CHALLENGES AND OPPORTUNITIES IN FORENSIC ANALYSIS FOR STATE-OF-THE-ART AND FUTURE VEHICLES

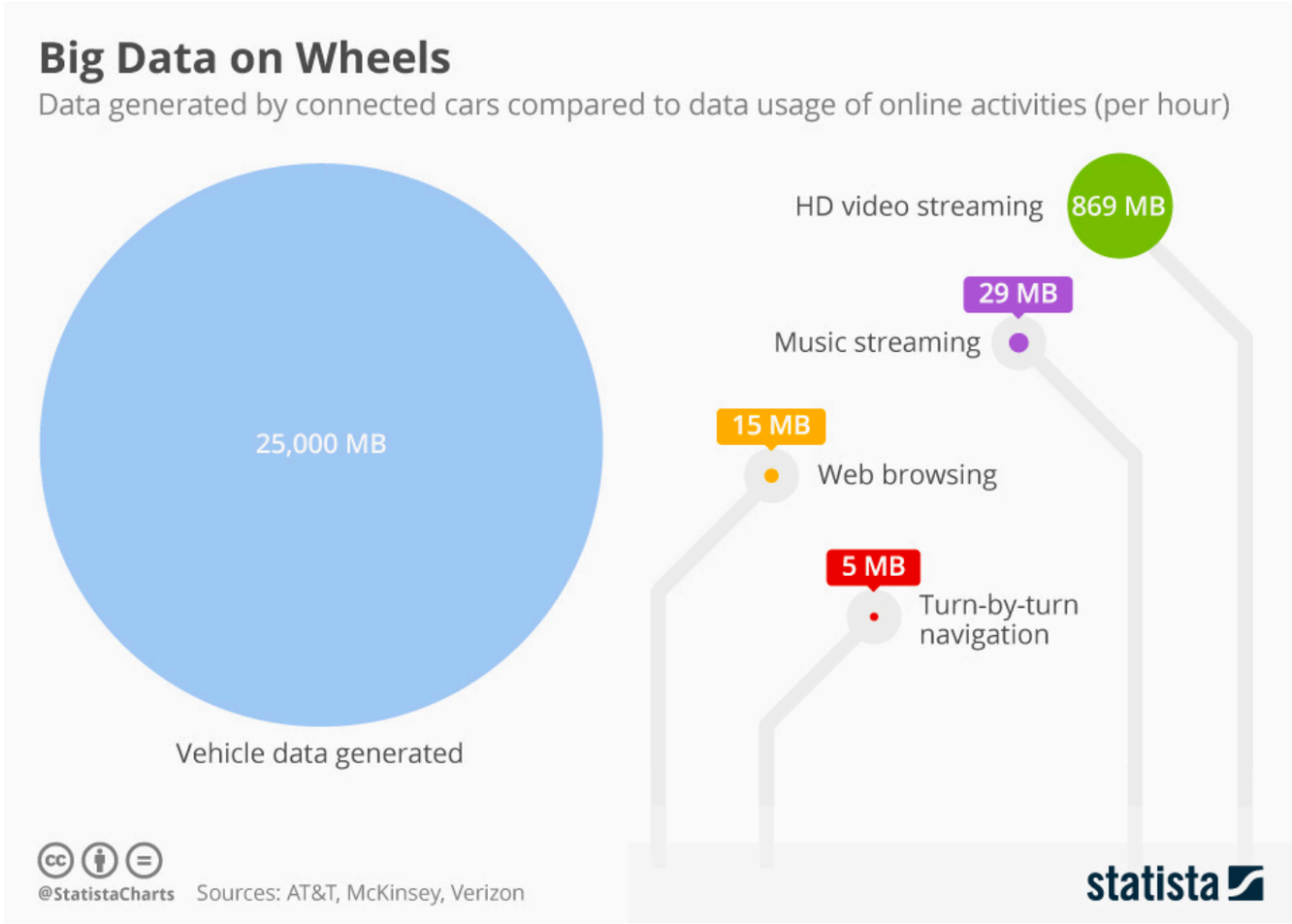
KEVIN GOMEZ BUQUERIN
TECHNICAL UNIVERSITY INGOLSTADT
AUDI AG

WHO AM I

- Kevin Gomez Buquerin
- Incident responder at Audi AG
- Master student at the technical university Ingolstadt
- B.Sc. in computer science for automotive and avionic systems
- Security research for real-time operating systems

WHY DO WE CARE?

- Change of burden of proof
- More mobility services
  - Updates over the air
  - Telematic services
  - Smart home connection
- Increased attack surface — Increased interest of researches/attackers
- Introduce general IT problems to vehicles



Source: https://www.statista.com

FORENSIC ANALYSIS (1)

When?

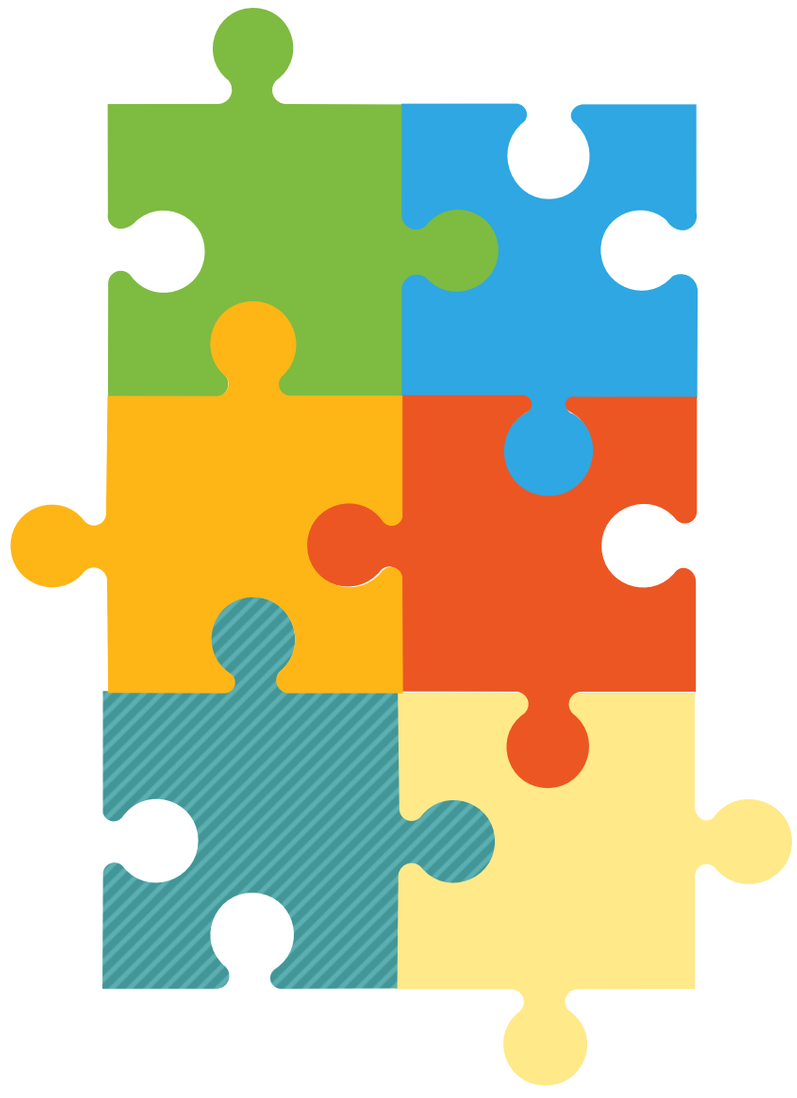
How?

What?

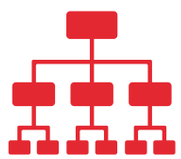
Where?

Who?

Why?



FORENSIC ANALYSIS (2)

- Requirements for forensic analysis:
  - Acceptance 
  - Functionality 
  - Robustness 
  - Reproducibility 
  - Integrity 
  - Consistency 
- Relevant for automotive forensics

ACCEPTANCE

Good

- Standardised interface is used to acquire data (such as OBD)
- Test-analysis were performed successfully

Bad

- No plan

FUNCTIONALITY

Good

- Know what you expect
- Try it first!

Bad

- Conclusions without valid results
- Wrong interpretation

ROBUSTNESS

Good

- Adaptable on different interfaces and interface versions
- Usable for several protocols
- Usable for different models of different OEMs

Bad

- Only works for one OEM
- Only usable with one specific interface on one specific protocol

REPRODUCIBILITY

Good

- Standardised interfaces
- Standardised toolsets

Bad

- Data only acquirable with the right tools

INTEGRITY

Good

- Make copies of memory images
- For court relevant actions: Work in pairs
- Integrity protection on log data

Bad

- Work on original data

CONSISTENCY

Good

- UDS Data Identifier *0xf19a*: Calibration repair shop code changed
- UDS Data Identifier *0xf189*: ECU software version number changed

Bad

- Some error code was thrown which indicates possible modification

RESEARCH CHALLENGES (1)

1. Complexity problem (complex systems and extensive processing of data representations)

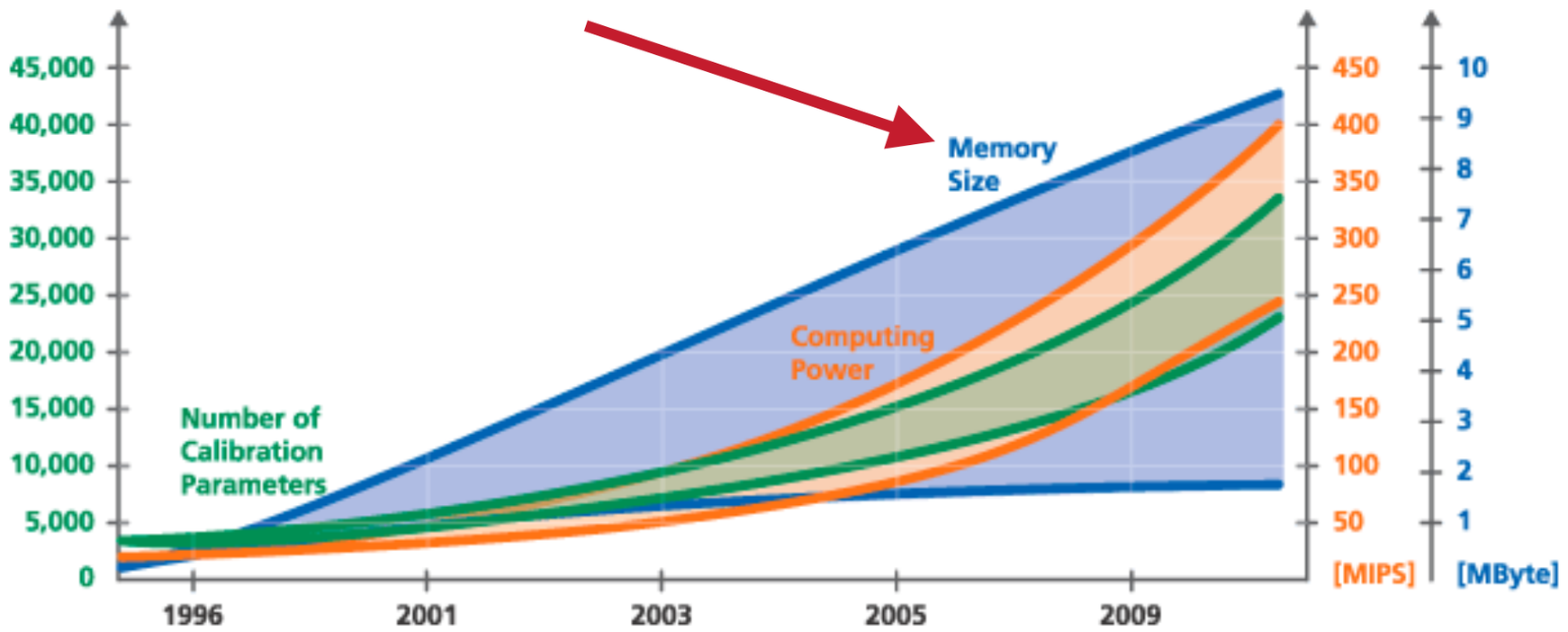
```
▼ Unified Diagnostic Service
    Service Identifier: 0x62 (Read Data By Identifier Positive Response)
    Supress Response: False (0x00)
    Data Identifier: 0x2a2f (Data Identifier 1)(Vehicle Manufacturer Specific)
    Data Identifier MSB: 0x2a (Data Identifier 1 MSB)
    Data Identifier LSB: 0x2f (Data Identifier 1 LSB)
    Data Record String: [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: [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: [redacted]
```

RESEARCH CHALLENGES (2)

2. Diversity problem (big volumes must be separated into smaller chunks)
   - Not relevant since ECU memory is very small compared to personal computers



RESEARCH CHALLENGES (3)

3. Consistency and correlation (multiple data sources need to be correlated)
   - There are a lot of ECUs within a vehicle. Therefore several different data sources are applicable

RESEARCH CHALLENGES (4)

4. Quantity or volume problem (there is a lot of data to analyse)

   - Despite the limited storage power of single ECUs, the number of ECUs do increase the quantity of volume to handle analyse

RESEARCH CHALLENGES (5)

5. Unified time-lining problem (many sources lead to problems with correlating timestamps, etc.)
   - Different interpretation of time over different ECUs.
     Assorted characteristics of precisions

- Usability in court is key!

MORE CHALLENGES

- Tamper-proof extraction of data
- Storage is very small
- GDPR
- Limited processing power
- Accessibility - located at the customer
- Legal basis
- Multiple vendors and suppliers of automotive subsystems

FORENSIC ANALYSIS ON MODERN VEHICLES (1)

1006	79.408035	192.168.88.249	192.168.88.238	UDS	73	Read Data By Identif
1008	79.427141	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identif
1009	79.427496	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message P
1010	79.427731	192.168.88.249	192.168.88.238	UDS	72	Read Data By Identif
1012	79.452597	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identif
1013	79.453027	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message P
1014	79.453539	192.168.88.249	192.168.88.238	UDS	69	Read Data by Identif

▶ Frame 1006: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▶ Ethernet II, Src: [redacted] Dst: [redacted]
▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
▶ Transmission Control Protocol, Src Port: 13400, Dst Port: 64014, Seq: 314, Ack: 197, Len: 19
▼ Diagnostics over Internet Protocol
  Protocol Version: 0x02 (DOIP_2012)
  Protocol Version Inverse: 0xfd
  Message Type: 0x8001 (Diagnostic Message)
  Message Length: 11
  Diagnostic Message Source Address: [redacted]
  Diagnostic Message Target Address: [redacted]
▼ Unified Diagnostic Service
  Service Identifier: 0x62 (Read Data By Identifier Positive Response)
  Supress Response: True (0x80)
  Data Identifier: 0xf189 (Data Identifier 1)(Vehicle Manufacturer ECU Software Version Number Data Identifier)
  Data Identifier MSB: 0xf1 (Data Identifier 1 MSB)
  Data Identifier LSB: 0x89 (Data Identifier 1 LSB)
  Data Record String: [redacted]

FORENSIC ANALYSIS ON MODERN VEHICLES (2)

1594	157.362790	192.168.88.249	192.168.88.238	UDS	91	Read Data By Ident
1596	157.364251	192.168.88.238	192.168.88.249	UDS	69	Read Data by Ident
1597	157.364594	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message
1598	157.373142	192.168.88.249	192.168.88.238	UDS	75	Read Data By Ident
1601	157.637535	192.168.88.238	192.168.88.249	UDS	68	Diagnostic Session
1602	157.638107	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message
1603	157.649016	192.168.88.249	192.168.88.238	UDS	72	Diagnostic Session

▶ Frame 1594: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▶ Ethernet II, Src: [redacted], Dst: [redacted]
▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
▶ Transmission Control Protocol, Src Port: 13400, Dst Port: 64037, Seq: 109, Ack: 99, Len: 37
▼ Diagnostics over Internet Protocol
  Protocol Version: 0x02 (DOIP_2012)
  Protocol Version Inverse: 0xfd
  Message Type: 0x8001 (Diagnostic Message)
  Message Length: 29
  Diagnostic Message Source Address: [redacted]
  Diagnostic Message Target Address: [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_ThermContr[redacted]

FORENSIC ANALYSIS ON MODERN VEHICLES (3)

1044	80.297394	192.168.88.249	192.168.88.238	UDS	75	Read Data By Identifier Positive Res
1048	80.324340	192.168.88.249	192.168.88.238	UDS	75	Read Data By Identifier Positive Res
1052	80.345281	192.168.88.249	192.168.88.238	UDS	73	Read Data By Identifier Positive Res
1056	80.413411	192.168.88.249	192.168.88.238	UDS	518	Read Data By Identifier Positive Res
1060	80.503640	192.168.88.249	192.168.88.238	UDS	80	Read Data By Identifier Positive Res

```
▶ Frame 1044: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
▶ Ethernet II, Src: [redacted] Dst: [redacted]
▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
▶ Transmission Control Protocol, Src Port: 13400, Dst Port: 64014, Seq: 673, Ack: 332, Len: 21
▼ Diagnostics over Internet Protocol
    Protocol Version: 0x02 (DOIP_2012)
    Protocol Version Inverse: 0xfd
    Message Type: 0x8001 (Diagnostic Message)
    Message Length: 13
    Diagnostic Message Source Address: [redacted]
    Diagnostic Message Target Address: [redacted]
▼ Unified Diagnostic Service
    Service Identifier: 0x62 (Read Data By Identifier Positive Response)
    Supress Response: True (0x80)
    Data Identifier: 0xf19a (Data Identifier 1)(Calibration Repair Shop Code Or Calibration Equipment Serial Number Data Identifier)
    Data Identifier MSB: 0xf1 (Data Identifier 1 MSB)
    Data Identifier LSB: 0x9a (Data Identifier 1 LSB)
    Data Record String: [redacted]
```

FORENSIC ANALYSIS ON MODERN VEHICLES (3)

1850	166.279147	192.168.88.249	192.168.88.238	UDS	73	Read Data By Identifier P
1852	166.334229	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1853	166.334380	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positi
1854	166.340480	192.168.88.249	192.168.88.238	UDS	69	Read Data by Identifier N
1856	166.503532	192.168.88.249	192.168.88.238	UDS	73	Read Data By Identifier P
1859	166.566379	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1860	166.567745	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positi
1861	166.574303	192.168.88.249	192.168.88.238	UDS	69	Read Data by Identifier N
1863	166.724645	192.168.88.249	192.168.88.238	UDS	73	Read Data By Identifier P

```
▶ Frame 1850: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▶ Ethernet II, Src: [redacted] Dst: [redacted]
▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
▶ Transmission Control Protocol, Src Port: 13400, Dst Port: 64037, Seq: 2207, Ack: 838, Len: 19
▼ Diagnostics over Internet Protocol
    Protocol Version: 0x02 (DOIP_2012)
    Protocol Version Inverse: 0xfd
    Message Type: 0x8001 (Diagnostic Message)
    Message Length: 11
    Diagnostic Message Source Address: [redacted]
    Diagnostic Message Target Address: [redacted]
▼ Unified Diagnostic Service
    Service Identifier: 0x62 (Read Data By Identifier Positive Response)
    Supress Response: False (0x00)
    Data Identifier: 0x6506 (Data Identifier 1)(Vehicle Manufacturer Specific)
    Data Identifier MSB: 0x65 (Data Identifier 1 MSB)
    Data Identifier LSB: 0x06 (Data Identifier 1 LSB)
    Data Record String: [redacted]
```

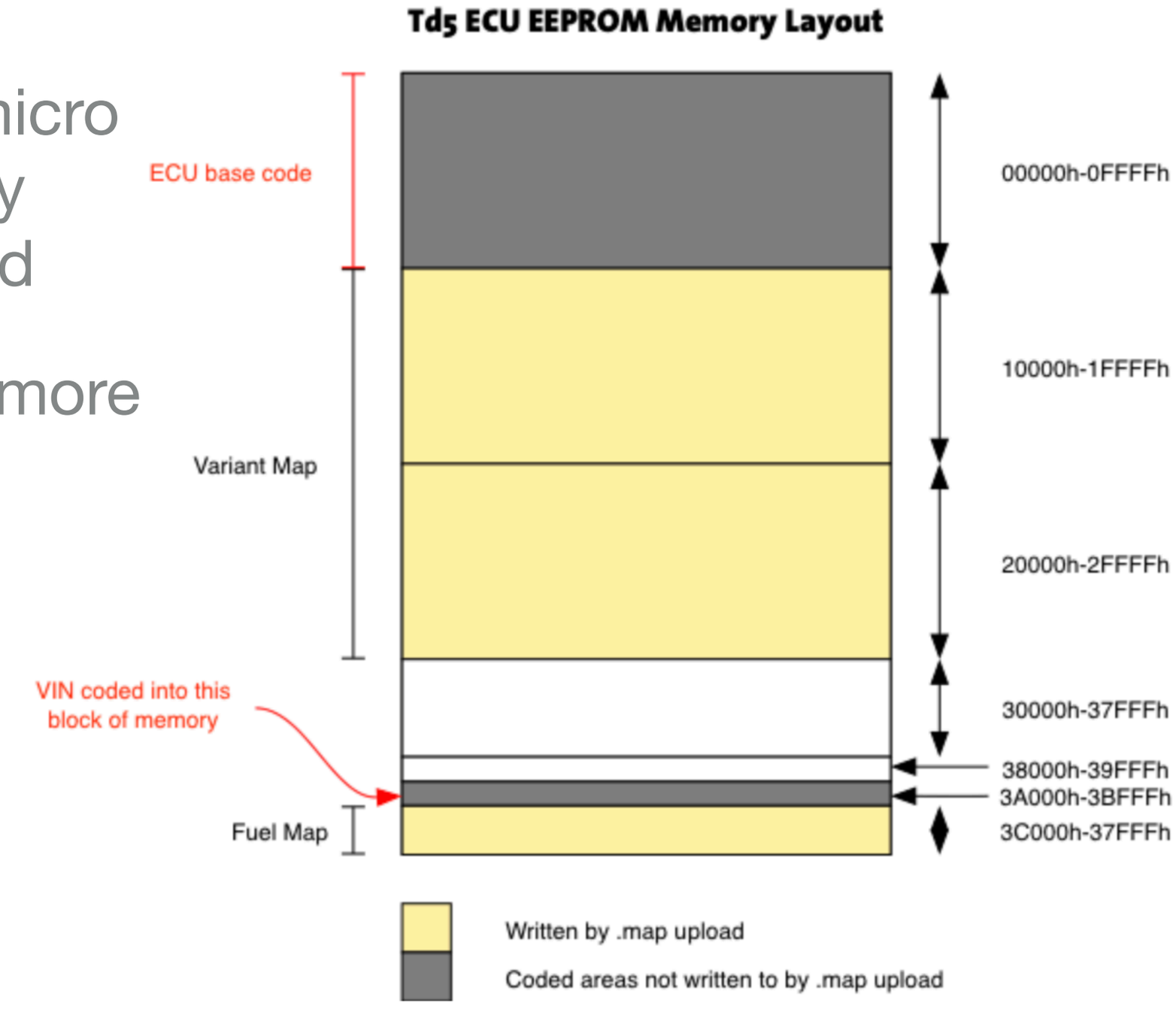
FURTHER SOURCES IN MODERN VEHICLES

- Presence of OBD trouble codes
- OEM backend
- Smartphone data
- Dash-Cams
- Embedded forensic on controller themselves

Problem: No EDR or dedicated storage for forensic data

OPPORTUNITIES (1)

- Static memory for micro controllers - Memory maps can be created
  - (!) ASLR become more and more a thing



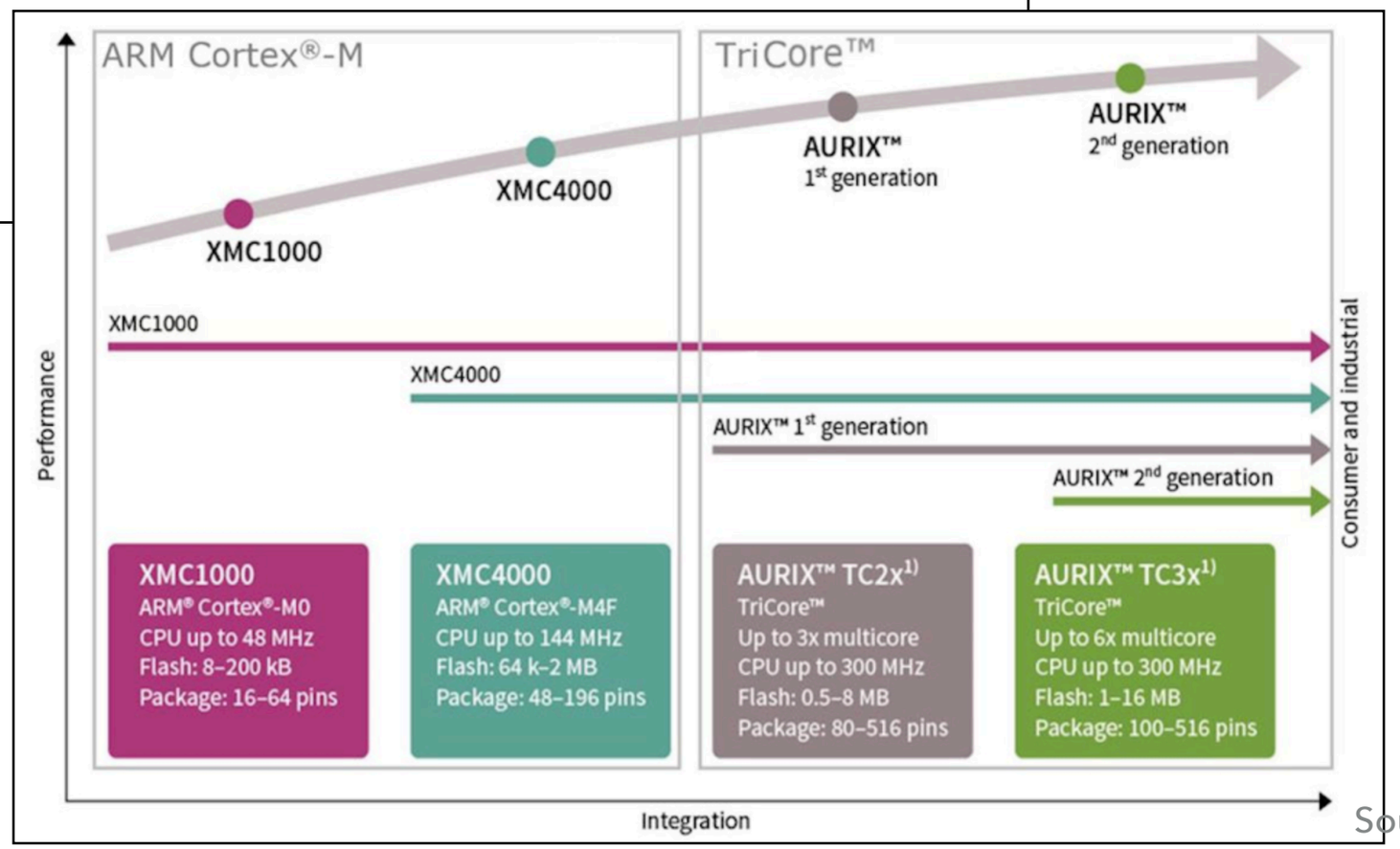
Source: http://www.discotd5.com

OPPORTUNITIES (2)

- Limited memory (depending on the device) and increasing processing power increases (automotive ethernet)

New Infineon System Basis Chips are the first to allow high speed communication with up to 5 Mbit/s

Sep 3, 2018 | Market News



Source: https://www.infineon.com

OPPORTUNITIES (3)

- A lot of data sources
  - E.g. a standard diagnostic trace create ~3900 unique packets over ~8 minutes

Measurement	Captured	Displayed
Packets	3883	3883 (100.0%)
Time span, s	466.703	466.703
Average pps	8.3	8.3
Average packet size, B	81	81
Bytes	316143	316143 (100.0%)
Average bytes/s	677	677
Average bits/s	5419	5419

- Need for EDRs by 2022 in Europe

OPPORTUNITIES (4)

- Embedded forensic techniques well established
- Increasing similarities to general computer systems
- Hypervisor-based controller

DESIGNLINES | AUTOMOTIVE DESIGNLINE

Platform Brings Hypervisor & Virtualization to Automotive

By Christoph Hammerschmidt, EE Times Europe, 01.06.14 0

Share Post Share on Facebook Share on Twitter

At this year's Consumer Electronics Show (CES) in Las Vegas, Harman showcases a scalable platform for in-vehicle infotainment in the connected car. The platform transplants concepts known from commercial and consumer computing -- such as hypervisors and virtual systems -- to automotive environments. Plus, it takes care about cyber security and eases system integration in vehicles.

Source: https://www.eetimes.com

OPEN QUESTIONS

- Who should gather, store, and analyse the data?
- Involvement of the driver if an incident occurs?
- Standardised storage system over all OEMs for relevant data?
- Event-based or store everything?

Thank you for your attention!

Q&A

@kgbuquerin