/2015/02/adac-reveals-security-flaw-bmw-connecteddrive-service/

Technical scope of research

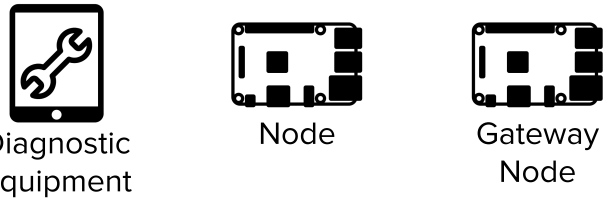


What is DoIP

Diagnostic over Internet Protocol: IP based transport protocol for vehicle diagnostic messages

- ❑ Specified in **ISO13400**
- ❑ **Request** and **Response**
- ❑ **UDP** and **TCP** port **13400**

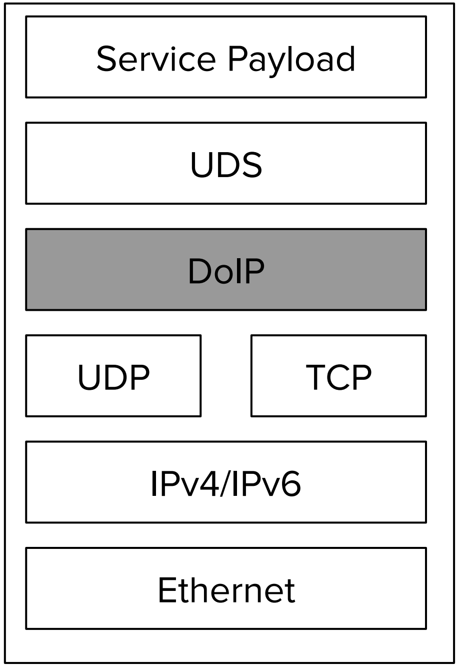
Provides 3 different entity types:



Diagnostic Equipment

Node

Gateway Node



Service Payload

UDS

DoIP

UDP

TCP

IPv4/IPv6

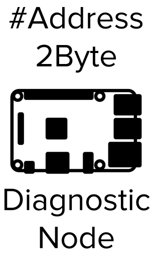
Ethernet

Simple Stack Representation

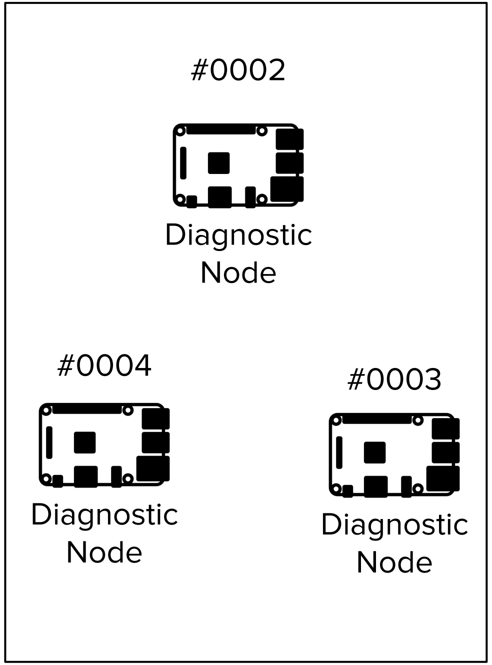
What is UDS

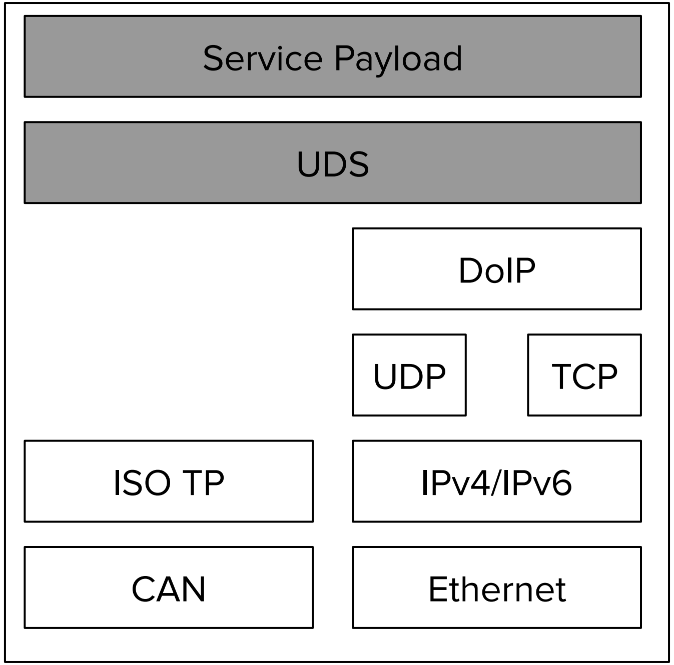
Unified Diagnostic Services: Protocol for diagnostic services calls and payload transport

- Specified in **ISO14229**
- **Request** and **Response**
- **Sub specs:**
  - **ISO15031**
  - **ISO27145**
  - **...**



Service ID	Service	Payload
#01	...	...
#02	...	...

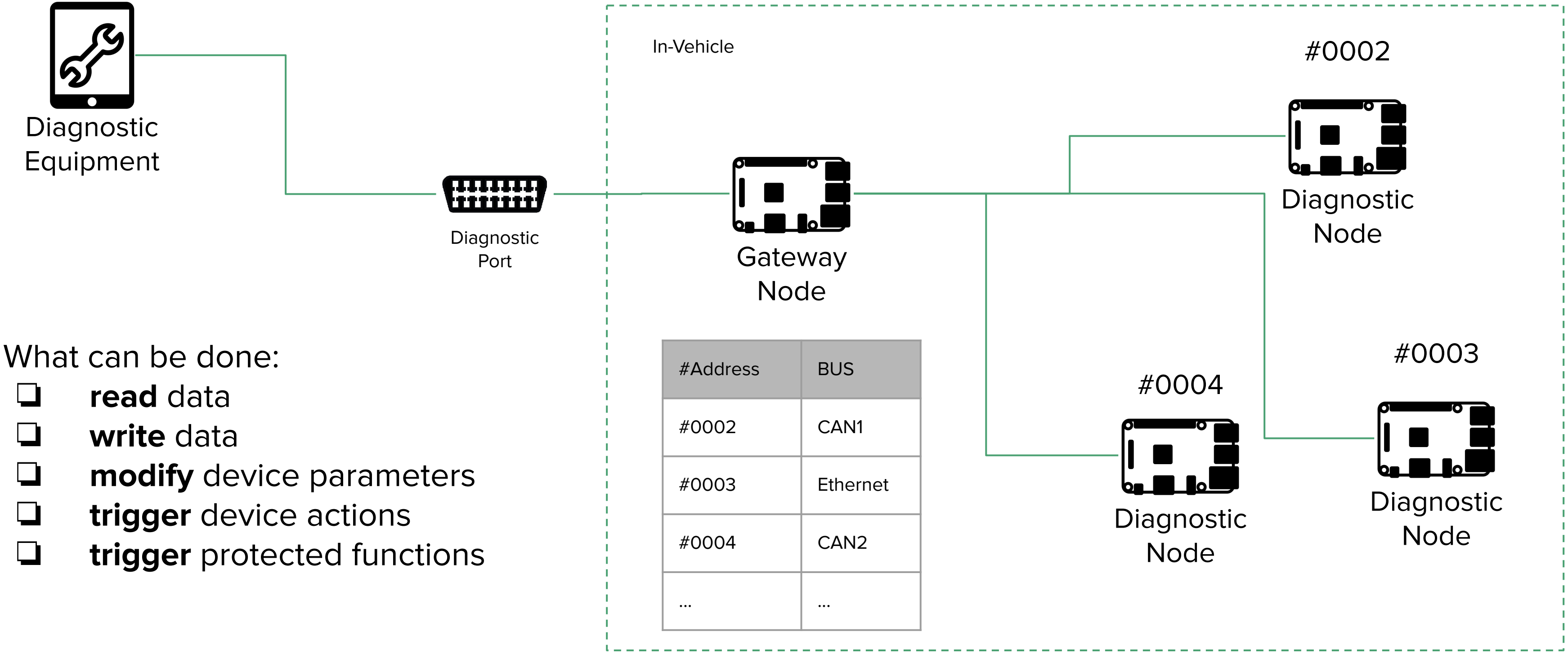




Simple Stack Representation - Example

How they work together

Combined the two protocols enable communication between the diagnostic device and the ECUs



#Address	BUS
#0002	CAN1
#0003	Ethernet
#0004	CAN2
...	...

What can be done:

❑ **read** data

❑ **write** data

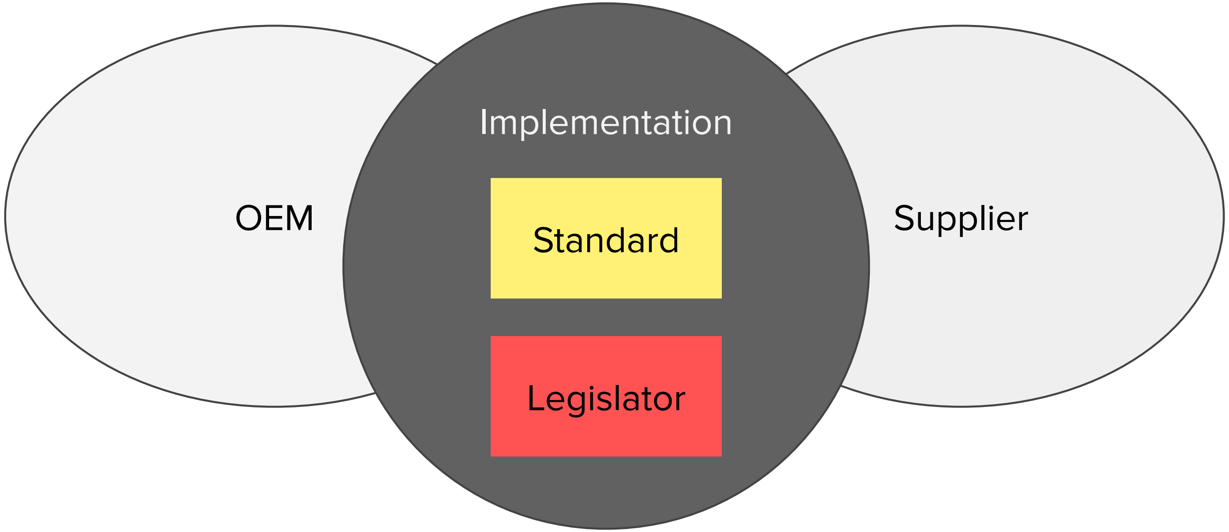
❑ **modify** device parameters

❑ **trigger** device actions

❑ **trigger** protected functions

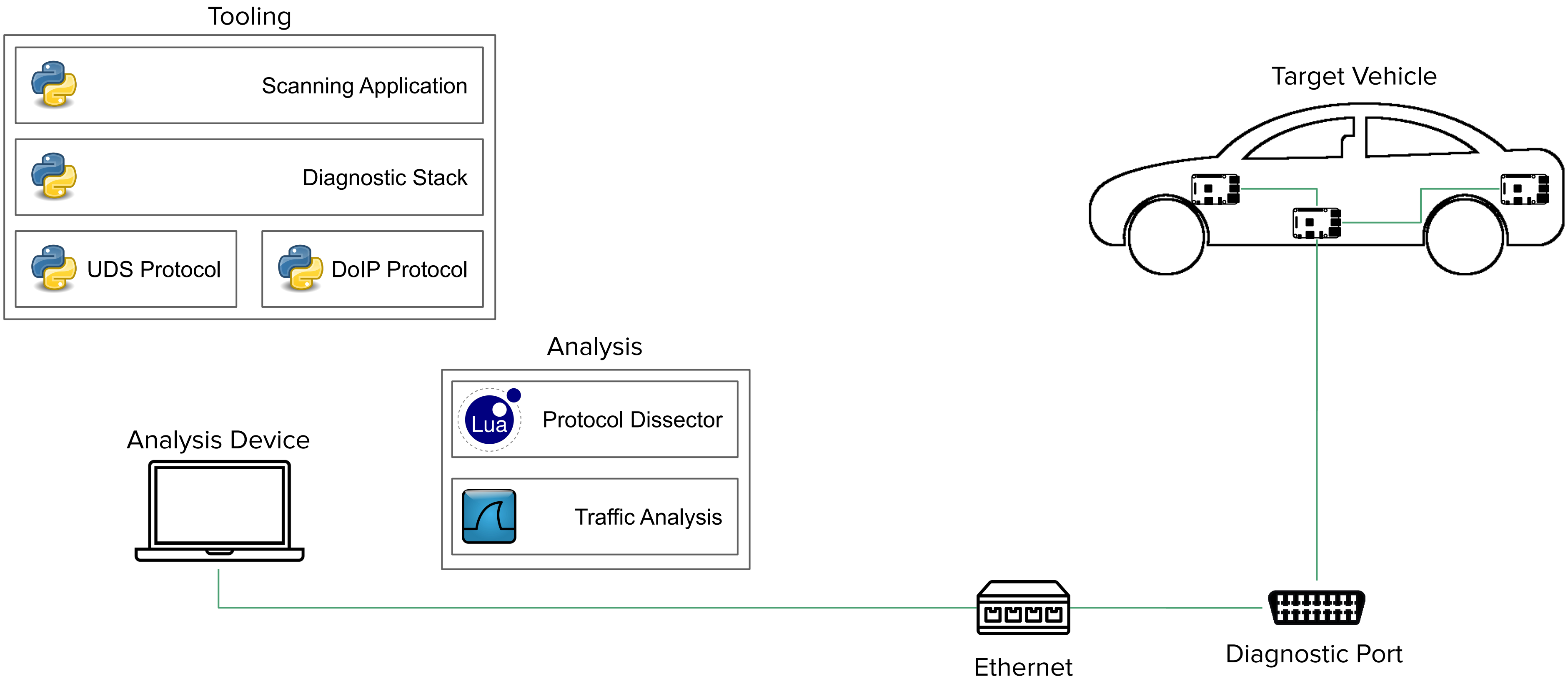
Protocol composition

Protocol defines dynamic/proprietary ranges for OEMs and Suppliers



Maybe left over debug functionality in the proprietary parts of the implementation

What have we done so far



Tooling

Scanning Application

Diagnostic Stack

UDS Protocol

DoIP Protocol

Analysis

Protocol Dissector

Traffic Analysis

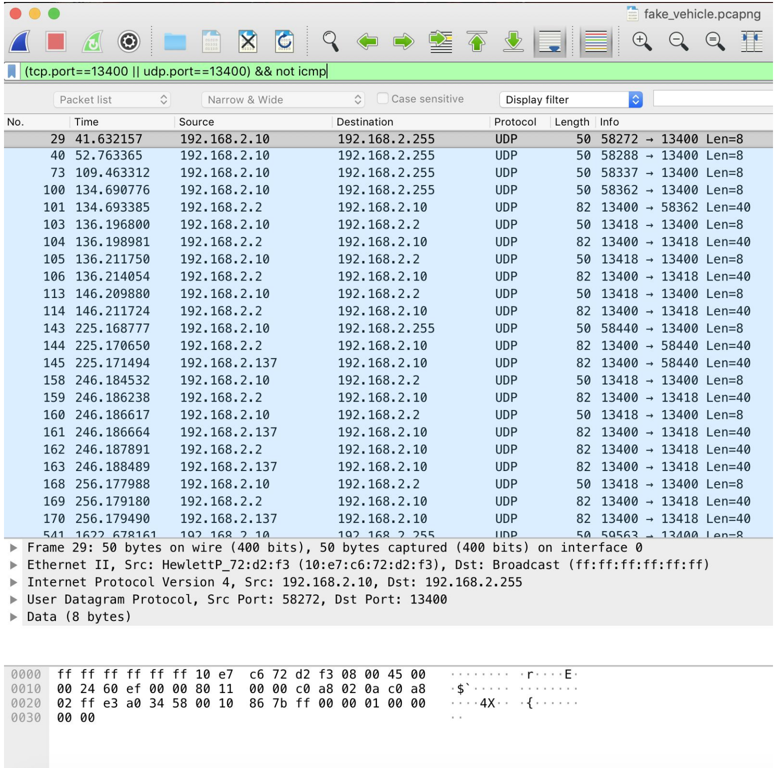
Analysis Device

Target Vehicle

Ethernet

Diagnostic Port

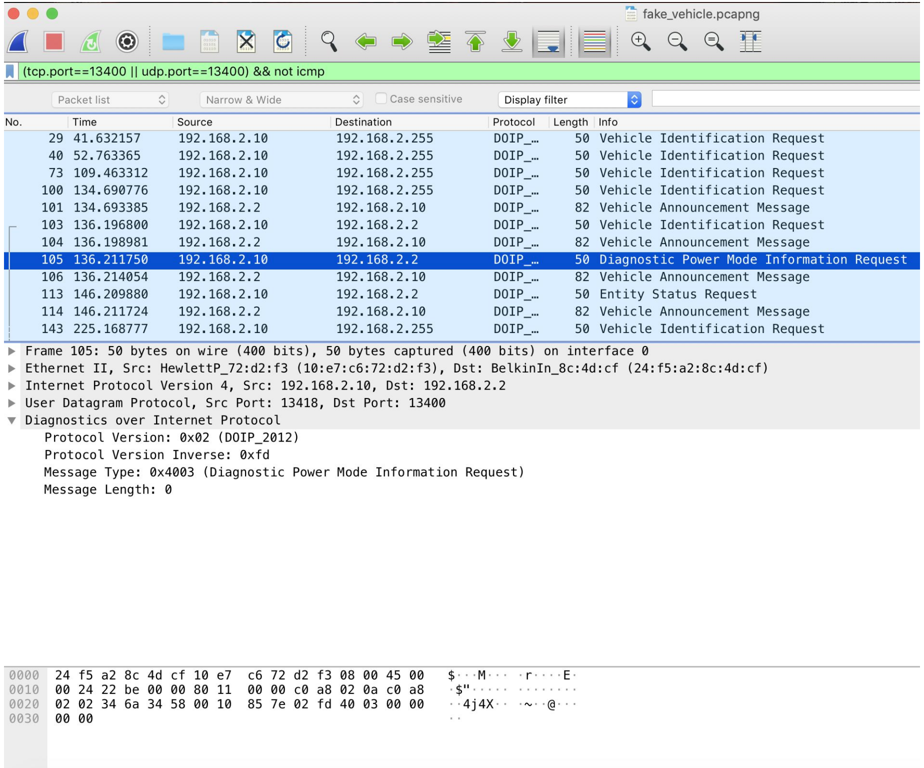
Tooling samples



```
(tcp.port==13400 || udp.port==13400) && not icmp
```

```
No.   Time         Source          Destination     Protocol Length Info
   29 41.632157    192.168.2.10    192.168.2.255   UDP        50  58272 → 13400 Len=8
   40 52.763365    192.168.2.10    192.168.2.255   UDP        50  58288 → 13400 Len=8
   73 109.463312   192.168.2.10    192.168.2.255   UDP        50  58337 → 13400 Len=8
  100 134.690776   192.168.2.10    192.168.2.255   UDP        50  58362 → 13400 Len=8
  101 134.693385   192.168.2.2     192.168.2.10    UDP        82  13400 → 58362 Len=40
  103 136.196800   192.168.2.10    192.168.2.2     UDP        50  13418 → 13400 Len=8
  104 136.198981   192.168.2.2     192.168.2.10    UDP        82  13400 → 13418 Len=40
  105 136.211750   192.168.2.10    192.168.2.2     UDP        50  13418 → 13400 Len=8
  106 136.214054   192.168.2.2     192.168.2.10    UDP        82  13400 → 13418 Len=40
  113 146.209880   192.168.2.10    192.168.2.2     UDP        50  13418 → 13400 Len=8
  114 146.211724   192.168.2.2     192.168.2.10    UDP        82  13400 → 13418 Len=40
  143 225.168777   192.168.2.10    192.168.2.255   UDP        50  58440 → 13400 Len=8
  144 225.170650   192.168.2.2     192.168.2.10    UDP        82  13400 → 58440 Len=40
  145 225.171494   192.168.2.137   192.168.2.10    UDP        82  13400 → 58440 Len=40
  158 246.184532   192.168.2.10    192.168.2.2     UDP        50  13418 → 13400 Len=8
  159 246.186238   192.168.2.2     192.168.2.10    UDP        82  13400 → 13418 Len=40
  160 246.186617   192.168.2.10    192.168.2.2     UDP        50  13418 → 13400 Len=8
  161 246.186664   192.168.2.137   192.168.2.10    UDP        82  13400 → 13418 Len=40
  162 246.187891   192.168.2.2     192.168.2.10    UDP        82  13400 → 13418 Len=40
  163 246.188489   192.168.2.137   192.168.2.10    UDP        82  13400 → 13418 Len=40
  168 256.177988   192.168.2.10    192.168.2.2     UDP        50  13418 → 13400 Len=8
  169 256.179180   192.168.2.2     192.168.2.10    UDP        82  13400 → 13418 Len=40
  170 256.179490   192.168.2.137   192.168.2.10    UDP        82  13400 → 13418 Len=40
  541 1622.678161  192.168.2.10    192.168.2.255   UDP        50  59563 → 13400 Len=8

▶ Frame 29: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0
▶ Ethernet II, Src: HewlettP_72:d2:f3 (10:e7:c6:72:d2:f3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.2.255
▶ User Datagram Protocol, Src Port: 58272, Dst Port: 13400
▶ Data (8 bytes)

0000  ff ff ff ff ff ff 10 e7  c6 72 d2 f3 08 00 45 00   ········ ·r····E·
0010  00 24 60 ef 00 00 80 11  00 00 c0 a8 02 0a c0 a8   ·$`····· ········
0020  02 ff e3 a0 34 58 00 10  86 7b ff 00 00 01 00 00   ····4X·· ·{······
0030  00 00                                              ··
```

without dissector

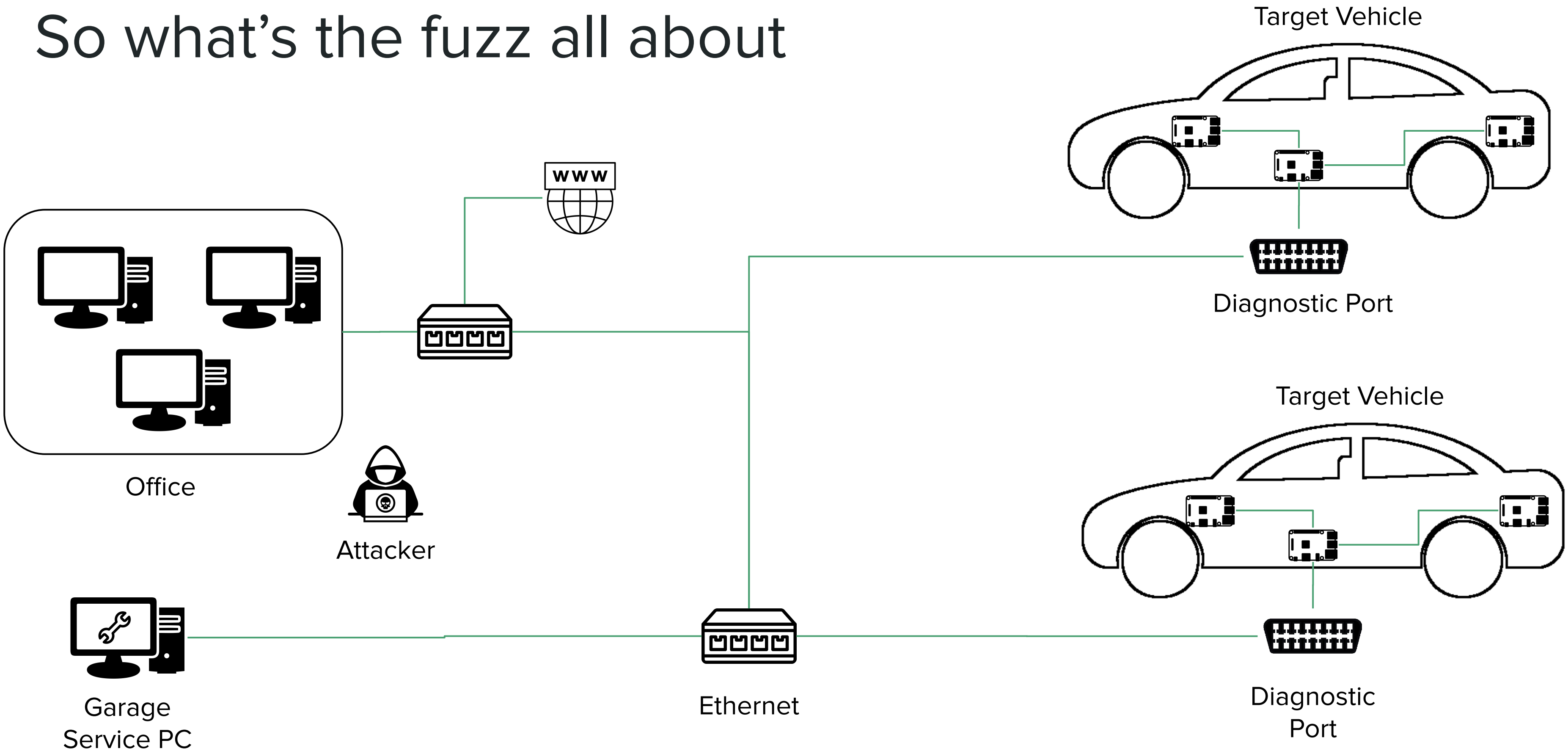


```
(tcp.port==13400 || udp.port==13400) && not icmp
```

```
No.   Time         Source          Destination     Protocol Length Info
   29 41.632157    192.168.2.10    192.168.2.255   DOIP_…     50  Vehicle Identification Request
   40 52.763365    192.168.2.10    192.168.2.255   DOIP_…     50  Vehicle Identification Request
   73 109.463312   192.168.2.10    192.168.2.255   DOIP_…     50  Vehicle Identification Request
  100 134.690776   192.168.2.10    192.168.2.255   DOIP_…     50  Vehicle Identification Request
  101 134.693385   192.168.2.2     192.168.2.10    DOIP_…     82  Vehicle Announcement Message
  103 136.196800   192.168.2.10    192.168.2.2     DOIP_…     50  Vehicle Identification Request
  104 136.198981   192.168.2.2     192.168.2.10    DOIP_…     82  Vehicle Announcement Message
  105 136.211750   192.168.2.10    192.168.2.2     DOIP_…     50  Diagnostic Power Mode Information Request
  106 136.214054   192.168.2.2     192.168.2.10    DOIP_…     82  Vehicle Announcement Message
  113 146.209880   192.168.2.10    192.168.2.2     DOIP_…     50  Entity Status Request
  114 146.211724   192.168.2.2     192.168.2.10    DOIP_…     82  Vehicle Announcement Message
  143 225.168777   192.168.2.10    192.168.2.255   DOIP_…     50  Vehicle Identification Request

▶ Frame 105: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0
▶ Ethernet II, Src: HewlettP_72:d2:f3 (10:e7:c6:72:d2:f3), Dst: BelkinIn_8c:4d:cf (24:f5:a2:8c:4d:cf)
▶ Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.2.2
▶ User Datagram Protocol, Src Port: 13418, Dst Port: 13400
▼ Diagnostics over Internet Protocol
    Protocol Version: 0x02 (DOIP_2012)
    Protocol Version Inverse: 0xfd
    Message Type: 0x4003 (Diagnostic Power Mode Information Request)
    Message Length: 0

0000  24 f5 a2 8c 4d cf 10 e7  c6 72 d2 f3 08 00 45 00   $···M··· ·r····E·
0010  00 24 22 be 00 00 80 11  00 00 c0 a8 02 0a c0 a8   ·$"····· ········
0020  02 02 34 6a 34 58 00 10  85 7e 02 fd 40 03 00 00   ··4j4X·· ·~··@···
0030  00 00                                              ··
```

with dissector

So what’s the fuzz all about



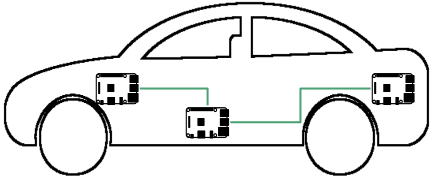
Let’s take that a bit further

Can we find vehicles in the local network?

Yes:

Nmap module

Target Vehicle



Can that be taken even further to disturb or attack ?

Yes:

PoC impl.

Example:
- **11** byte payload sufficient for simple scenario

How can we use that?

Automotive forensics

Automotive forensics is the use of digital forensics techniques and methods to collect data and digital evidence stored in automotive systems.

Techniques and methods include **live- and post-mortem** forensic analysis.

Acquisition is performed in an **online or offline** manner.

Requirements for court

Based on Alexander Geschonnek[1]

Consistency

Robustness

Integrity

Functionality

Acceptance

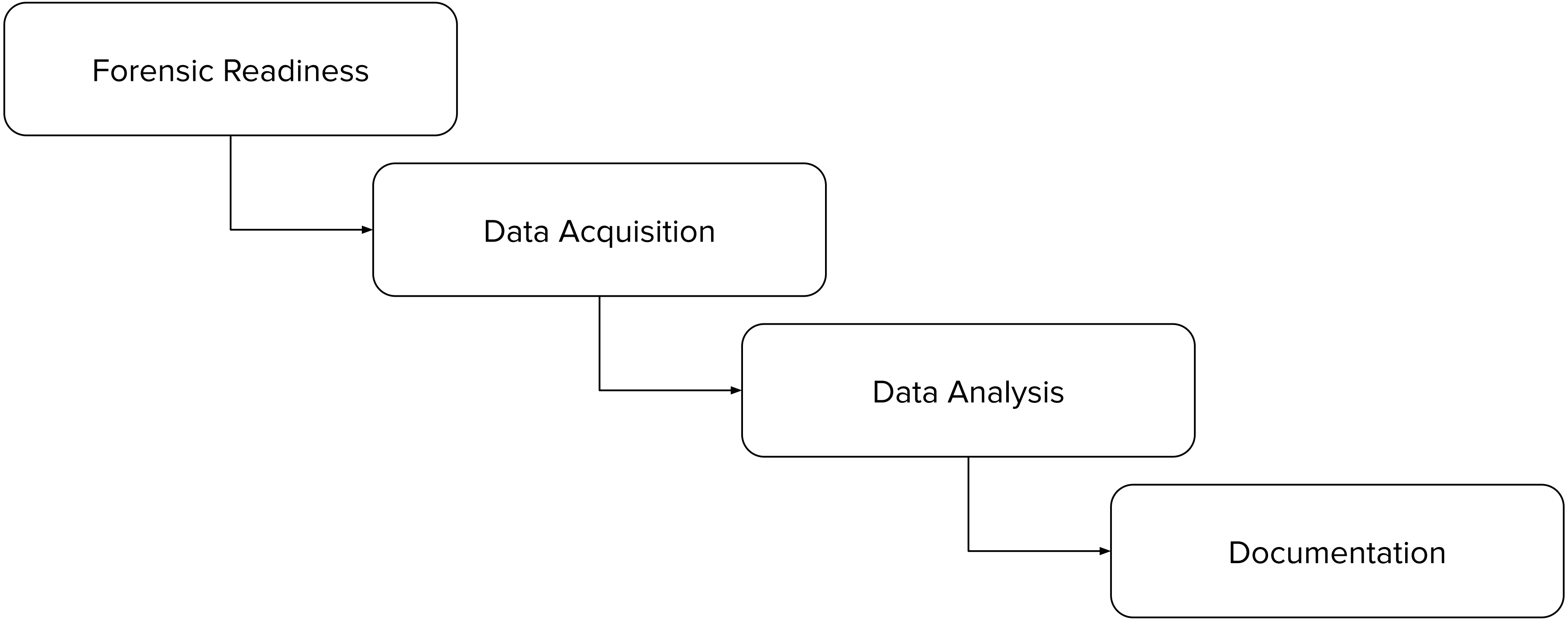
Reproducibility

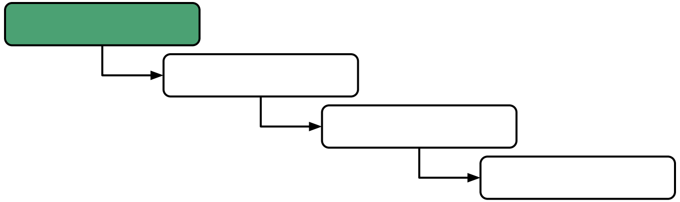
[1] Alexander Geschonneck - Computer-Forensik - Computerstraftaten erkennen, ermitteln, aufklären

Research challenges

Digital forensics	**Relevance for vehicles**
Complexity	Relevant
Diversity	Not relevant
Consistence and correlation	Relevant
Quantity or volume	Relevant
Unified time-lining	Relevant

Automotive forensics concept

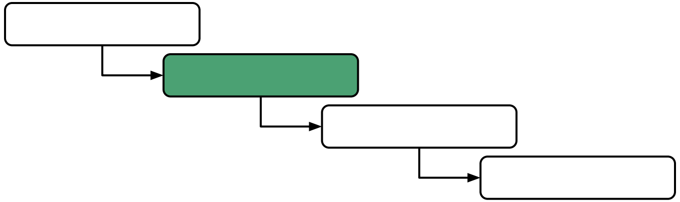




Forensic readiness

Defined by:

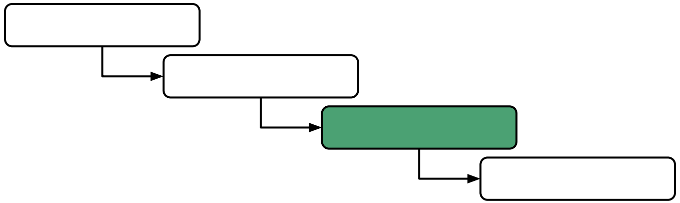
- Presence of **data sources** ✓
  - Diagnostic interface OBD-II
- Available **tools** ✓
  - Python framework implementing DoIP and UDS standards
  - Self build OBD-II to Ethernet cable
  - Analysis computer running Wireshark including dissector
- **Level** of development —
  - Automotive forensics resources are limited
  - Analysis was performed beforehand on test-vehicles



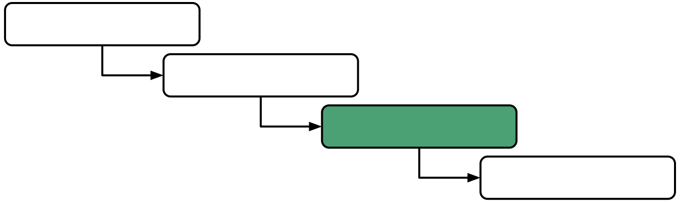
Data acquisition

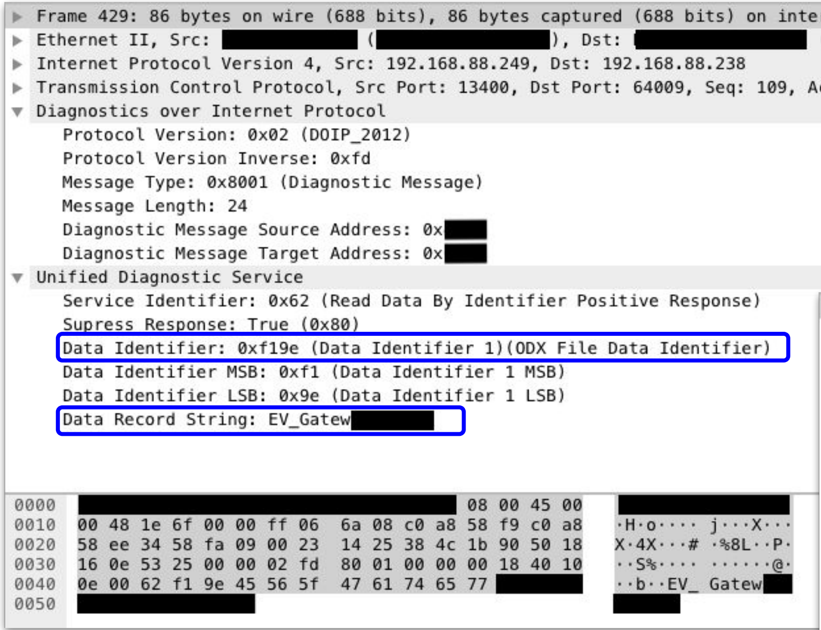
1. Try all possible **Target Addresses** (TA) ➔ `0x0000` to `0xffff`
2. Send **UDS Service Identifiers** (SId) to installed devices
    a. *repairShopCodeOrTesterSerialNumberDataIdentifier* (`0xf198`)
    b. *applicationSoftwareFingerprintDataIdentifier* (`0xf181`)
    c. *ECUInstallationDateDataIdentifier* (`0xf19d`)
    d. Etc.
3. While communicating, **capture traffic** using Wireshark
4. **Duplicate captures** and save original files on an external drive

Data analysis

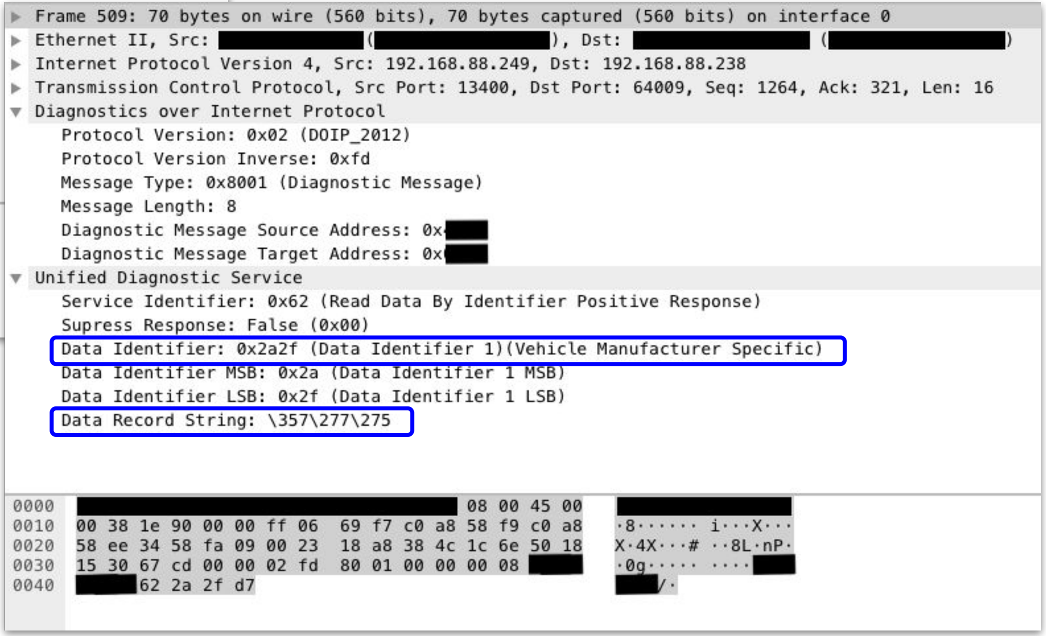


- **Filter PCAP** for positive response messages
    - `uds.service_identifier==0x62`
- **Determine**, for possible **evidence** and **interesting frames**
- **Changes** to the vehicle **are identifiable** → Illegal tuning scenario
    - *VehicleManufacturerECUHardwareNumberDataIdentifier* (`0xf191`)
    - *VehicleManufacturerECUSoftwareNumberDataIdentifier* (`0xf189`)
    - *CalibrationRepairShopCodeOrCalibrarionEquipmentSerialNumberDataIdentifier* (`0xf19a`)
- Some data is readable other is not
- Data identifier `0x2a2f` (Vehicle Manufacturer Specific) requires additional reversing or internal documentation



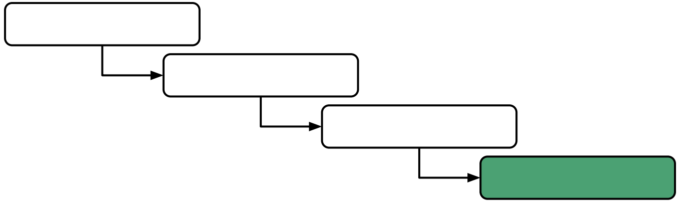


```
▶ Frame 429: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: [redacted] ([redacted]), Dst: [redacted] ([redacted])
▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
▶ Transmission Control Protocol, Src Port: 13400, Dst Port: 64009, Seq: 109, Ack: 99, Len: 32
▼ Diagnostics over Internet Protocol
    Protocol Version: 0x02 (DOIP_2012)
    Protocol Version Inverse: 0xfd
    Message Type: 0x8001 (Diagnostic Message)
    Message Length: 24
    Diagnostic Message Source Address: 0x[redacted]
    Diagnostic Message Target Address: 0x[redacted]
▼ Unified Diagnostic Service
    Service Identifier: 0x62 (Read Data By Identifier Positive Response)
    Supress Response: True (0x80)
    Data Identifier: 0xf19e (Data Identifier 1)(ODX File Data Identifier)
    Data Identifier MSB: 0xf1 (Data Identifier 1 MSB)
    Data Identifier LSB: 0x9e (Data Identifier 1 LSB)
    Data Record String: EV_Gatew[redacted]

0000  [redacted]                08 00 45 00   [redacted]
0010  00 48 1e 6f 00 00 ff 06  6a 08 c0 a8 58 f9 c0 a8   ·H·o····  j···X···
0020  58 ee 34 58 fa 09 00 23  14 25 38 4c 1b 90 50 18   X·4X···#  ·%8L··P·
0030  16 0e 53 25 00 00 02 fd  80 01 00 00 00 18 40 10   ··S%····  ······@·
0040  0e 00 62 f1 9e 45 56 5f  47 61 74 65 77 [redacted]  ··b··EV_ Gatew[redacted]
0050  [redacted]                                         [redacted]
```



```
▶ Frame 509: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: [redacted] ([redacted]), Dst: [redacted] ([redacted])
▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
▶ Transmission Control Protocol, Src Port: 13400, Dst Port: 64009, Seq: 1264, Ack: 321, Len: 16
▼ Diagnostics over Internet Protocol
    Protocol Version: 0x02 (DOIP_2012)
    Protocol Version Inverse: 0xfd
    Message Type: 0x8001 (Diagnostic Message)
    Message Length: 8
    Diagnostic Message Source Address: 0x[redacted]
    Diagnostic Message Target Address: 0x[redacted]
▼ Unified Diagnostic Service
    Service Identifier: 0x62 (Read Data By Identifier Positive Response)
    Supress Response: False (0x00)
    Data Identifier: 0x2a2f (Data Identifier 1)(Vehicle Manufacturer Specific)
    Data Identifier MSB: 0x2a (Data Identifier 1 MSB)
    Data Identifier LSB: 0x2f (Data Identifier 1 LSB)
    Data Record String: \357\277\275

0000  [redacted]                08 00 45 00   [redacted]
0010  00 38 1e 90 00 00 ff 06  69 f7 c0 a8 58 f9 c0 a8   ·8······  i···X···
0020  58 ee 34 58 fa 09 00 23  18 a8 38 4c 1c 6e 50 18   X·4X···#  ··8L·nP·
0030  15 30 67 cd 00 00 02 fd  80 01 00 00 00 08 [redacted]   ·0g·····  ····[redacted]
0040  [redacted] 62 2a 2f d7                             [redacted]/·
```

Documentation



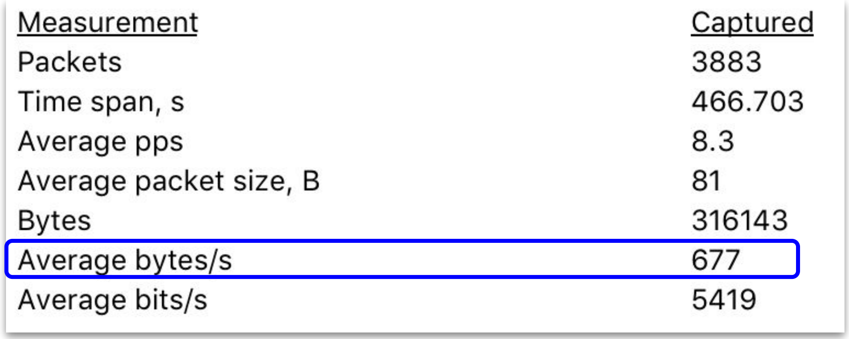
- Every step was documented
- Consolidate all into one **final documentation / report**
- Report needs to be ready for presentations in front of court
- **Answer** stated **questions** e. g.:
    - Who is the attacker?
    - Has someone performed changes to the vehicle?
    - Who performed changes?
    - Etc.
- Make sure **no inconsistencies** are present
- Any third-party should be able to **reproduce** the results

Gap analysis

- No **tamper proof** data storage
- No **standardised EDRs** → Storage of dedicated security events
- General forensic analysis **tooling**
- Forensic analysis **tools for multiple vehicles** and **OEMs**
- **Differences** between **OEMs**
- **Differences** between **models of OEMs**

Opportunities

- **Static memory** for micro-controllers → Use of memory maps
- Limited memory allows **fast acquisition** (depending on the device)
- **Increasing similarities** to general computer systems
- **Processing power** increases
- **Amount of data** sources
- **EDRs** by 2022 in Europe
- **Embedded forensics** is well established
- **Hypervisor**-based controller



Measurement	Captured
Packets	3883
Time span, s	466.703
Average pps	8.3
Average packet size, B	81
Bytes	316143
Average bytes/s	677
Average bits/s	5419

Summary

- **The Protocol:**
  - Connecting vehicles to company networks holds potential security risks
  - Currently malware for vehicles are unknown (yet :-))
  - The effectiveness of security mechanisms of the protocols strongly depend on the implementation of the manufacturer / supplier
- **Automotive Forensics:**
  - Forensic readiness shows a lot of gaps
  - Automotive forensics holds a lot of potential
  - There are a lot of data sources in modern vehicles
  - GDPR compliance will be challenging with regard to future mobility service concepts

Thanks to

Icons provided by:

AlexNordlicht, AliCoskun, AneequeAhmed, artshop, CarinMarzaro, ChoNix, DonBLC, dsathiyaraj, fredley, GraphicTigers, IcoMoon, iconcheese, LibbyVentura, Mello, PedroSantos, PiotrekChuchla, priyanka, Rauan, RoyyanWijaya, Sari, SidiqFathurochman, sultanmohammed, ThreeSixFive, VectorsPoint, yantiani

Thank you for your attention!

Q & A

Christopher Corbett and Kevin Gomez Buquerin