Automotive Ethernet Fuzzing: From Purchasing ECU to SOME/IP Fuzzing

Jonghyuk Song, Soohwan Oh, Woongjo Choi
AUTOCRYPT

Who are we?

AUTOCRYPT a Mobility Security Company for Autonomous, Connected Vehicles, and Beyond

- Jonghyuk Song (jhsong@autocrypt.io)
  - AUTOCRYPT Red Team leader, automotive cyber security researcher
  - Offensive security researcher, CTF player (Defcon CTF Finalist 2009, 2011, 2017)
- Soohwan Oh
  - Automotive engineer and security tester at AUTOCRYPT
  - Experts for fuzzing test and issue analysis on the in-vehicle networks
- Woongjo Choi
  - AUTOCRYPT Blue Team leader, automotive security tester
  - Software test expert : vehicle, mobile, application processor, ultrasound system, etc.

This talk is for

- How to setup test environment with real ECUs?
- How to do Automotive Ethernet fuzzing on the ECU?

→ A practical guide to SOME/IP fuzzing with the real ECUs.

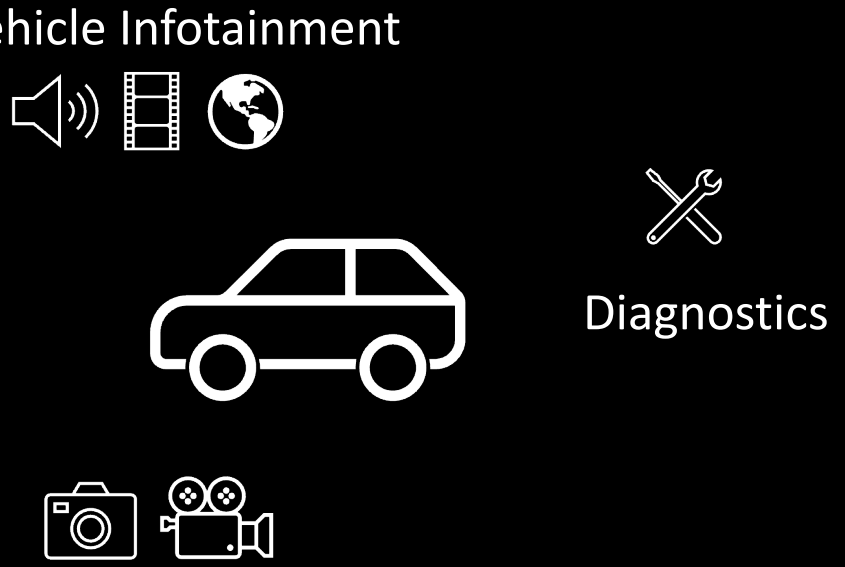
Advent of Automotive Ethernet

Higher data bandwidth is required for ADAS, infotainment, …

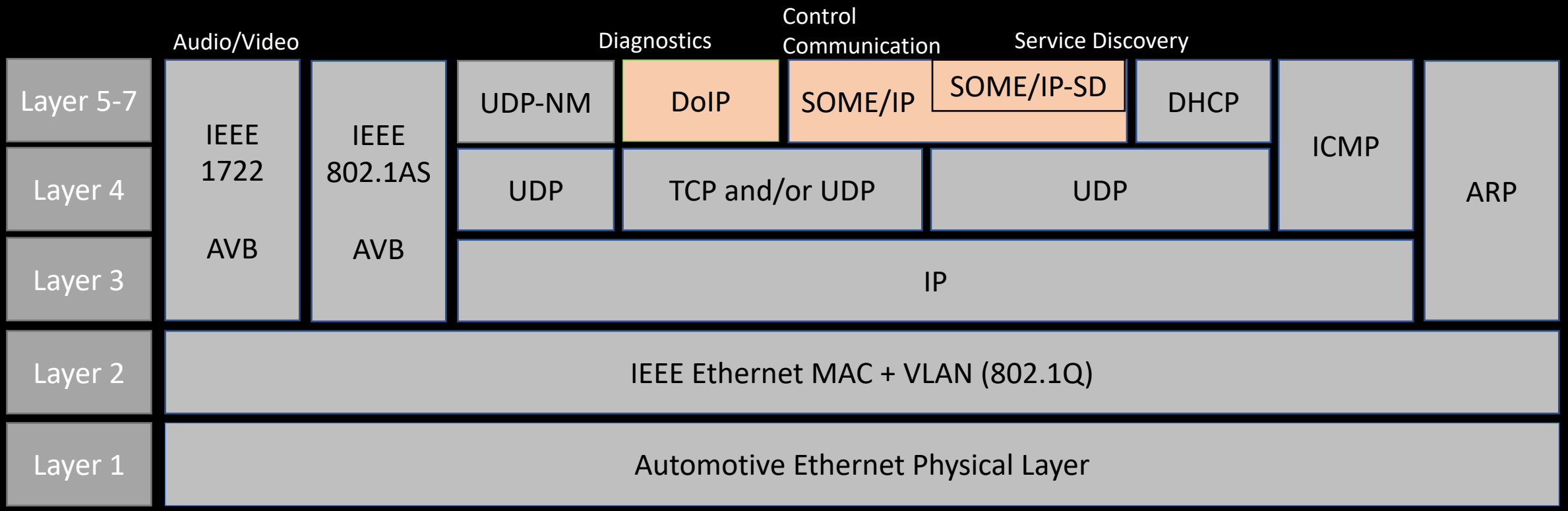
CAN is not enough to handle it.

Automakers have started to adopt Automotive Ethernet.

- BMW X3, X4, X5, i3, i8, …
- Jaguar XJ, XF, …
- Volkswagen Passat



Automotive Ethernet Protocols



- SOME/IP (Scalable service-Oriented MiddlewarE over IP)
  - Control communication protocol between ECUs. (RPC, event notifications)

- DoIP (Diagnostics Over IP)
  - Automotive diagnostic protocol based on IP

Dr. Lars Völker, BMW Group, Communication Protocols for Ethernet in the vehicle, 2013

Automotive Ethernet Fuzzing?

Automotive Ethernet has not yet been tested enough.

→Let’s do SOME/IP fuzzing!

→ Is it essential buying a car?

Let’s test on ECU

It’s expensive to buy a whole car for every single test.

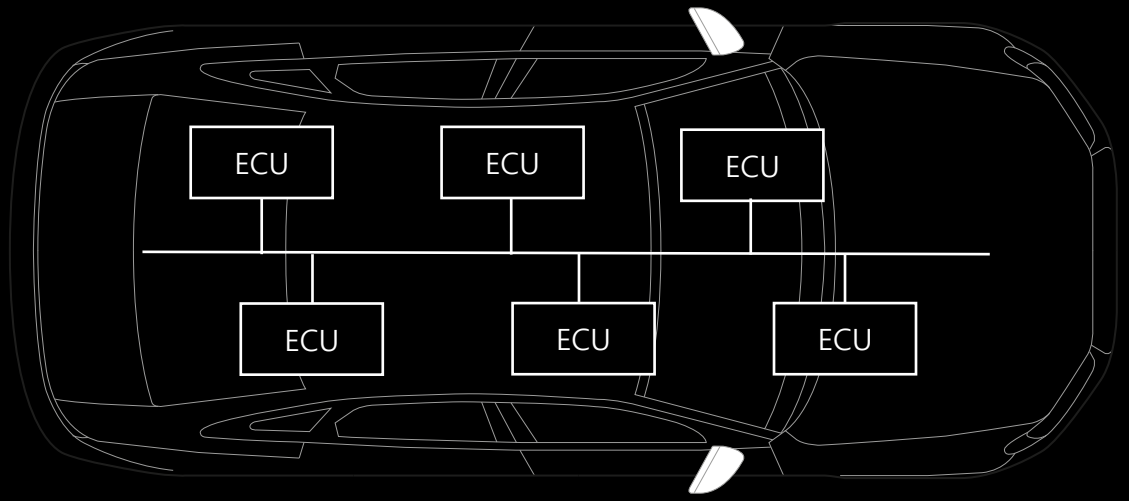
→ Let’s hack an ECU first!

How?

Where can we buy?

Which ECU is proper for test?

Then how to setup?



* ECU: Electric Control Unit

Procedures

1. Select ECU
2. Buy ECU
3. Setup test environment
4. Network configuration for SOME/IP
5. Discovery SOME/IP services
6. Fuzzing

Select ECU

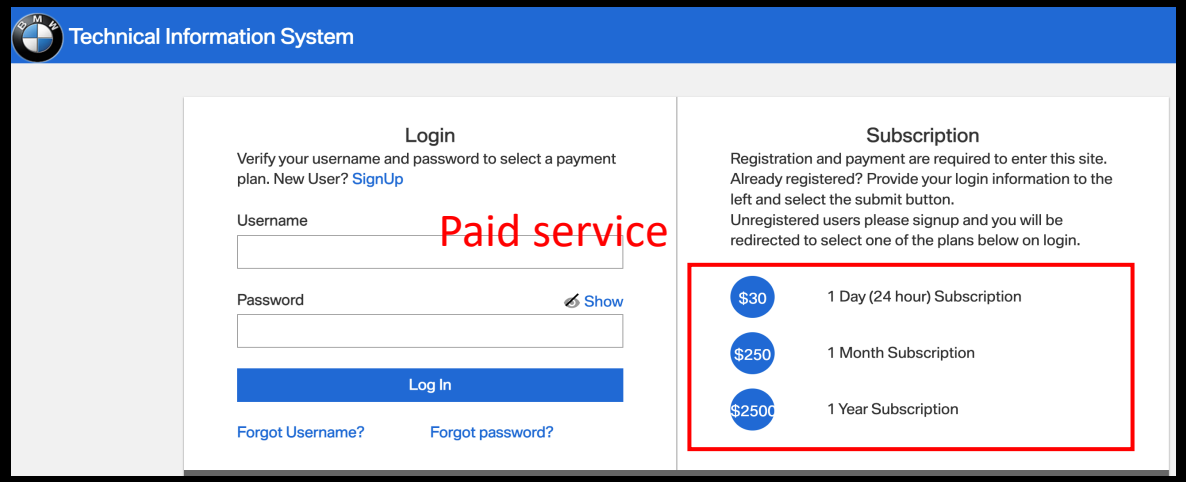
ECU Survey & Selection

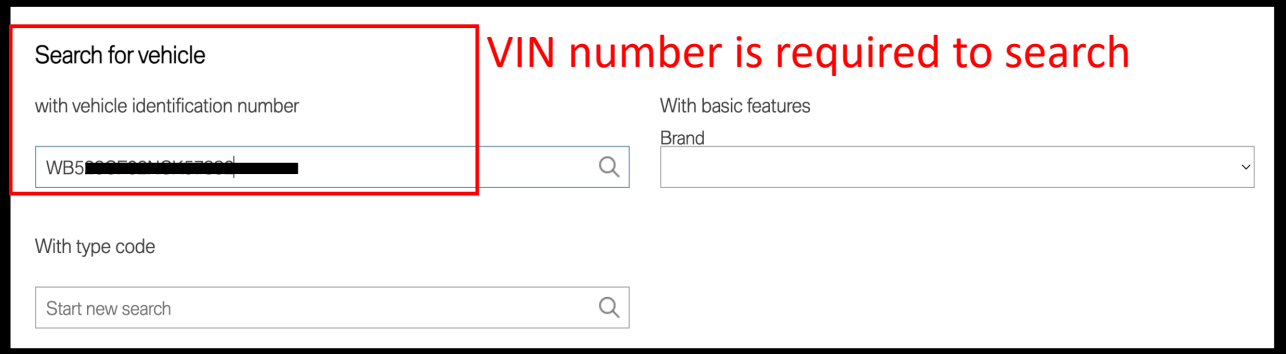
- We chose a BMW iX head unit ECU.
  - Most head unit ECU support Automotive Ethernet.

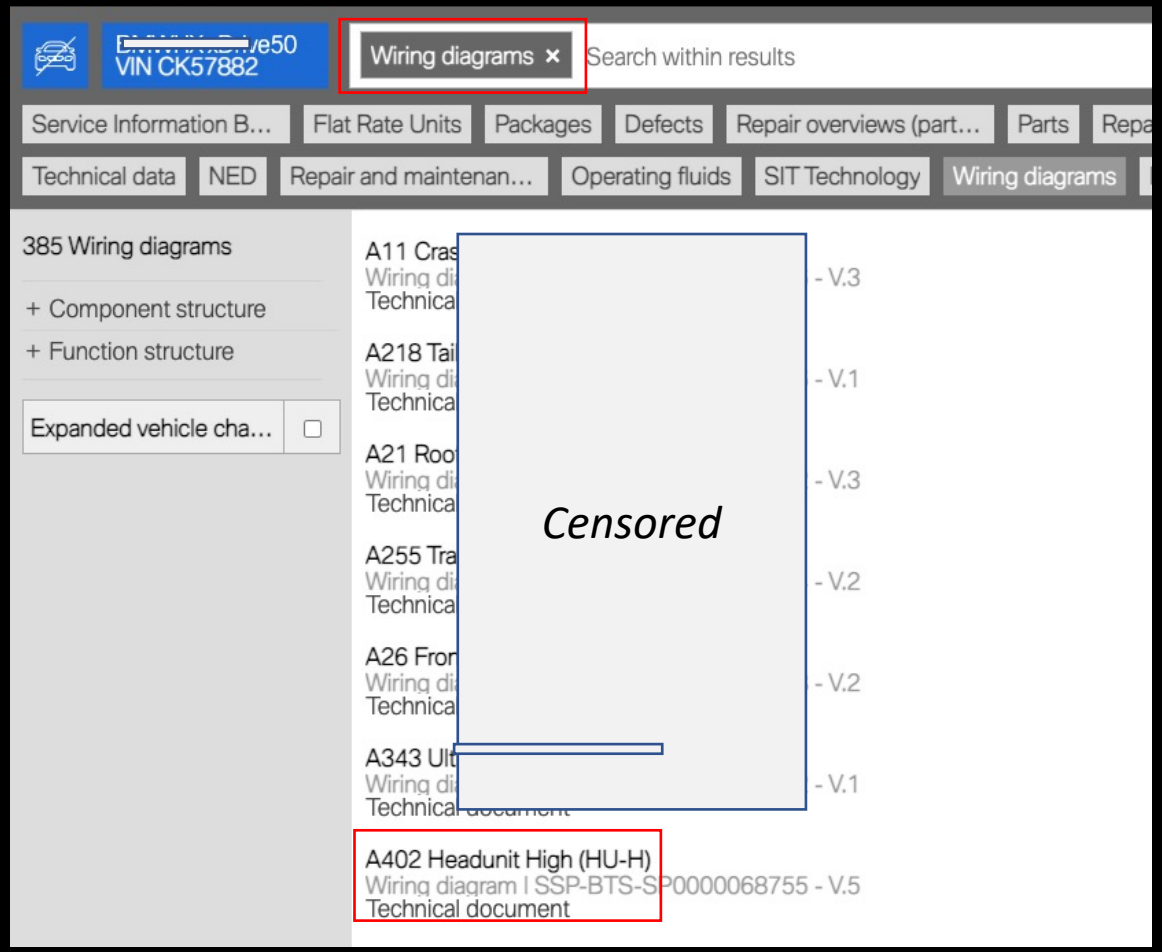
- Why BMW?
  - Automotive Ethernet industry leader
    - First automaker to use Ethernet in a production vehicle.

      (X5 model uses Ethernet in camera system at 2013)
    - BMW provides ECU info on TIS (Technical Information System)
      - wiring diagrams, pin map, connector, basic info, …

BMW Technical Information System







www.bmwtis.com

Google serves various VIN numbers

Google

bmw ix vin number

https://www.dealerrater.com › classifieds › 2022-BMW-...

2022 BMW iX, new, $97570 VIN WB[redacted]

See the new 2022 **BMW iX** priced at $97570. The iX with a **VIN** of WB[redacted] located in Chandler, AZ, has 0 miles, is Storm Bay Metallic with a ...

★★★★☆ 평점: 3.7 · 리뷰 719개



https://www.youcanic.com › vehicle › where-vin-numb...

Where is the VIN number on a BMW? - YOUCANIC

2022. 6. 2. — **BMW** Vehicle Identification **Number** (**VIN**) can be found printed in several locations on the vehicle.



Google 홈페이지로

https://vehicleidentificationnumber.com › bmw

BMW - Vehicle Identification Number

Additionally, you can find the **VIN** at various locations on your car. Frequently you can find your **VIN number** in one of the following locations: on the driver's ...

https://www.group1auto.com › details › vin=WB533CF...

New 2023 BMW iX M60 - VIN: WB[redacted]

2022 BMW iX

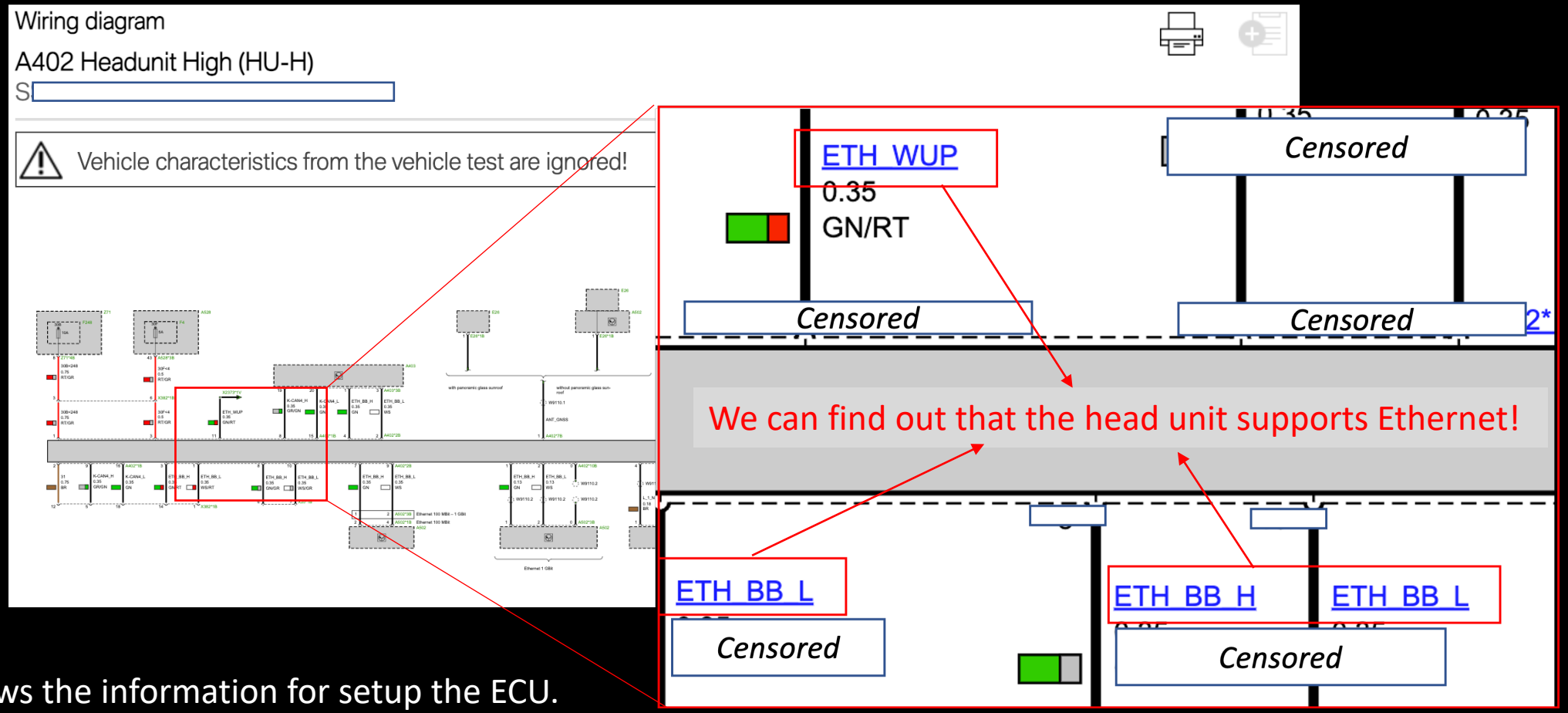
$91,245 • new



Basics

Condition	New
Interior Color	Black
Exterior Color	Sophisto
Drivetrain	All-Wheel Drive
Transmission	Automatic
Fuel	Electric
Engine	Electric
VIN	WB[redacted]
Stock Number	CK57882
Mileage	0

Wiring Diagram



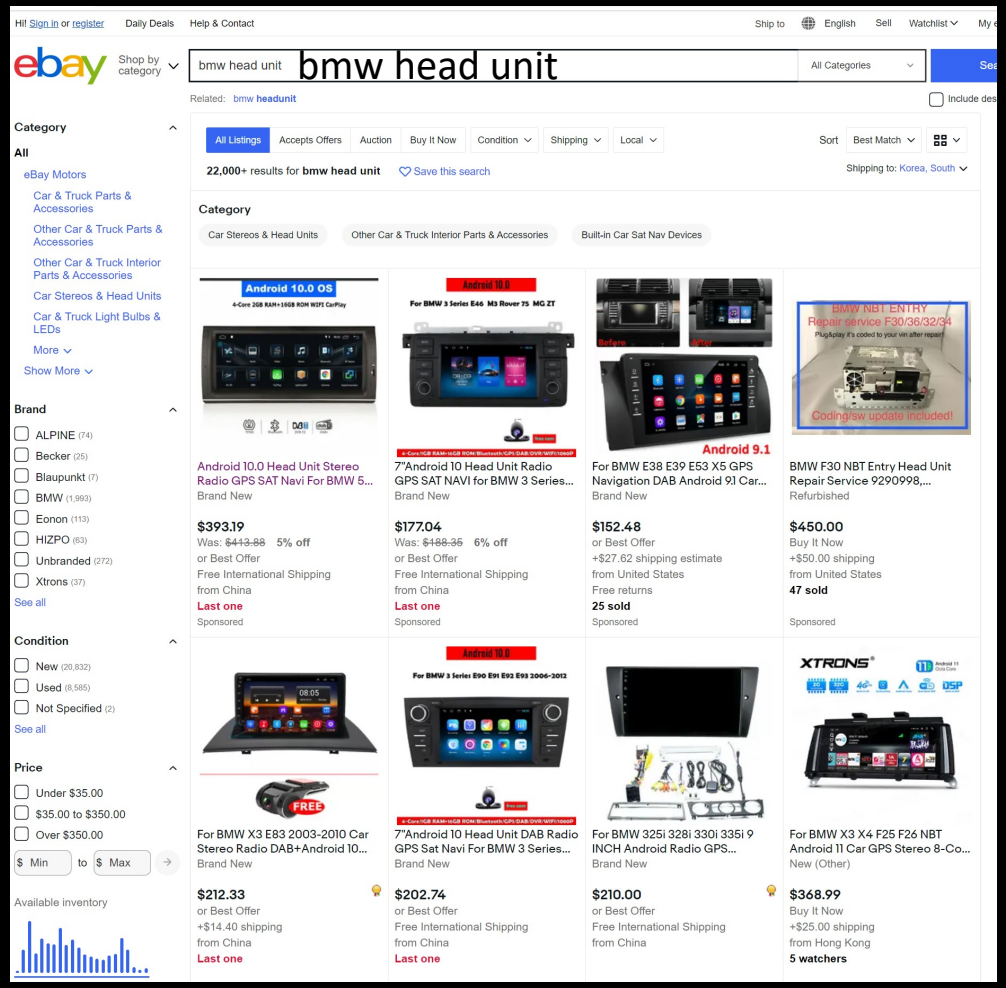
Wiring diagram shows the information for setup the ECU.
power, ground, ETH, …

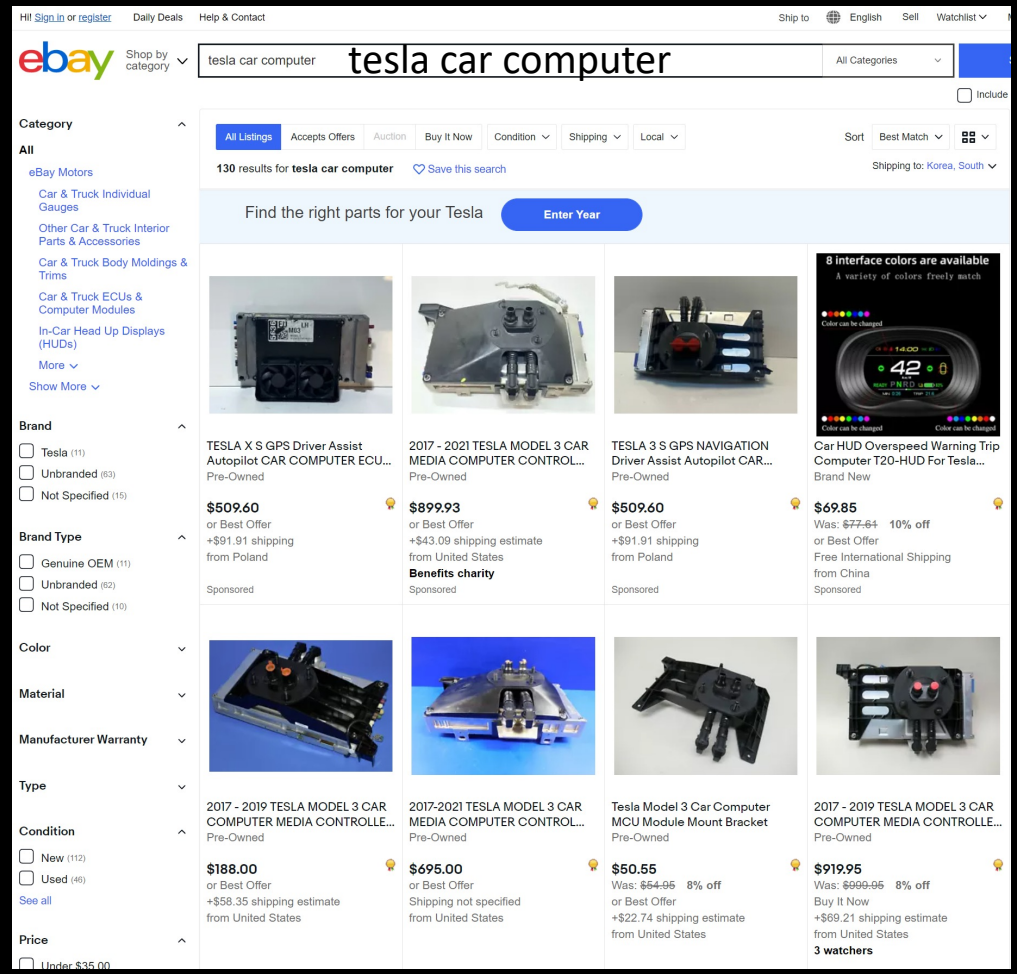
Buy ECU

Gain ECUs from real automakers

- In South Korea,
  - BMW
    - Some service centers sell ECUs.
    - We searched the BMW service centers from BMW Korea homepage → Phone call → Buy
  - Tesla
    - Service centers sell ECUs but not as an individual unit.
    - The ECUs should be installed in the car.
  - Hyundai
    - Hyundai Mobis agency sells ECUs.

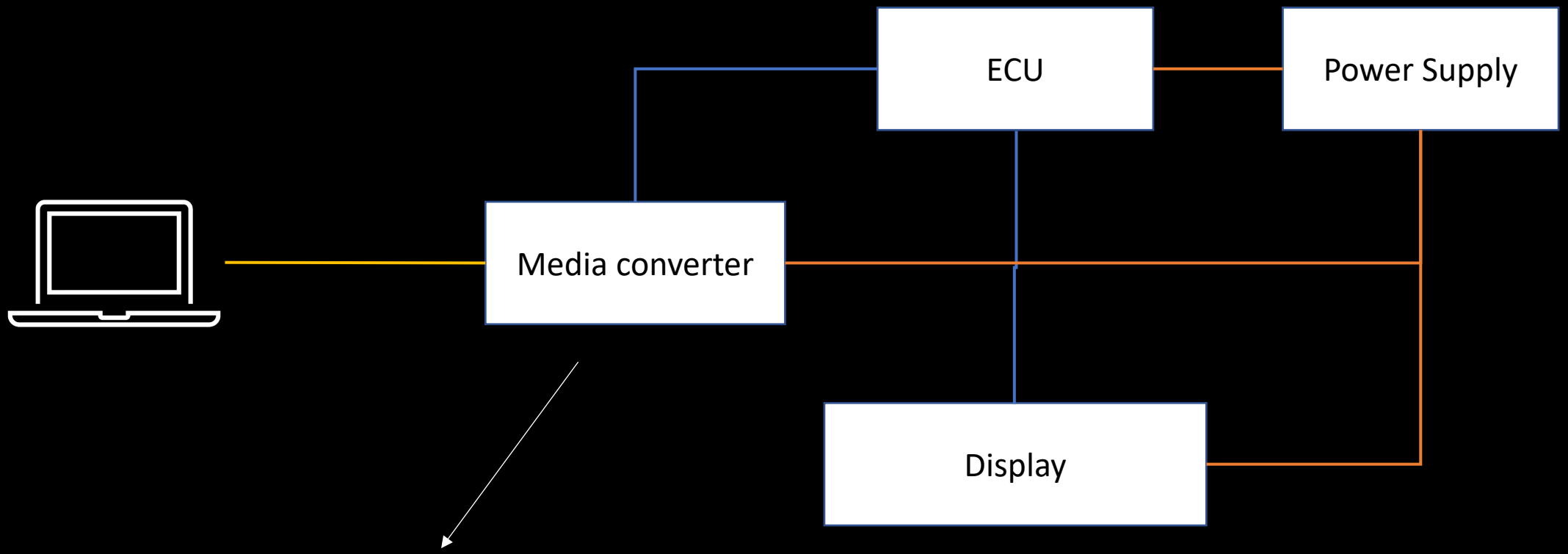
Used ECUs are able to obtain from eBay



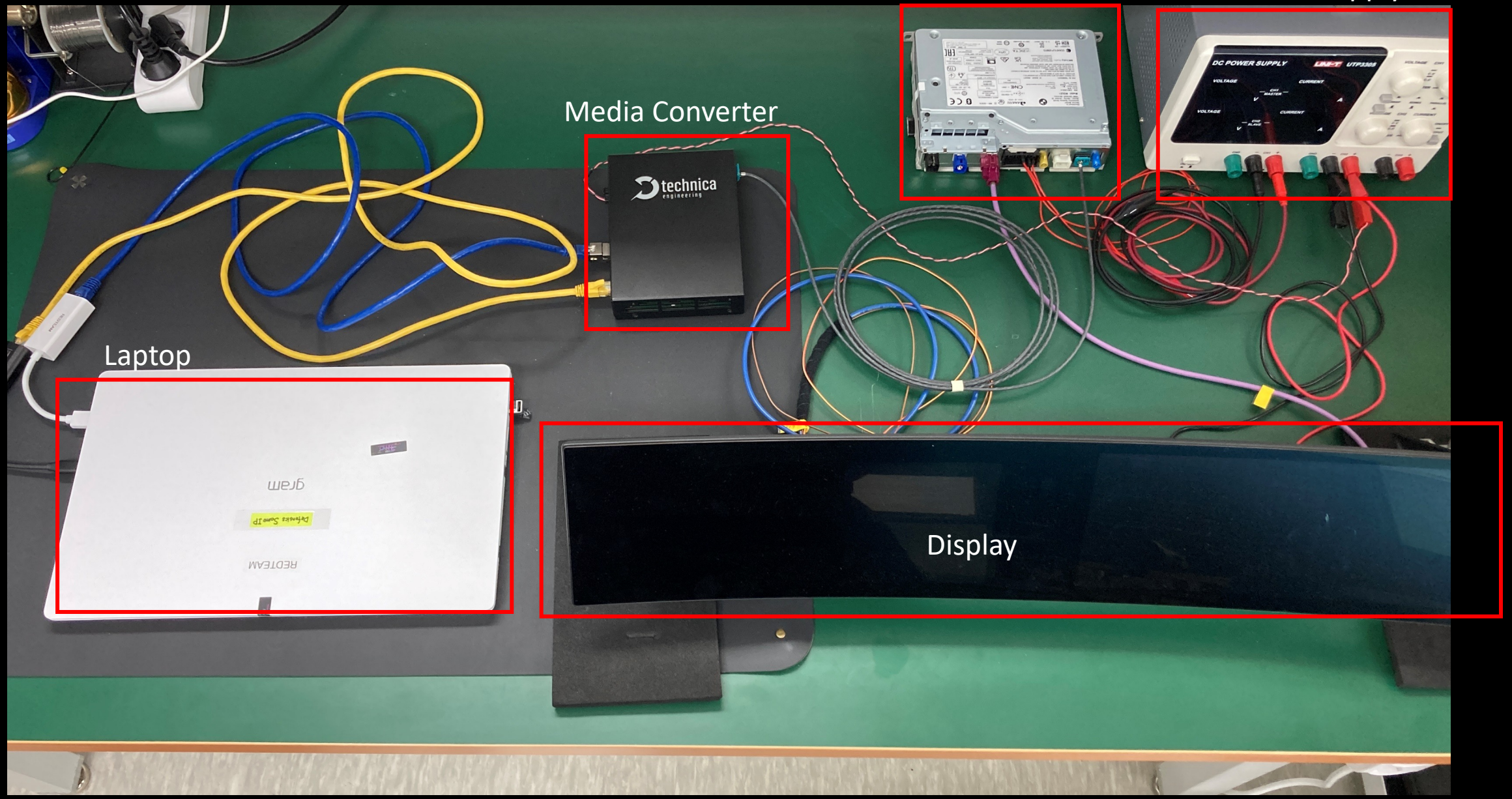


Setup Test Environment

Overview

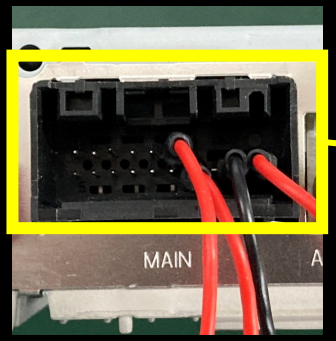


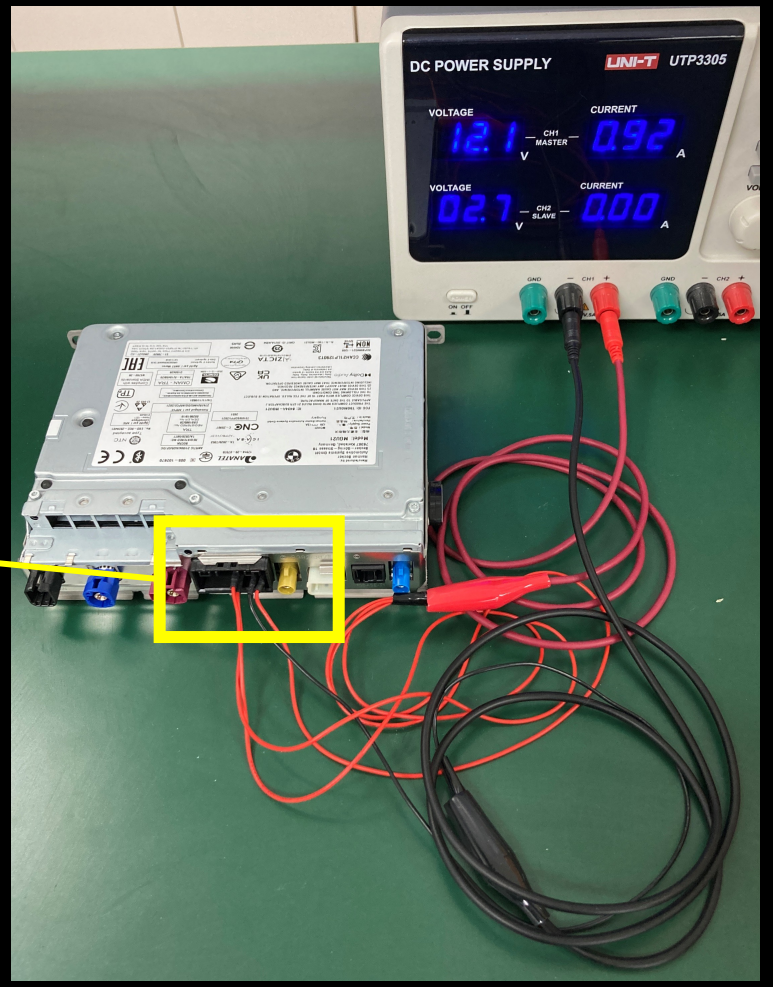
Conversion between Automotive Ethernet and standard Gigabit Ethernet


ECU
Power Supply
Media Converter
technica
engineering
DC POWER SUPPLY
Laptop
gram
Display

Connect power to ECU

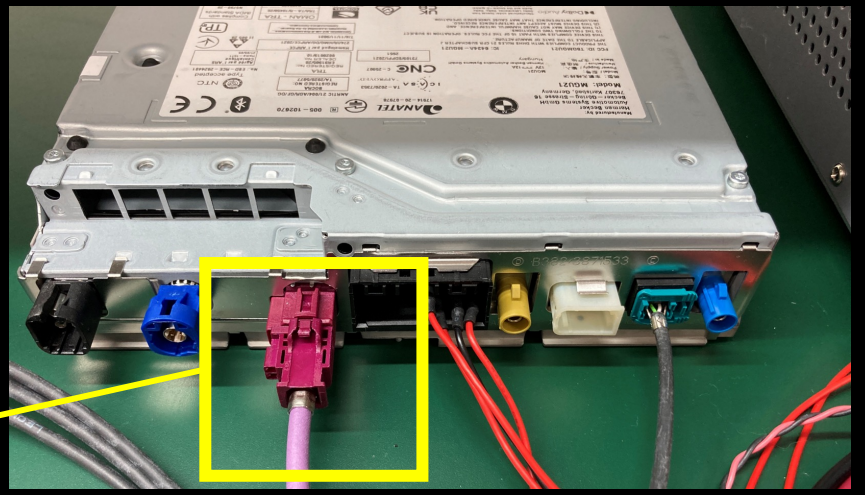
- Red (+)
  - Power (12V)
  - Ethernet wake up (12V)
- Black (-)
  - Ground

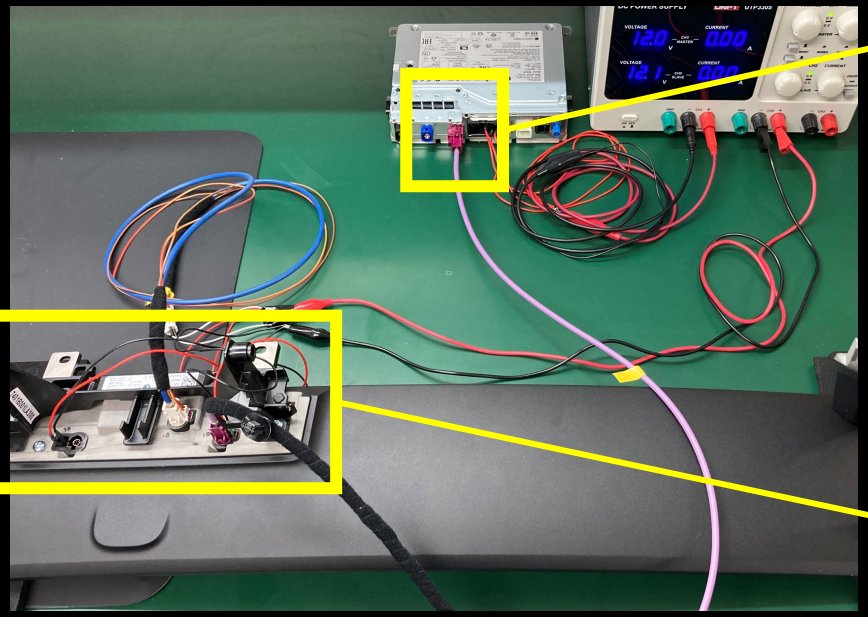


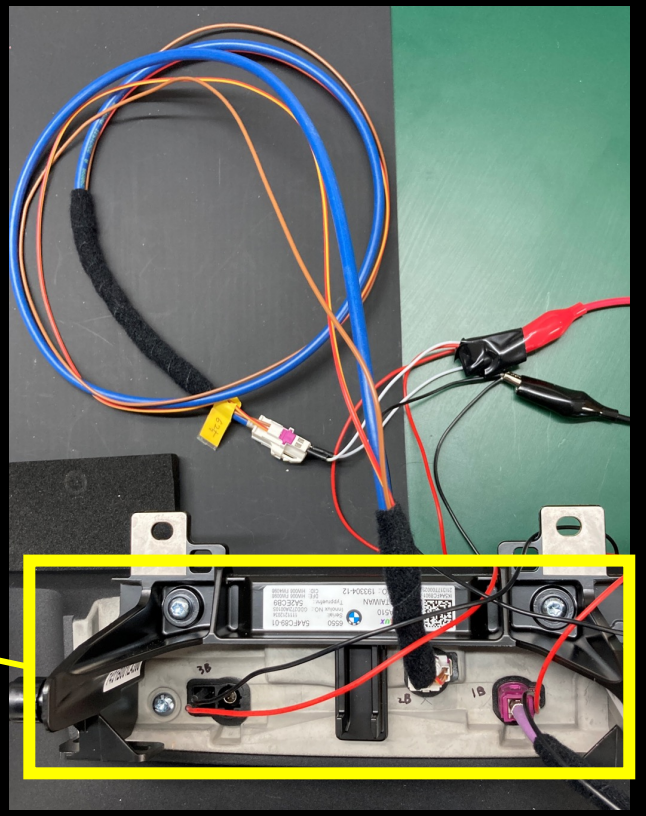


You can check the pin map from TIS.

Setup display



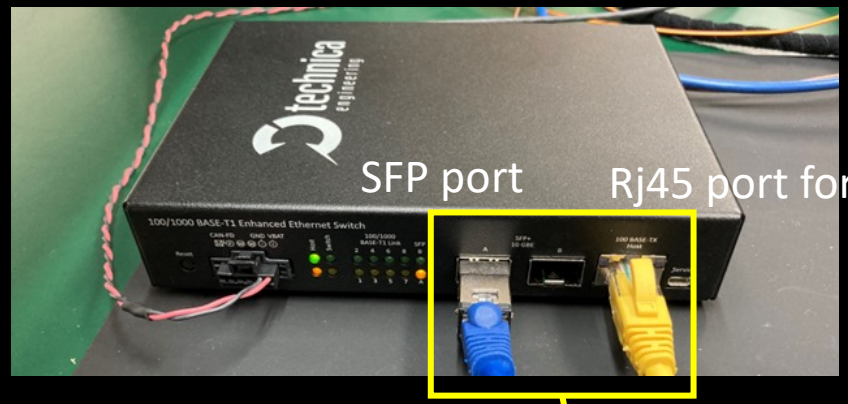




Power On!

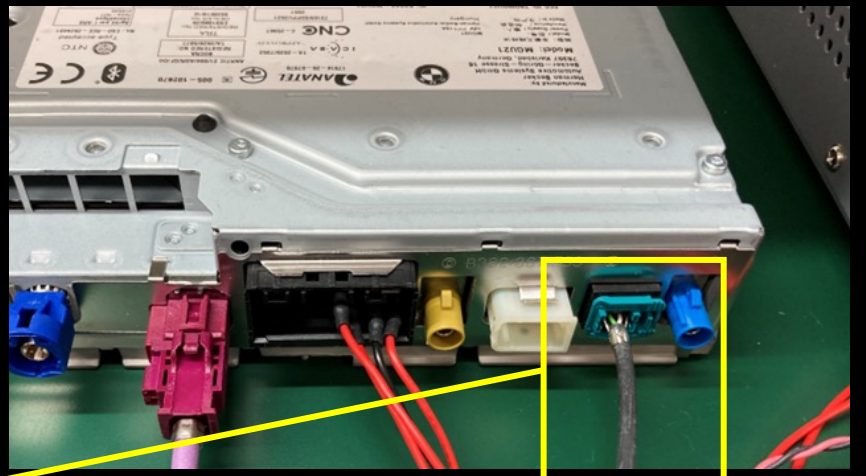

DC POWER SUPPLY
LINI-T UTP3305
VOLTAGE
CURRENT
12.0
1.34
12.0
0.51
BMW

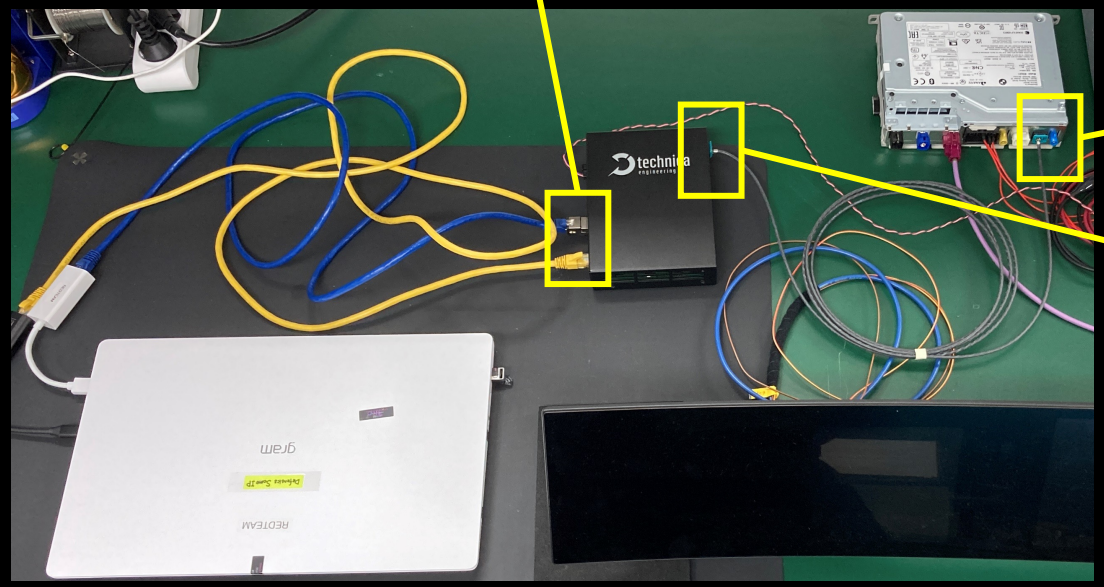
ECU – Media Converter – Laptop

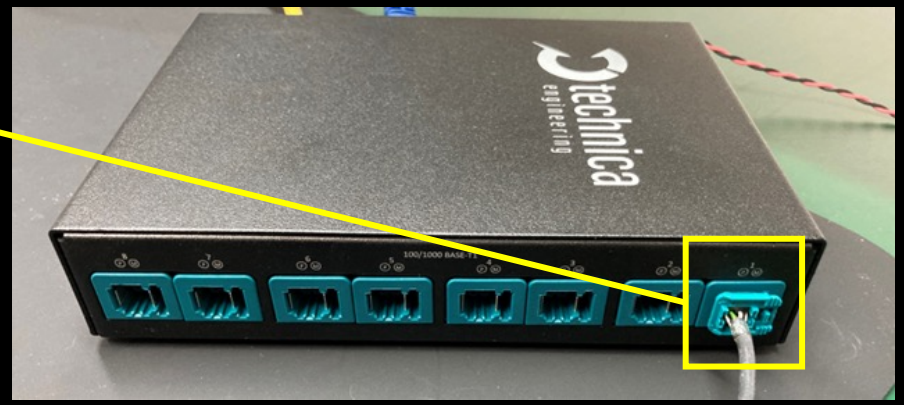


SFP port

Rj45 port for control page



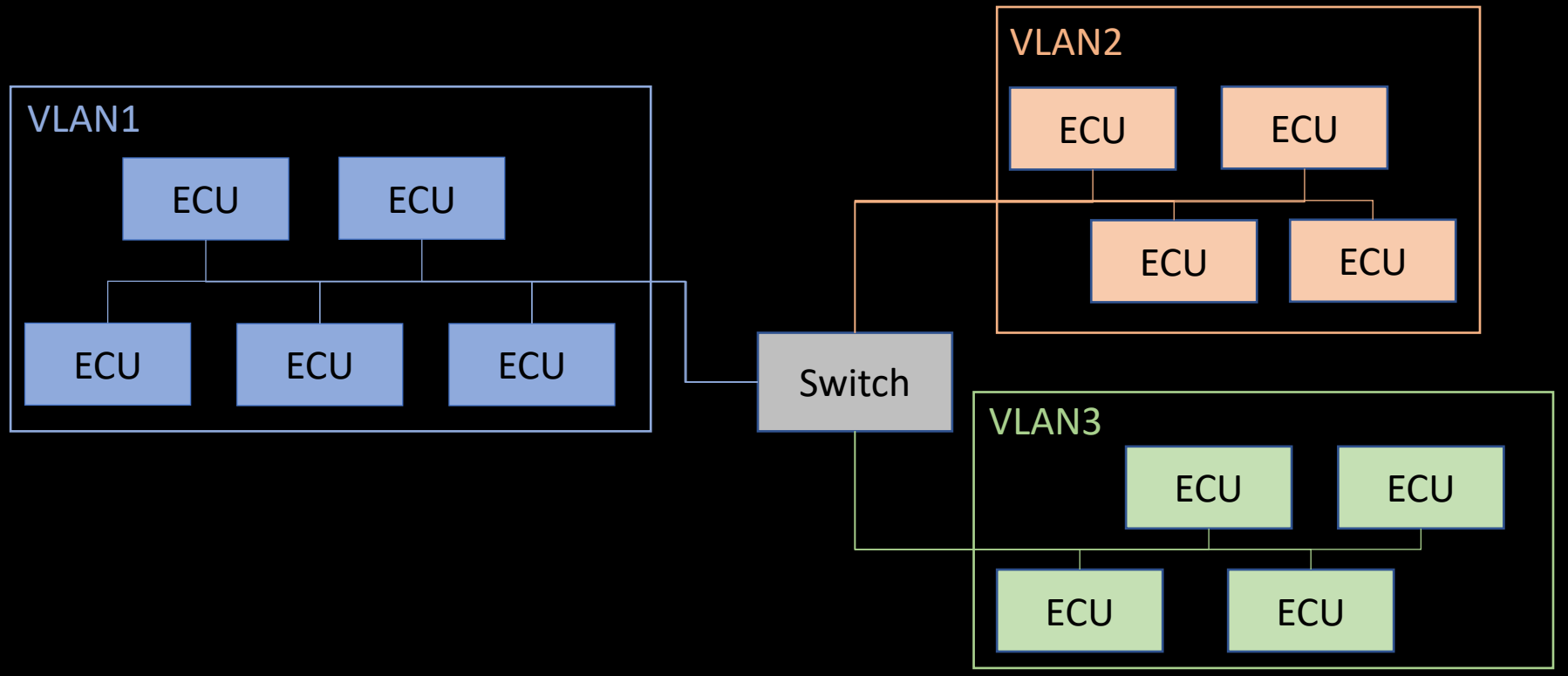




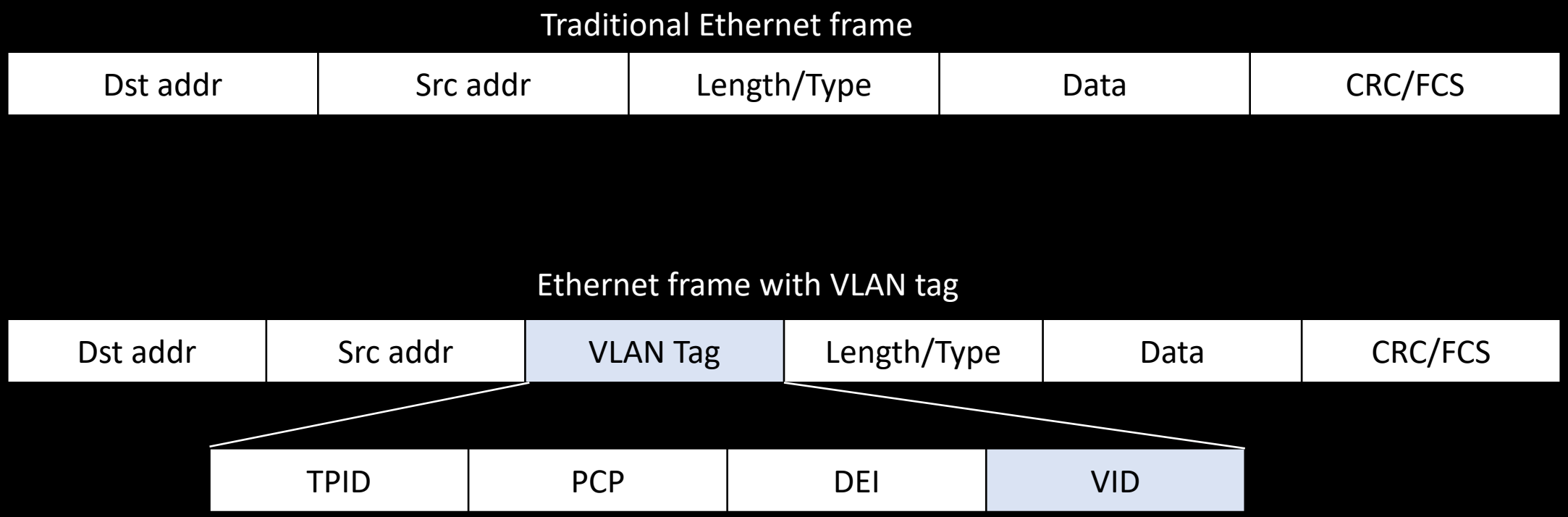
Network Configuration for SOME/IP

Virtual LAN (VLAN) for Automotive Ethernet

- Automotive Ethernet uses VLAN to separate in-vehicle network logically.



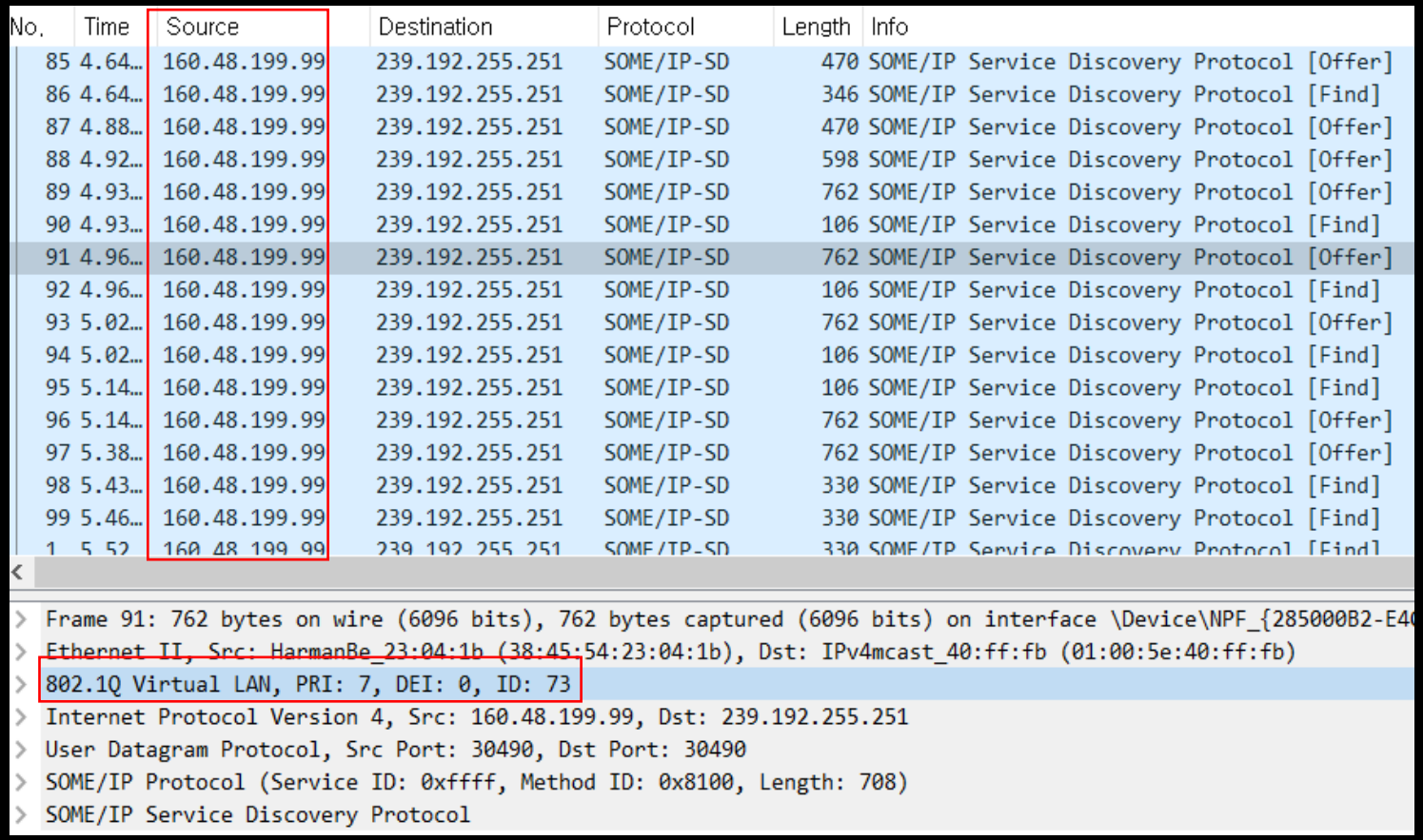
Virtual LAN (VLAN) for Automotive Ethernet



How to know IP and VLAN ID?

Wireshark shows IP and VLAN ID.

(Some USB to Ethernet adapter doesn't show VLAN ID. If you can't see VLAN ID, it will be a good idea to change the adapter.)



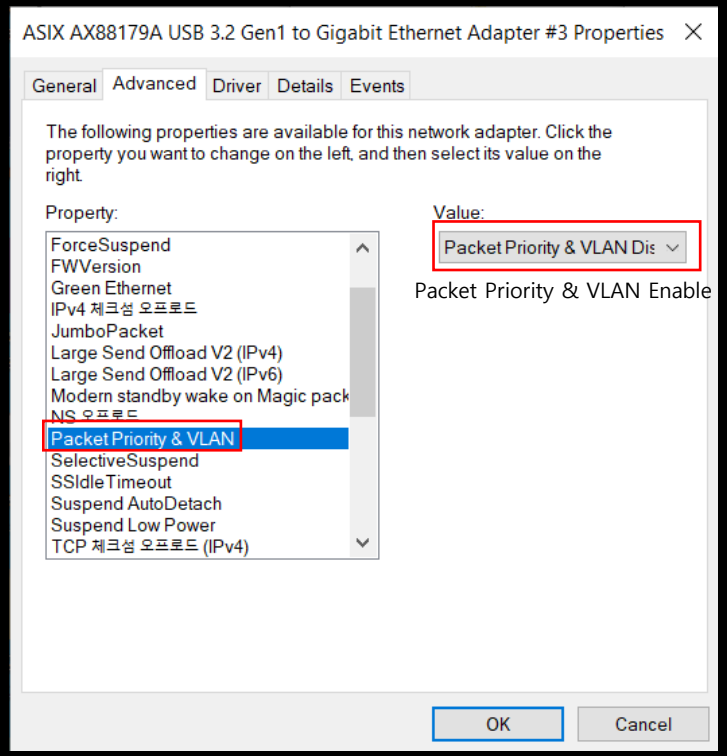
No.	Time	Source	Destination	Protocol	Length	Info
85	4.64…	160.48.199.99	239.192.255.251	SOME/IP-SD	470	SOME/IP Service Discovery Protocol [Offer]
86	4.64…	160.48.199.99	239.192.255.251	SOME/IP-SD	346	SOME/IP Service Discovery Protocol [Find]
87	4.88…	160.48.199.99	239.192.255.251	SOME/IP-SD	470	SOME/IP Service Discovery Protocol [Offer]
88	4.92…	160.48.199.99	239.192.255.251	SOME/IP-SD	598	SOME/IP Service Discovery Protocol [Offer]
89	4.93…	160.48.199.99	239.192.255.251	SOME/IP-SD	762	SOME/IP Service Discovery Protocol [Offer]
90	4.93…	160.48.199.99	239.192.255.251	SOME/IP-SD	106	SOME/IP Service Discovery Protocol [Find]
91	4.96…	160.48.199.99	239.192.255.251	SOME/IP-SD	762	SOME/IP Service Discovery Protocol [Offer]
92	4.96…	160.48.199.99	239.192.255.251	SOME/IP-SD	106	SOME/IP Service Discovery Protocol [Find]
93	5.02…	160.48.199.99	239.192.255.251	SOME/IP-SD	762	SOME/IP Service Discovery Protocol [Offer]
94	5.02…	160.48.199.99	239.192.255.251	SOME/IP-SD	106	SOME/IP Service Discovery Protocol [Find]
95	5.14…	160.48.199.99	239.192.255.251	SOME/IP-SD	106	SOME/IP Service Discovery Protocol [Find]
96	5.14…	160.48.199.99	239.192.255.251	SOME/IP-SD	762	SOME/IP Service Discovery Protocol [Offer]
97	5.38…	160.48.199.99	239.192.255.251	SOME/IP-SD	762	SOME/IP Service Discovery Protocol [Offer]
98	5.43…	160.48.199.99	239.192.255.251	SOME/IP-SD	330	SOME/IP Service Discovery Protocol [Find]
99	5.46…	160.48.199.99	239.192.255.251	SOME/IP-SD	330	SOME/IP Service Discovery Protocol [Find]
1	5.52	160.48.199.99	239.192.255.251	SOME/IP-SD	330	SOME/IP Service Discovery Protocol [Find]

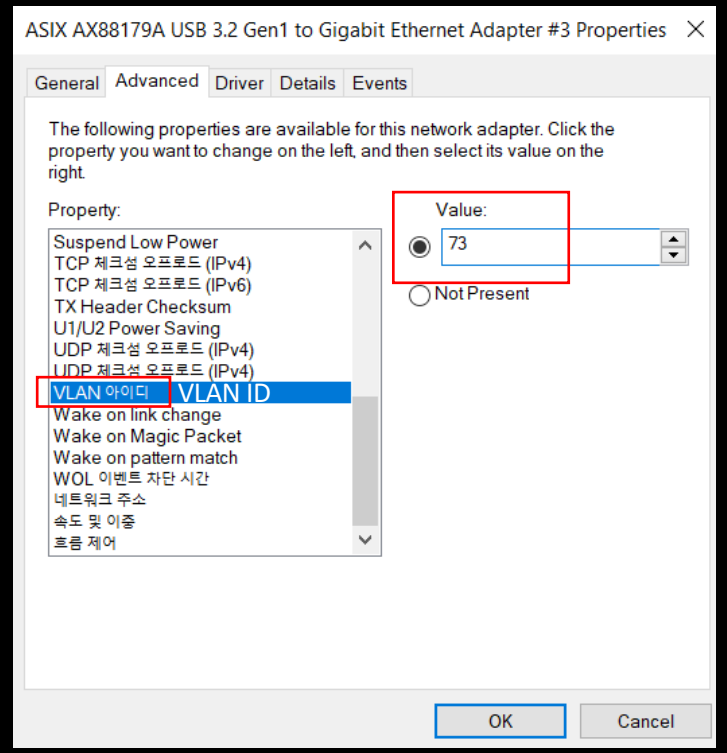
```
> Frame 91: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) on interface \Device\NPF_{285000B2-E4
> Ethernet II, Src: HarmanBe_23:04:1b (38:45:54:23:04:1b), Dst: IPv4mcast_40:ff:fb (01:00:5e:40:ff:fb)
> 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 73
> Internet Protocol Version 4, Src: 160.48.199.99, Dst: 239.192.255.251
> User Datagram Protocol, Src Port: 30490, Dst Port: 30490
> SOME/IP Protocol (Service ID: 0xffff, Method ID: 0x8100, Length: 708)
> SOME/IP Service Discovery Protocol
```

Setup IP and VLAN

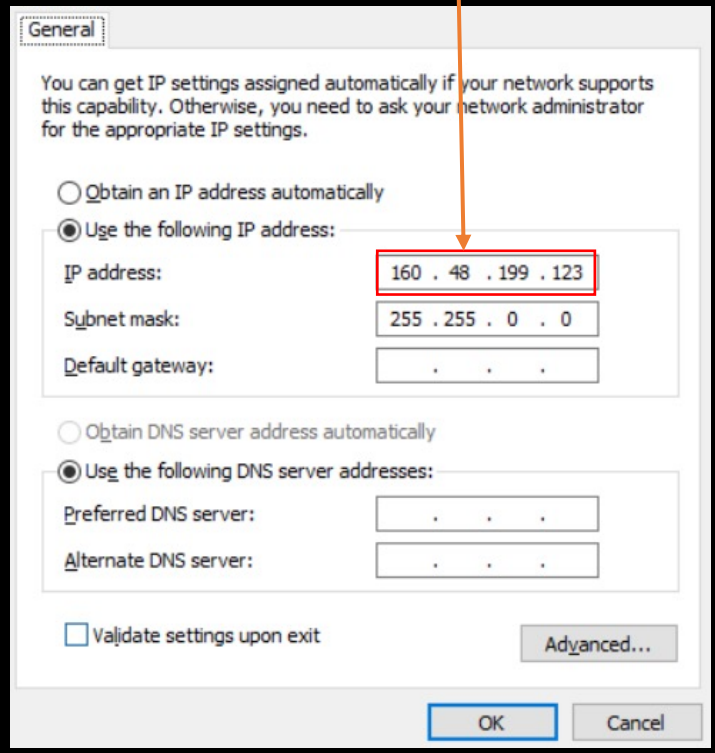
(Windows) Ethernet properties → Networking → Configure → Advanced

- "PacketPriority & VLAN" → "Packet Priority & VLAN Enable"
- "VLAN ID" → "Value" → *vlan id*





Select any IP in same subnetwork



Discovery SOME/IP Services

SOME/IP Service Discovery (SD)

Several SOME/IP services are running on the different ports at ECU.
To fuzz a SOME/IP service, we should know the port and the service ID.

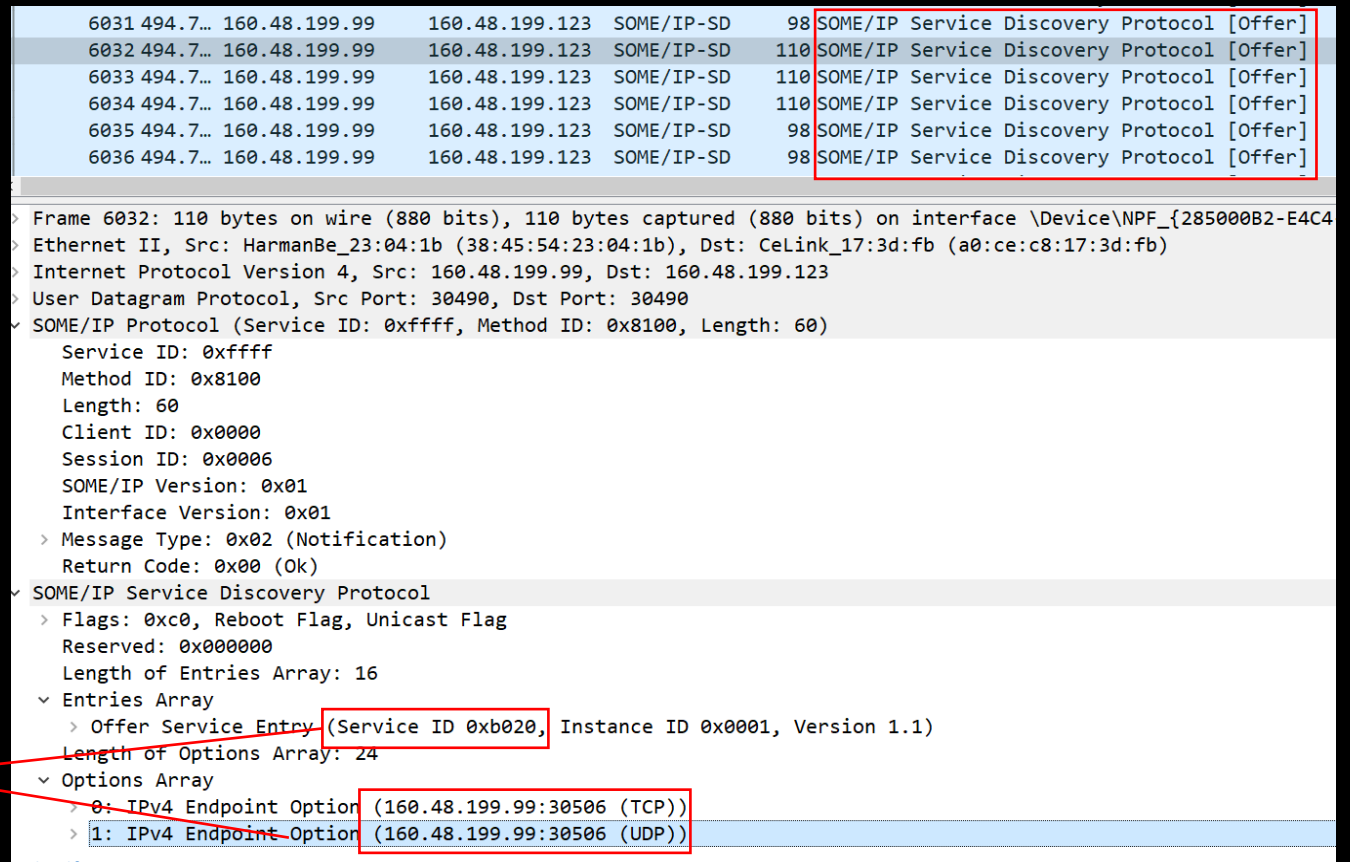
- Check “OFFER” message

ECU periodically broadcast ”OFFER” containing the service IDs and port numbers.

- Send “FIND” message

ECU will respond with ”OFFER”.

“*OFFER*” message includes service ID and port



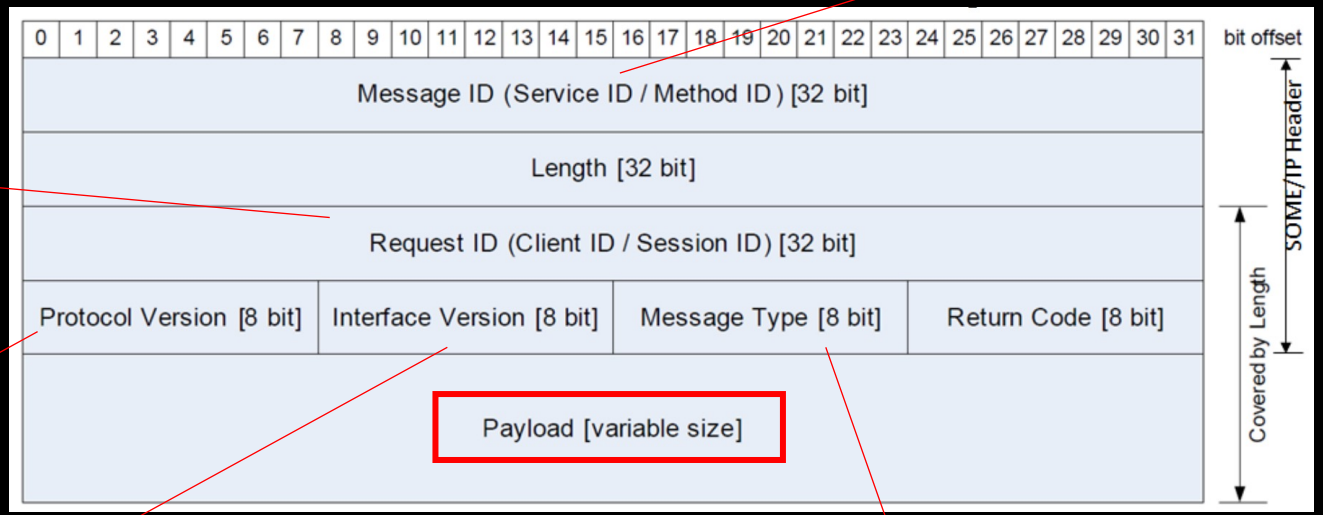
https://www.autosar.org/fileadmin/user_upload/standards/foundation/1-2/AUTOSAR_PRS_SOMEIPServiceDiscoveryProtocol.pdf

Let’s Do Fuzzing!

Fuzz Data Generation

Service ID [16 Bit]	0 [1 Bit]	Method ID [last 15 Bit]

Client ID [16 Bits]	Session ID [16 Bits]



0x01

0x01

Number	Value	Description
0x00	REQUEST	A request expecting a response (even void)
0x01	REQUEST_NO_RETURN	A fire&forget request
0x02	NOTIFICATION	A request of a notification/event callback expecting no response
0x80	RESPONSE	The response message
0x81	ERROR	The response containing an error)
0x20	TP_REQUEST	A TP request expecting a response (even void)
0x21	TP_REQUEST_NO_RETURN	A TP fire&forget request
0x22	TP_NOTIFICATION	A TP request of a notification/event call-back expecting no response
0x23	TP_RESPONSE	The TP response message
0x24	TP_ERROR	The TP response containing an error)

https://www.autosar.org/fileadmin/user_upload/standards/foundation/1-0/AUTOSAR_PRS_SOMEIPProtocol.pdf

How to know ECU's state?

- Return codes
  - We can guess the ECU's state and error handling logics.

Return Codes	Name
0x00	E_OK
0x01	E_NOT_OK
…	…
0x06	E_TIMEOUT
0x09	E_MALFORMED_MESSAGE

- Check response on the valid SOME/IP-SD message
  - no response from ECU → SOME/IP service is dead?

- Check periodic SOME/IP-SD messages from the ECU
  - no longer "*OFFER*" messages transmission from the ECU → SOME/IP service is dead?

Implementation: Scapy supports SOME/IP!



Create SOME/IP package:

```
sip = SOMEIP()
sip.iface_ver = 0
sip.proto_ver = 1
sip.msg_type = "REQUEST"
sip.retcode = "E_OK"
sip.srv_id = 0x1234
sip.method_id = 0x421
```

You can insert fuzz data here

Add the payload:

```
sip.add_payload(Raw ("Hello"))
```

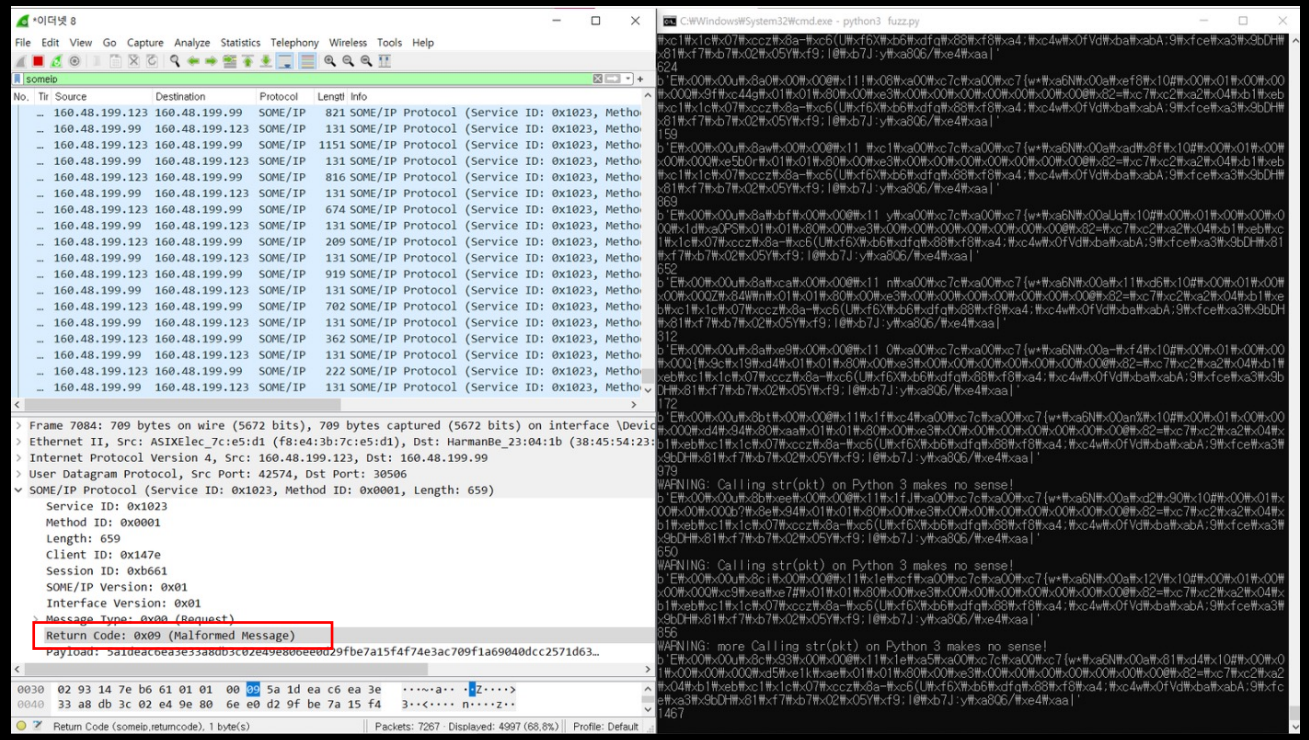
Stack it and send it:

```
p = i/u/sip
send(p)
```

https://scapy.readthedocs.io/en/latest/layers/automotive.html#some-ip-and-some-ip-sd-messages

Results

- BMW
  - Still, we do fuzzing …
  - Haven’t found anything yet



- But we found some crashes of other OEM’s ECUs.
  - we can’t disclose it because of NDA.

Conclusion

- You can do car hacking without a whole car itself.
  - You can buy, setup and test ECUs.

- Let’s do fuzzing Automotive Ethernet.
  - It’s an early stage. There’s still much to fuzz.
  - We will try DoIP.