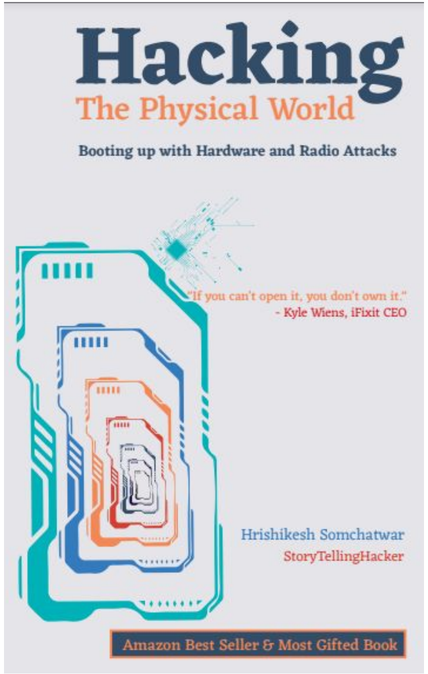
Wheels of Wonder

Unveiling Car Hacking Poetry at Defcamp

Hrishikesh Somchatwar
StoryTellingHacker

ABOUT ME

- Hrishikesh Somchatwar (Twitter) @StorytelnHacker
- Bestselling Author on Amazon “Hacking the Physical World”
- Speaker/Trainer at various security cons such as Bsides Delhi 2019, c0c0n 2019, Bsides Ahmedabad 2021, HackFest Canada 2021, Defcamp Romania 2019 and a bunch of others
- Podcast on Apple Podcasts, Spotify, google podcast “StorytellingHacker”


Hacking
The Physical World
Booting up with Hardware and Radio Attacks
"If you can't open it, you don't own it."
- Kyle Wiens, iFixit CEO
Hrishikesh Somchatwar
StoryTellingHacker
Amazon Best Seller & Most Gifted Book

Agenda

- Structure of a Car
- Attack surface
- Abuse techniques
- Reports

Structure of a car

- Electronics Hardware

Structure of a car

- Electronics Hardware
- Mechanics

Structure of a car

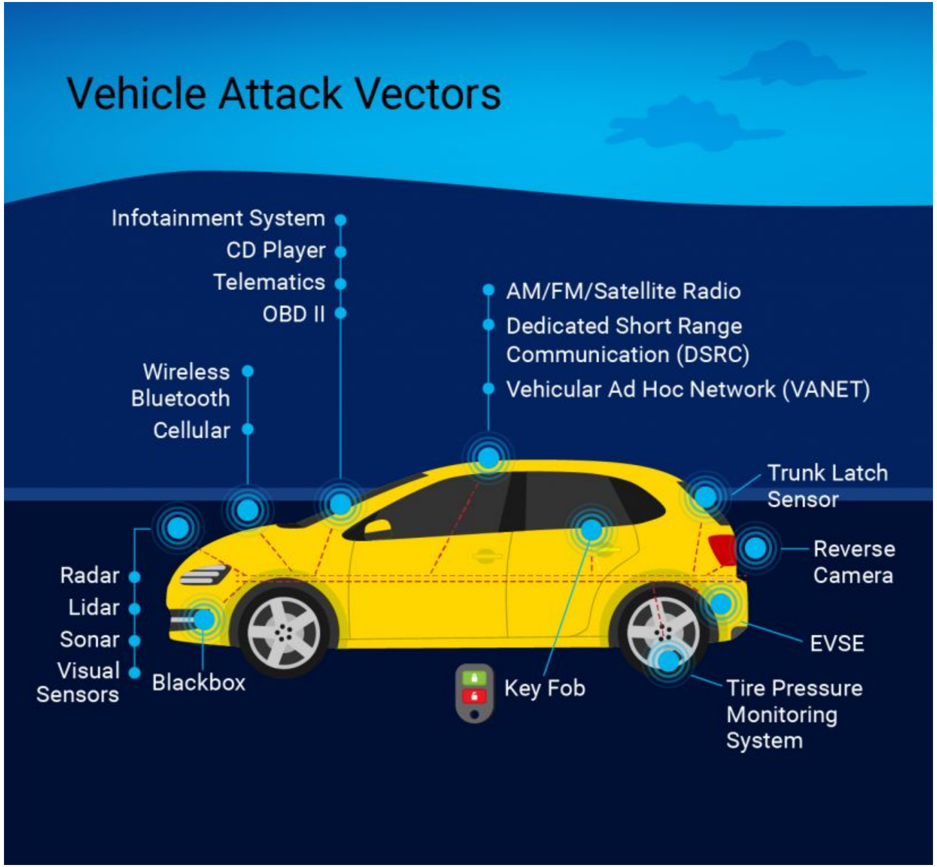
- Electronics Hardware
- Mechanics
- Radio Communication

Structure of a car

- Electronics Hardware
- Mechanics
- Radio Communication
- Sensors

STRUCTURE

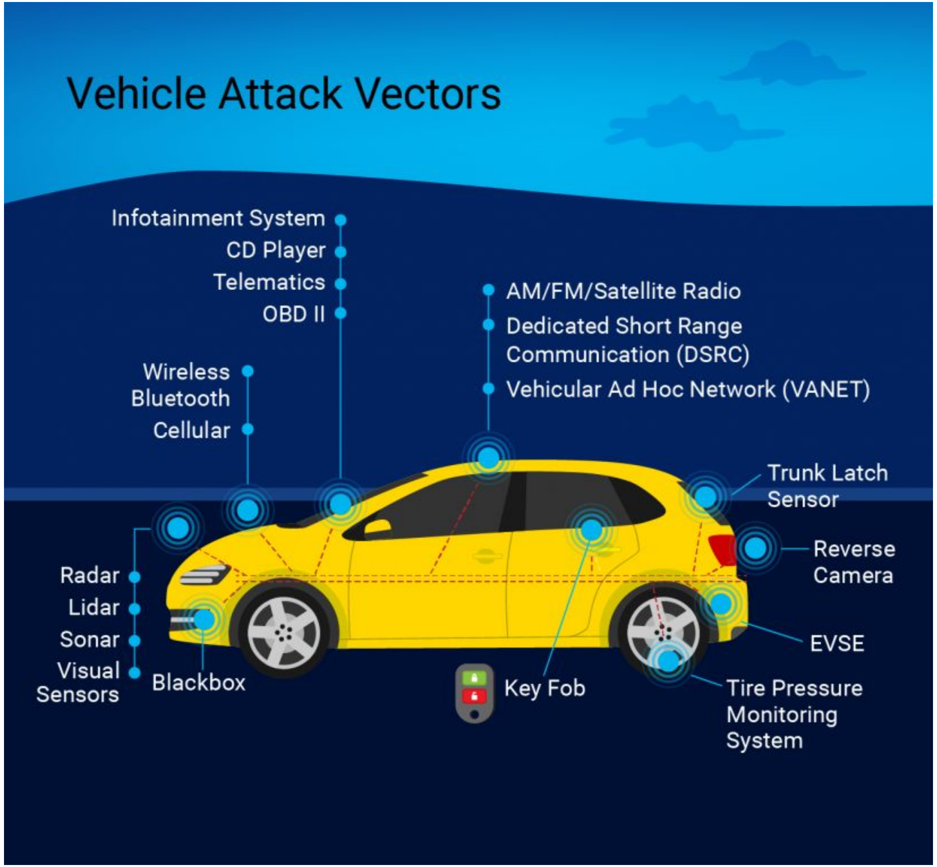
But!



STRUCTURE

But!

There is one problem approach in a pentest.

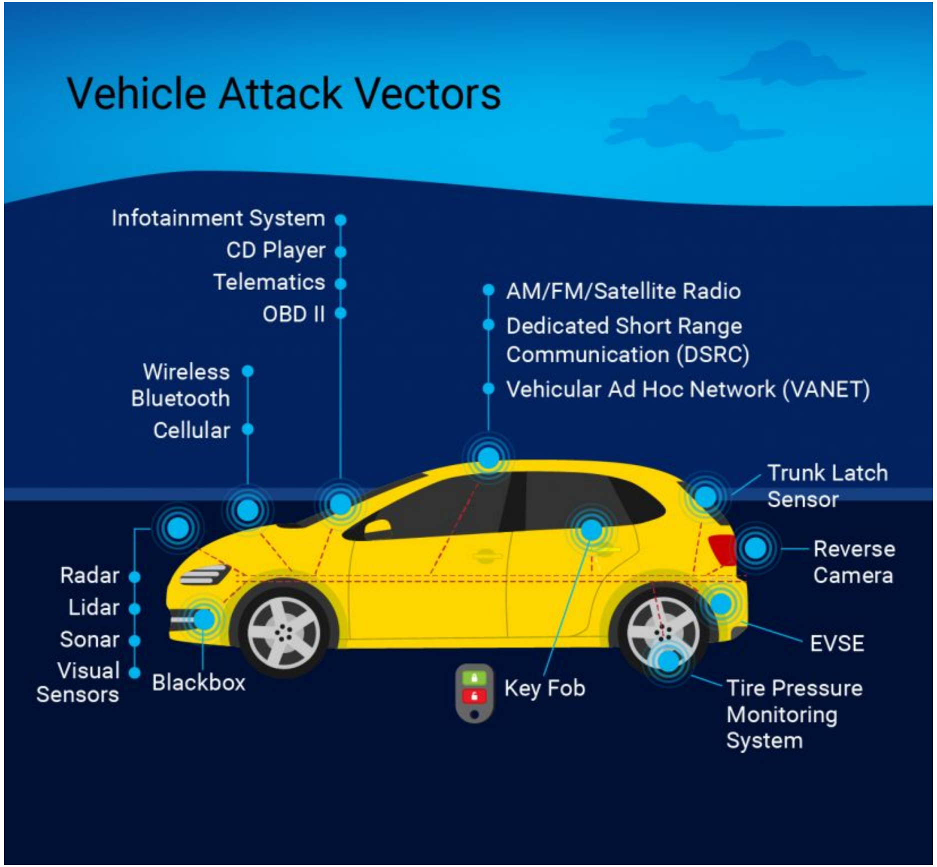


STRUCTURE

But!

There is one problem approach in a pentest.

<u>Telematics Control Unit</u> is ignored



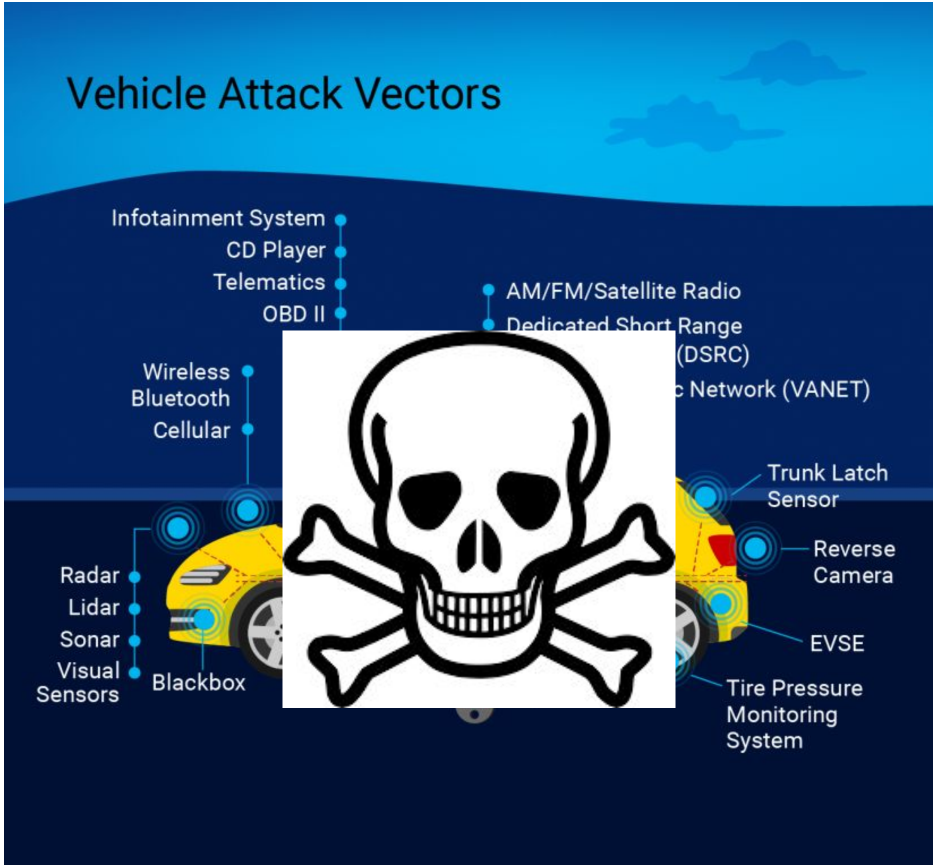
STRUCTURE

But!

There is one problem approach in a pentest.

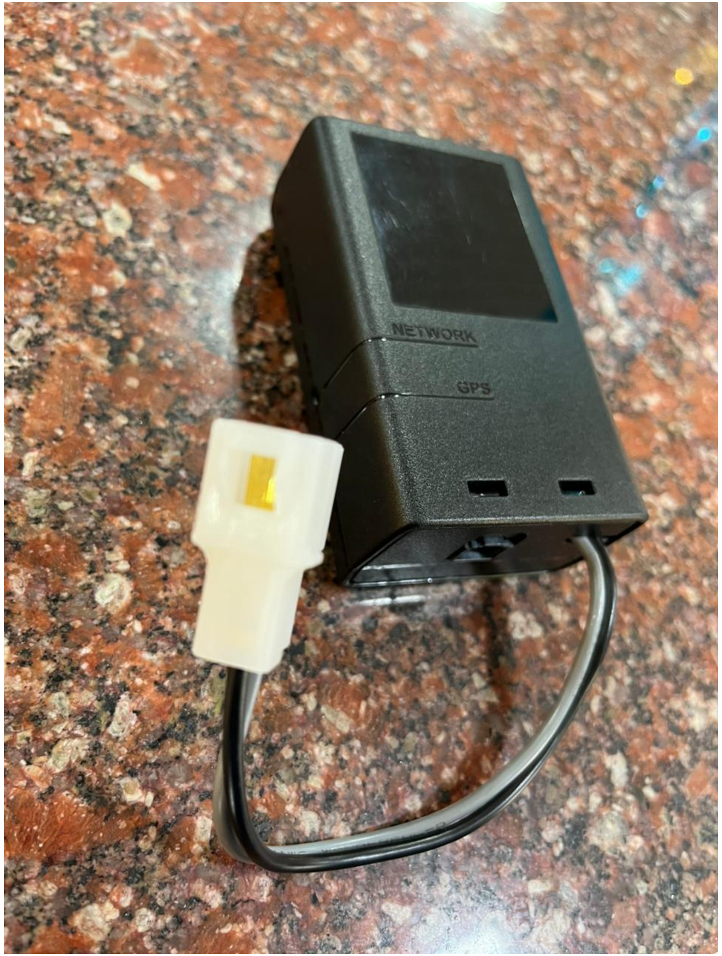
<u>Telematics Control Unit</u> is ignored

That’s why Car Hacking!



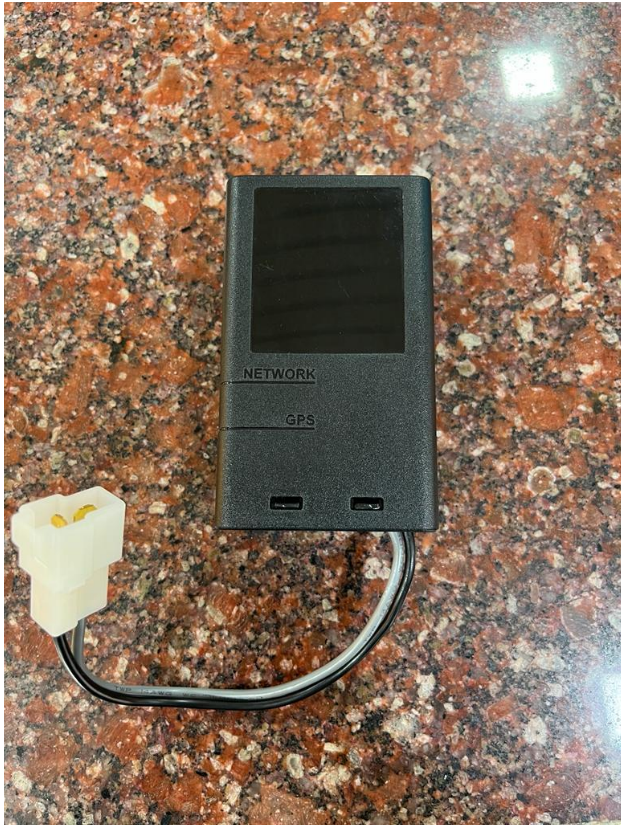
We will be mostly focusing on telematics control unit attacks!

Our target



INTERFACES

- Telecom

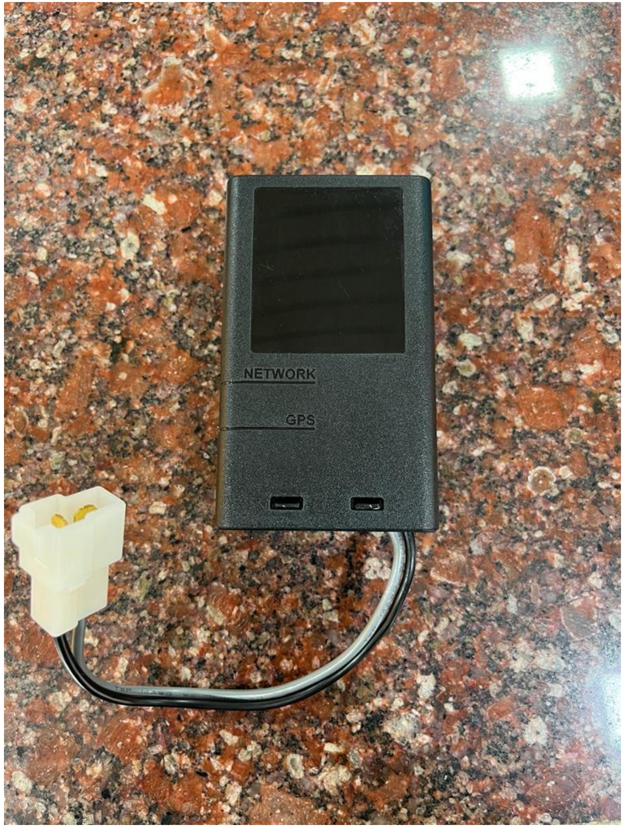


INTERFACES

- Telecom
- GPS

INTERFACES

- Telecom
- GPS
- Hardware

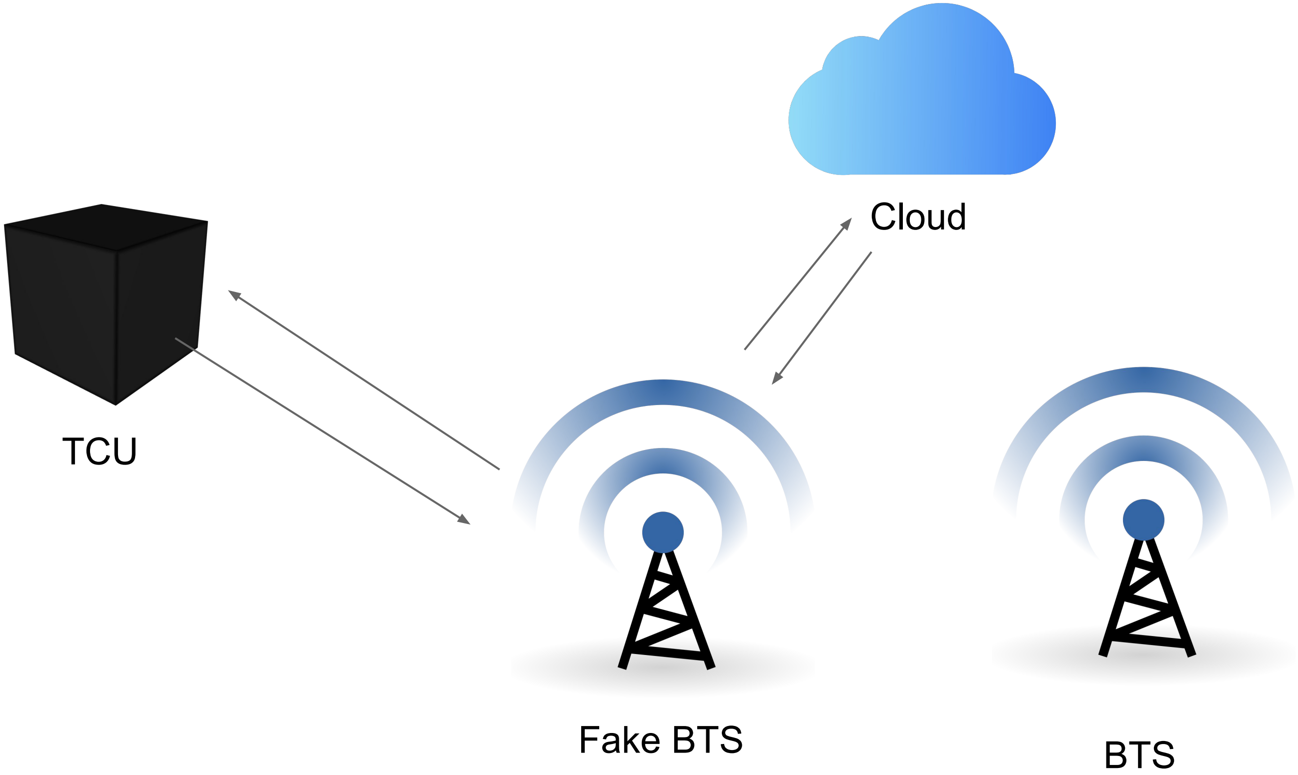


INTERFACES

- Telecom
- GPS
- Hardware
- Radio

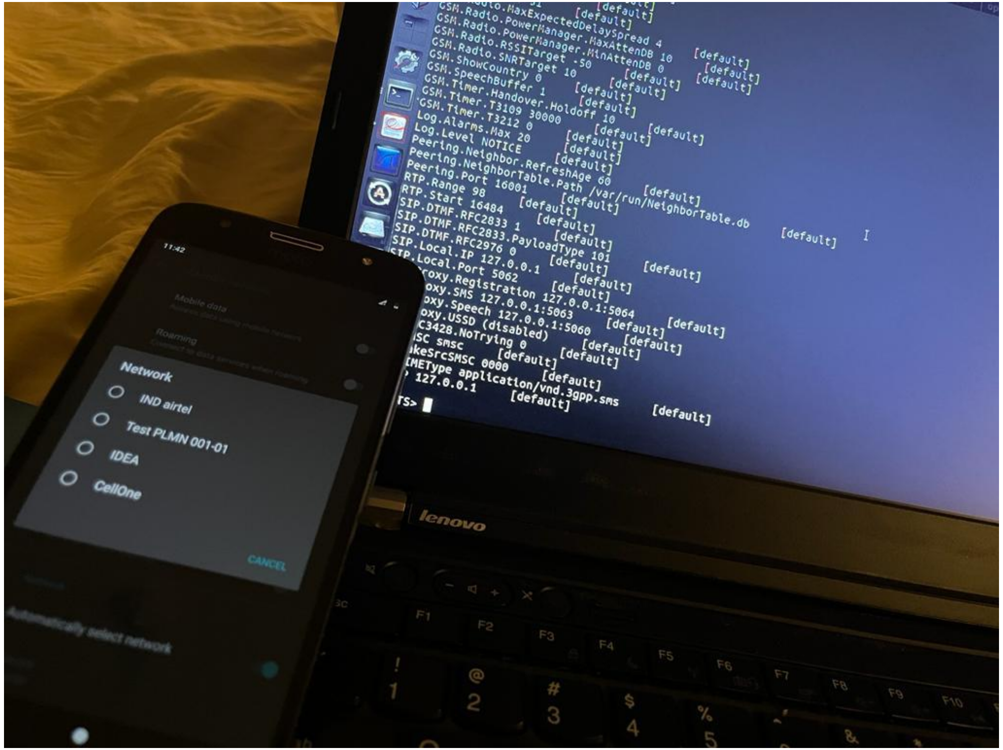
Telecom

Flowgraph



TELECOM

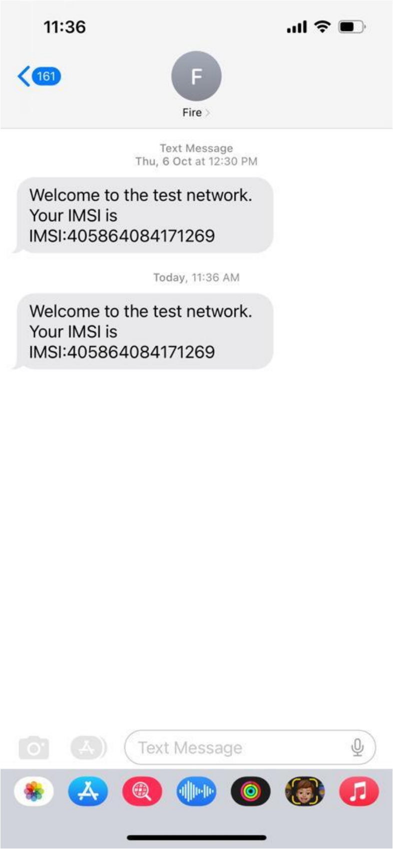
- FakeBTS
- Fake Cellphone networks
- Tricking the phones
- Named TEST PLMN 001-01



```
GSM.Radio.MaxExpectedDelaySpread 4                [default]
GSM.Radio.PowerManager.MaxAttenDB 10      [default]
GSM.Radio.PowerManager.MinAttenDB 0        [default]
GSM.Radio.RSSITarget -50          [default]
GSM.Radio.SNRTarget 10          [default]
GSM.ShowCountry 0        [default]
GSM.SpeechBuffer 1        [default]
GSM.Timer.Handover.Holdoff 10
GSM.Timer.T3109 30000          [default]
GSM.Timer.T3212 0                       [default]
Log.Alarms.Max 20         [default]
Log.Level NOTICE          [default]
Peering.Neighbor.RefreshAge 60       [default]
Peering.NeighborTable.Path /var/run/NeighborTable.db        [default]
Peering.Port 16001           [default]
RTP.Range 98          [default]
RTP.Start 16484          [default]
SIP.DTMF.RFC2833 1          [default]
SIP.DTMF.RFC2833.PayloadType 101
SIP.DTMF.RFC2976 0          [default]
SIP.Local.IP 127.0.0.1          [default]
SIP.Local.Port 5062          [default]
 roxy.Registration 127.0.0.1:5064
 oxy.SMS 127.0.0.1:5063          [default]
 oxy.Speech 127.0.0.1:5060          [default]
 oxy.USSD (disabled)          [default]
 C3428.NoTrying 0          [default]
 SC smsc          [default]
 keSrcSMSC 0000          [default]
 IMEType application/vnd.3gpp.sms          [default]
 127.0.0.1          [default]
TS>
```

Fun with fake tower

- Created a fake cellphone tower

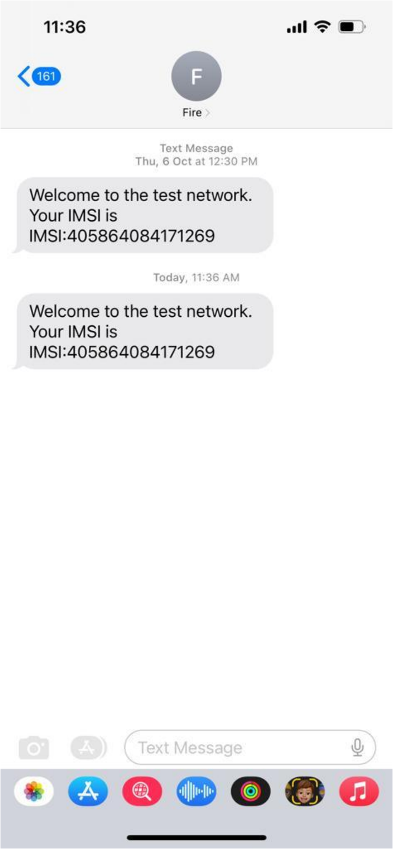


Welcome to the test network. Your IMSI is IMSI:405864084171269

Welcome to the test network. Your IMSI is IMSI:405864084171269

Fun with fake tower

- Created a fake cellphone tower
- Tricked iPhone to connect to that tower



Text Message
Thu, 6 Oct at 12:30 PM

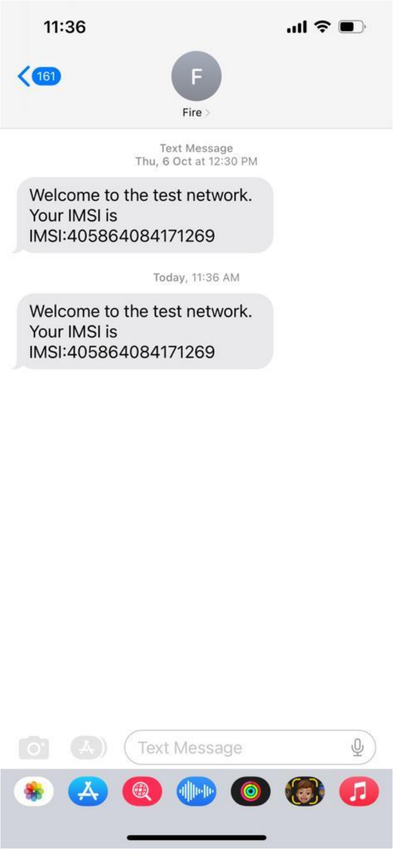
Welcome to the test network. Your IMSI is IMSI:405864084171269

Today, 11:36 AM

Welcome to the test network. Your IMSI is IMSI:405864084171269

FUN WITH FAKE TOWER

- Created a fake cellphone tower
- Tricked iPhone to connect to that tower
- Started sending fake calls and texts



Text Message
Thu, 6 Oct at 12:30 PM

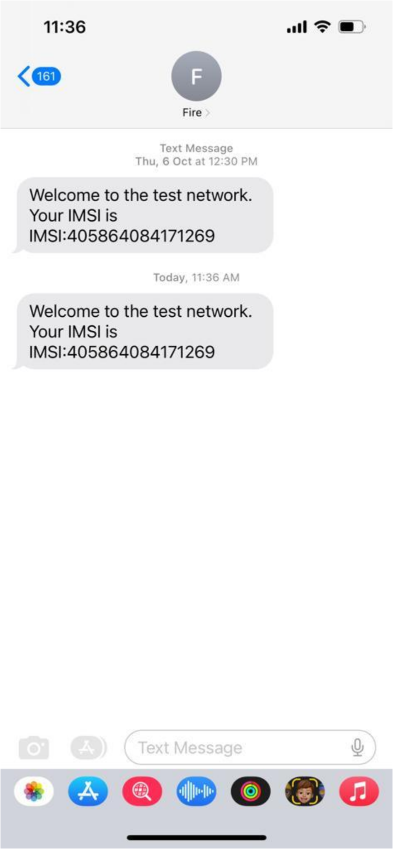
Welcome to the test network. Your IMSI is IMSI:405864084171269

Today, 11:36 AM

Welcome to the test network. Your IMSI is IMSI:405864084171269

Fun with fake tower

- Created a fake cellphone tower
- Tricked iPhone to connect to that tower
- Started sending fake calls and texts
- Had fun! ;)



Text Message
Thu, 6 Oct at 12:30 PM

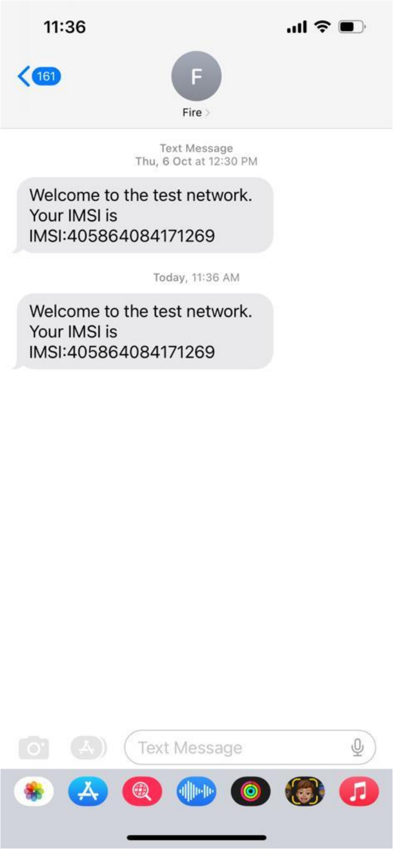
Welcome to the test network. Your IMSI is IMSI:405864084171269

Today, 11:36 AM

Welcome to the test network. Your IMSI is IMSI:405864084171269

Fun with fake tower

- Created a fake cellphone tower
- Tricked iPhone to connect to that tower
- Started sending fake calls and texts
- Had fun! ;)



Text Message
Thu, 6 Oct at 12:30 PM

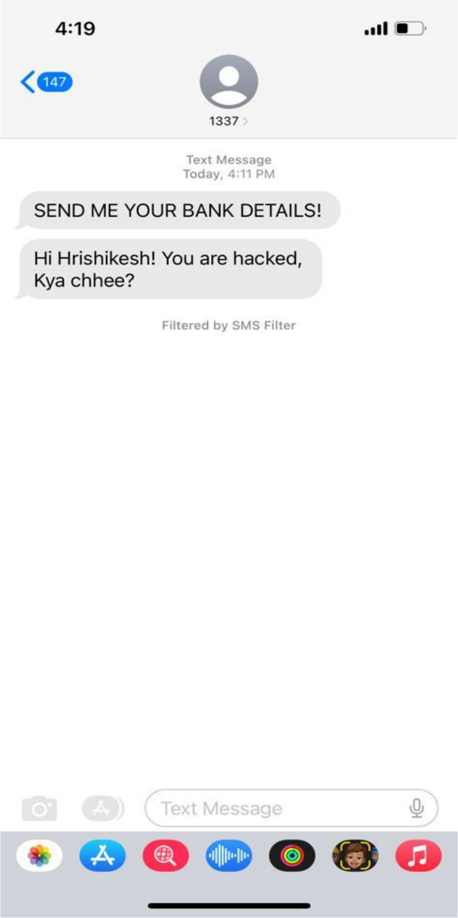
Welcome to the test network. Your IMSI is IMSI:405864084171269

Today, 11:36 AM

Welcome to the test network. Your IMSI is IMSI:405864084171269

Fun with fake tower

- Created a fake cellphone tower
- Tricked iPhone to connect to that tower
- Started sending fake calls and texts
- Had fun! ;)



Text Message
Today, 4:11 PM

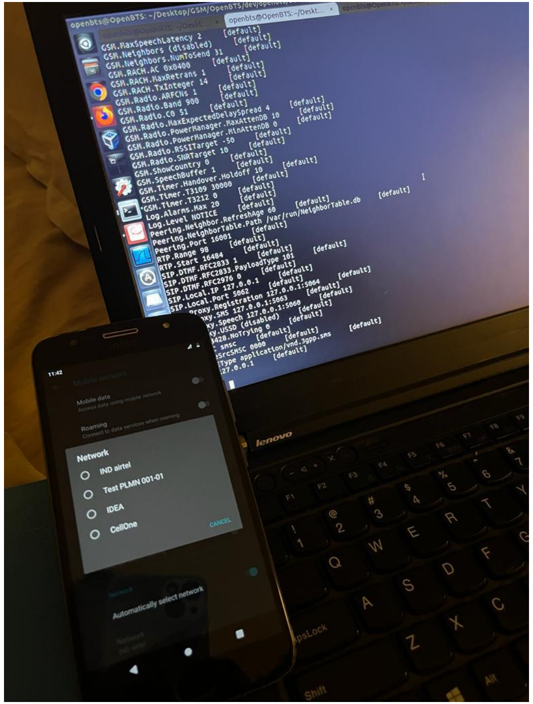
SEND ME YOUR BANK DETAILS!

Hi Hrishikesh! You are hacked, Kya chhee?

Filtered by SMS Filter

TELECOM

- Number of fake towers



```
openbts@OpenBTS: ~/Desktop/GSM/OpenBTS/dev/openbts/...
openbts@OpenBTS: ~/Deskt...   openbts@OpenBTS: ~/Deskt...
                                [default]
GSM.MaxSpeechLatency 2          [default]
GSM.Neighbors (disabled)        [default]
GSM.Neighbors.NumToSend 31      [default]
GSM.RACH.AC 0x0400      [default]
GSM.RACH.MaxRetrans 1       [default]
GSM.RACH.TxInteger 14       [default]
GSM.Radio.ARFCNs 1      [default]
GSM.Radio.Band 900      [default]
GSM.Radio.C0 51     [default]
GSM.Radio.MaxExpectedDelaySpread 4      [default]
GSM.Radio.PowerManager.MaxAttenDB 10        [default]
GSM.Radio.PowerManager.MinAttenDB 0     [default]
GSM.Radio.RSSITarget -50        [default]
GSM.Radio.SNRTarget 10      [default]
GSM.ShowCountry 0       [default]
GSM.SpeechBuffer 1      [default]
GSM.Timer.Handover.Holdoff 10       [default]
GSM.Timer.T3109 30000       [default]
GSM.Timer.T3212 0       [default]
Log.Alarms.Max 20       [default]
Log.Level NOTICE        [default]
Peering.Neighbor.RefreshAge 60      [default]
Peering.NeighborTable.Path /var/run/NeighborTable.db        [default]
Peering.Port 16001      [default]
RTP.Range 98        [default]
RTP.Start 16484     [default]
SIP.DTMF.RFC2833 1      [default]
SIP.DTMF.RFC2833.PayloadType 101        [default]
SIP.DTMF.RFC2976 0      [default]
SIP.Local.IP 127.0.0.1      [default]
SIP.Local.Port 5062     [default]
SIP.Proxy.Registration 127.0.0.1:5064       [default]
  oxy.SMS 127.0.0.1:5063        [default]
  oxy.Speech 127.0.0.1:5060     [default]
  xy.USSD (disabled)        [default]
  3428.NoTrying 0       [default]
   smsc     [default]
  eSrcSMSC 0000     [default]
  eType application/vnd.3gpp.sms        [default]
  127.0.0.1     [default]
```

11:42

Mobile network

Mobile data
Access data using mobile network

Roaming
Connect to data services when roaming

Network

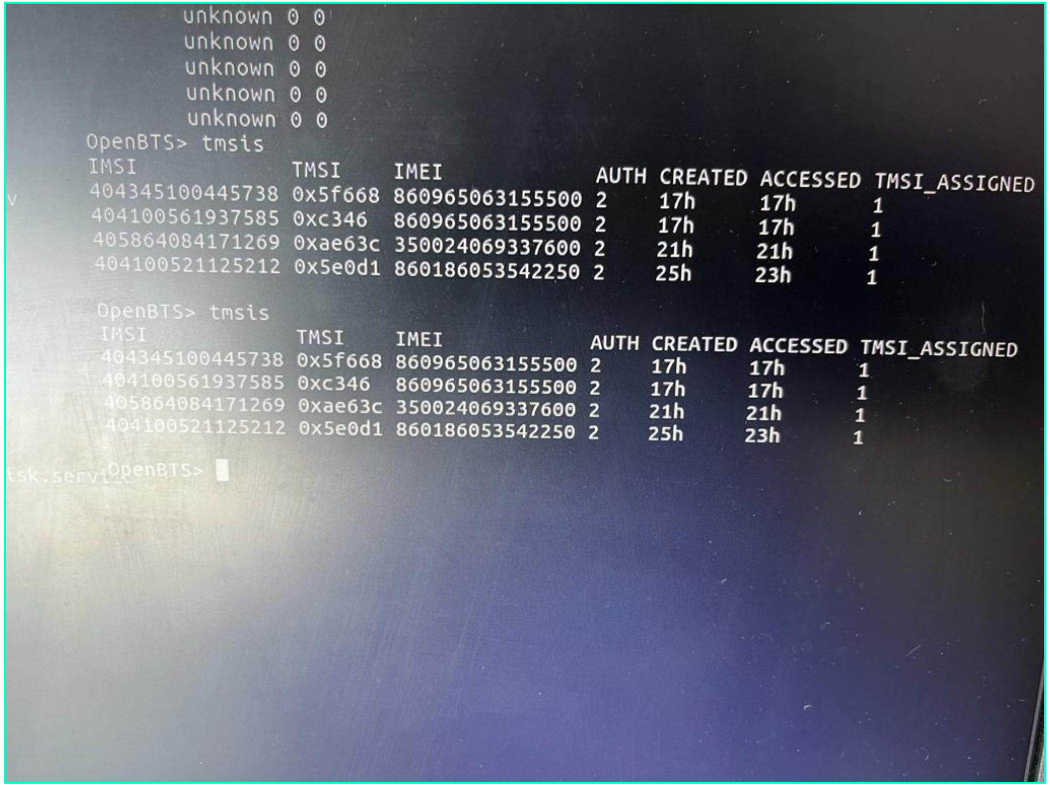
○ IND airtel
○ Test PLMN 001-01
○ IDEA
○ CellOne

CANCEL

Automatically select network

TELECOM

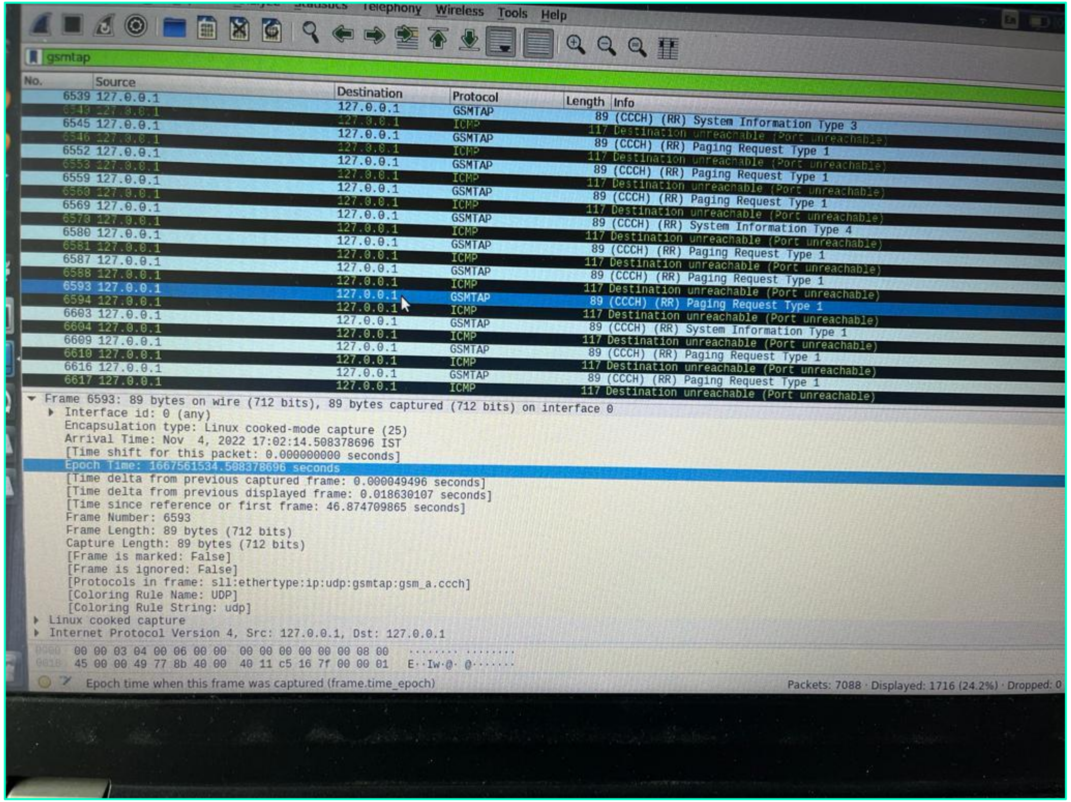
- All connected devices to my tower
- IMEI, IMSI etc is open
- Can give calls
- Messages to anyone



```
            unknown 0 0
            unknown 0 0
            unknown 0 0
            unknown 0 0
            unknown 0 0
OpenBTS> tmsis
IMSI            TMSI     IMEI            AUTH CREATED ACCESSED TMSI_ASSIGNED
404345100445738 0x5f668 860965063155500 2    17h     17h      1
404100561937585 0xc346  860965063155500 2    17h     17h      1
405864084171269 0xae63c 350024069337600 2    21h     21h      1
404100521125212 0x5e0d1 860186053542250 2    25h     23h      1

OpenBTS> tmsis
IMSI            TMSI     IMEI            AUTH CREATED ACCESSED TMSI_ASSIGNED
404345100445738 0x5f668 860965063155500 2    17h     17h      1
404100561937585 0xc346  860965063155500 2    17h     17h      1
405864084171269 0xae63c 350024069337600 2    21h     21h      1
404100521125212 0x5e0d1 860186053542250 2    25h     23h      1

sk.serviOpenBTS> █
```

TELECOM

- Wireshark analysis



```
No.   Source      Destination  Protocol  Length Info
6539 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) System Information Type 3
6543 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6545 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6546 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6552 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6553 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6559 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6560 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6569 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) System Information Type 4
6570 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6580 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6581 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6587 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6588 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6593 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6594 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6603 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) System Information Type 1
6604 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6609 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6610 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6616 127.0.0.1    127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6617 127.0.0.1    127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
```

```
▾ Frame 6593: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Nov  4, 2022 17:02:14.508378696 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667561534.508378696 seconds
    [Time delta from previous captured frame: 0.000049496 seconds]
    [Time delta from previous displayed frame: 0.018630107 seconds]
    [Time since reference or first frame: 46.874709865 seconds]
    Frame Number: 6593
    Frame Length: 89 bytes (712 bits)
    Capture Length: 89 bytes (712 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:udp:gsmtap:gsm_a.ccch]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
```

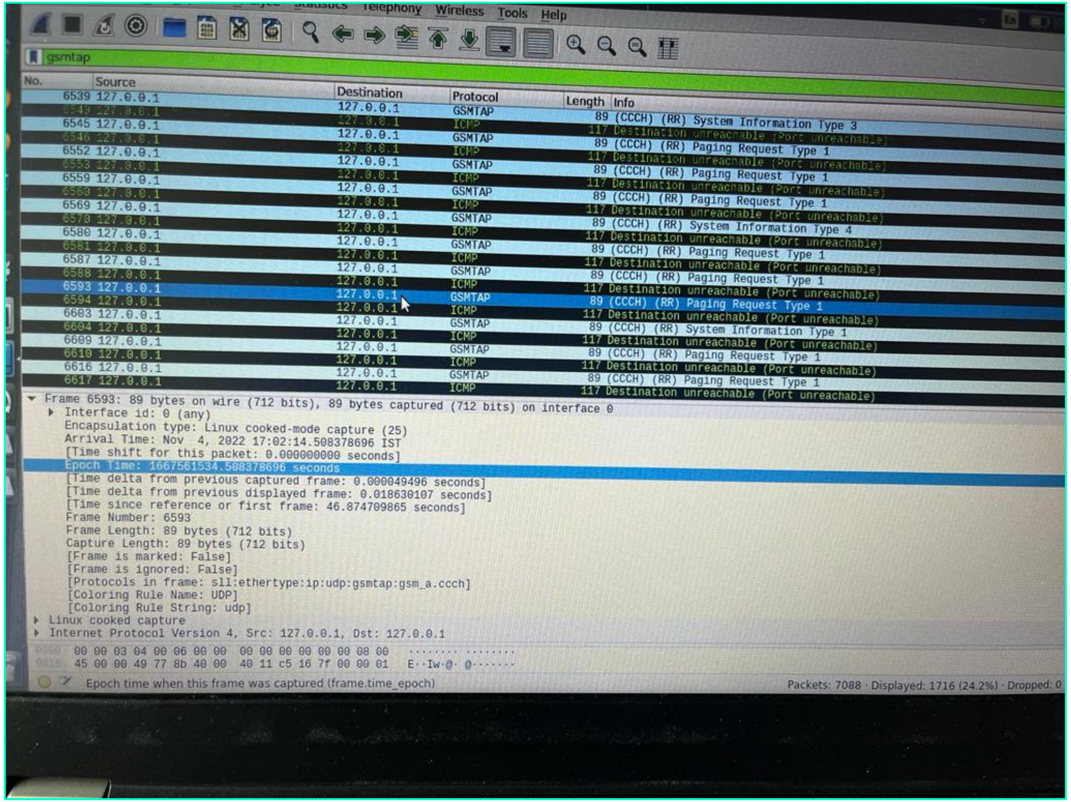
```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ........ ........
0010  45 00 00 49 77 8b 40 00  40 11 c5 16 7f 00 00 01   E··Iw·@· @·······
```

Epoch time when this frame was captured (frame.time_epoch)

Packets: 7088 · Displayed: 1716 (24.2%) · Dropped: 0

TELECOM

- Wireshark analysis
- Man in the Middle Attack

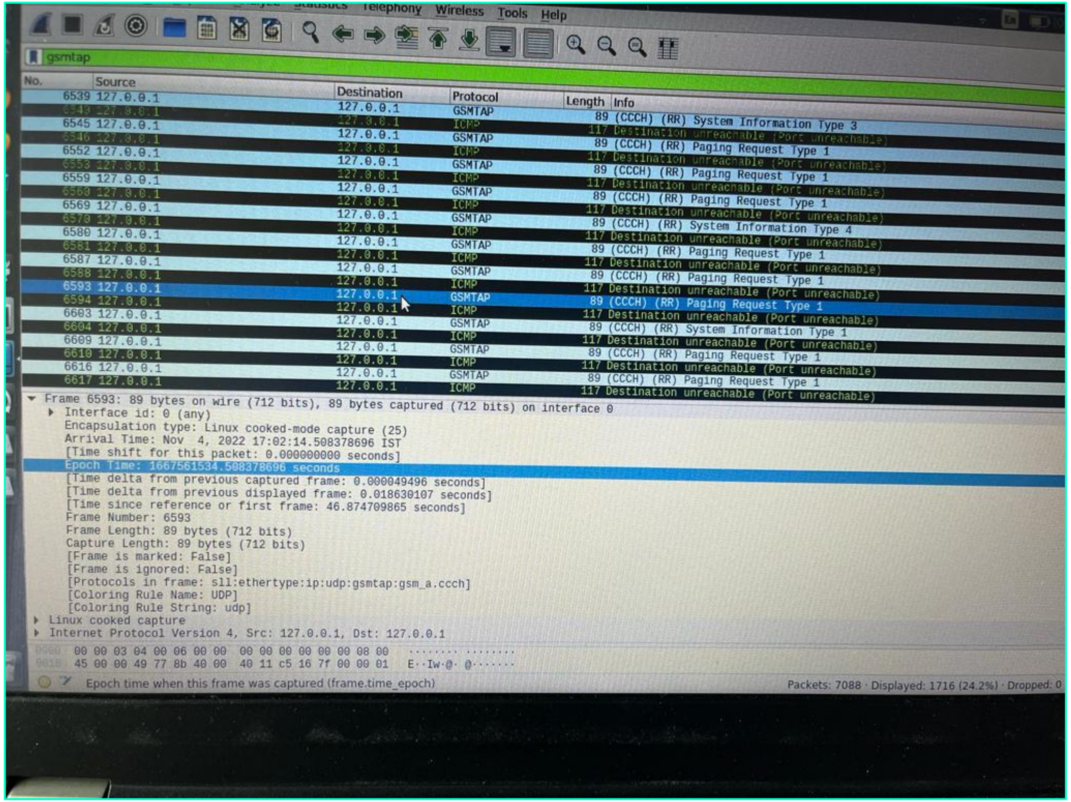


```
No.   Source      Destination  Protocol  Length Info
6539 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) System Information Type 3
6543 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6545 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6546 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6552 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6553 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6559 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6560 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6569 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) System Information Type 4
6570 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6580 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6581 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6587 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6588 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6593 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6594 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6603 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) System Information Type 1
6604 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6609 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6610 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
6616 127.0.0.1    127.0.0.1    GSMTAP       89 (CCCH) (RR) Paging Request Type 1
6617 127.0.0.1    127.0.0.1    ICMP        117 Destination unreachable (Port unreachable)
```

```
▾ Frame 6593: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Nov  4, 2022 17:02:14.508378696 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667561534.508378696 seconds
    [Time delta from previous captured frame: 0.000049496 seconds]
    [Time delta from previous displayed frame: 0.018630107 seconds]
    [Time since reference or first frame: 46.874709865 seconds]
    Frame Number: 6593
    Frame Length: 89 bytes (712 bits)
    Capture Length: 89 bytes (712 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:udp:gsmtap:gsm_a.ccch]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 49 77 8b 40 00  40 11 c5 16 7f 00 00 01   E··Iw·@· @·······

Epoch time when this frame was captured (frame.time_epoch)        Packets: 7088 · Displayed: 1716 (24.2%) · Dropped: 0
```

TELECOM

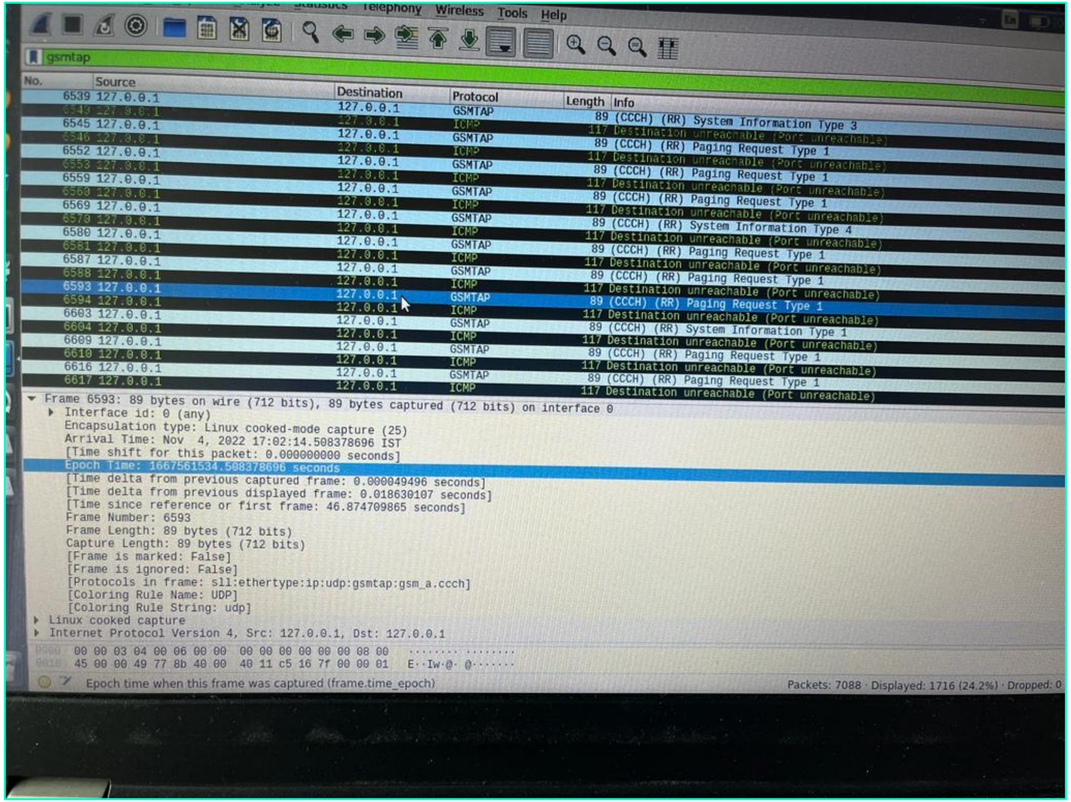
- Wireshark analysis
- Man in the Middle Attack
- Check for interfaces



```
gsmtap

No.  Source     Destination  Protocol  Length Info
6539 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) System Information Type 3
6543 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6545 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6546 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6552 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6553 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6559 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6560 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6569 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) System Information Type 4
6570 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6580 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6581 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6587 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6588 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6593 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6594 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6603 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) System Information Type 1
6604 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6609 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6610 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)
6616 127.0.0.1  127.0.0.1    GSMTAP     89 (CCCH) (RR) Paging Request Type 1
6617 127.0.0.1  127.0.0.1    ICMP      117 Destination unreachable (Port unreachable)

▾ Frame 6593: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Nov  4, 2022 17:02:14.508378696 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667561534.508378696 seconds
    [Time delta from previous captured frame: 0.000049496 seconds]
    [Time delta from previous displayed frame: 0.018630107 seconds]
    [Time since reference or first frame: 46.874709865 seconds]
    Frame Number: 6593
    Frame Length: 89 bytes (712 bits)
    Capture Length: 89 bytes (712 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:udp:gsmtap:gsm_a.ccch]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 49 77 8b 40 00  40 11 c5 16 7f 00 00 01   E··Iw·@· @·······

Epoch time when this frame was captured (frame.time_epoch)        Packets: 7088 · Displayed: 1716 (24.2%) · Dropped: 0
```

TELECOM

- Wireshark analysis
- Man in the Middle Attack
- Check for interfaces
- Find FOTA creds, Firmware Links, Web portals etc.



gsmtap

```
No.   Source      Destination  Protocol  Length Info
 6539 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) System Information Type 3
 6543 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6545 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6546 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6552 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6553 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6559 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6560 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6569 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) System Information Type 4
 6570 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6580 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6581 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6587 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6588 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6593 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6594 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6603 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) System Information Type 1
 6604 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6609 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6610 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
 6616 127.0.0.1   127.0.0.1    GSMTAP        89 (CCCH) (RR) Paging Request Type 1
 6617 127.0.0.1   127.0.0.1    ICMP         117 Destination unreachable (Port unreachable)
```

```
▾ Frame 6593: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Nov  4, 2022 17:02:14.508378696 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667561534.508378696 seconds
    [Time delta from previous captured frame: 0.000049496 seconds]
    [Time delta from previous displayed frame: 0.018630107 seconds]
    [Time since reference or first frame: 46.874709865 seconds]
    Frame Number: 6593
    Frame Length: 89 bytes (712 bits)
    Capture Length: 89 bytes (712 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:udp:gsmtap:gsm_a.ccch]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ........ ........
0010  45 00 00 49 77 8b 40 00  40 11 c5 16 7f 00 00 01   E..Iw.@. @.......
```

Epoch time when this frame was captured (frame.time_epoch)

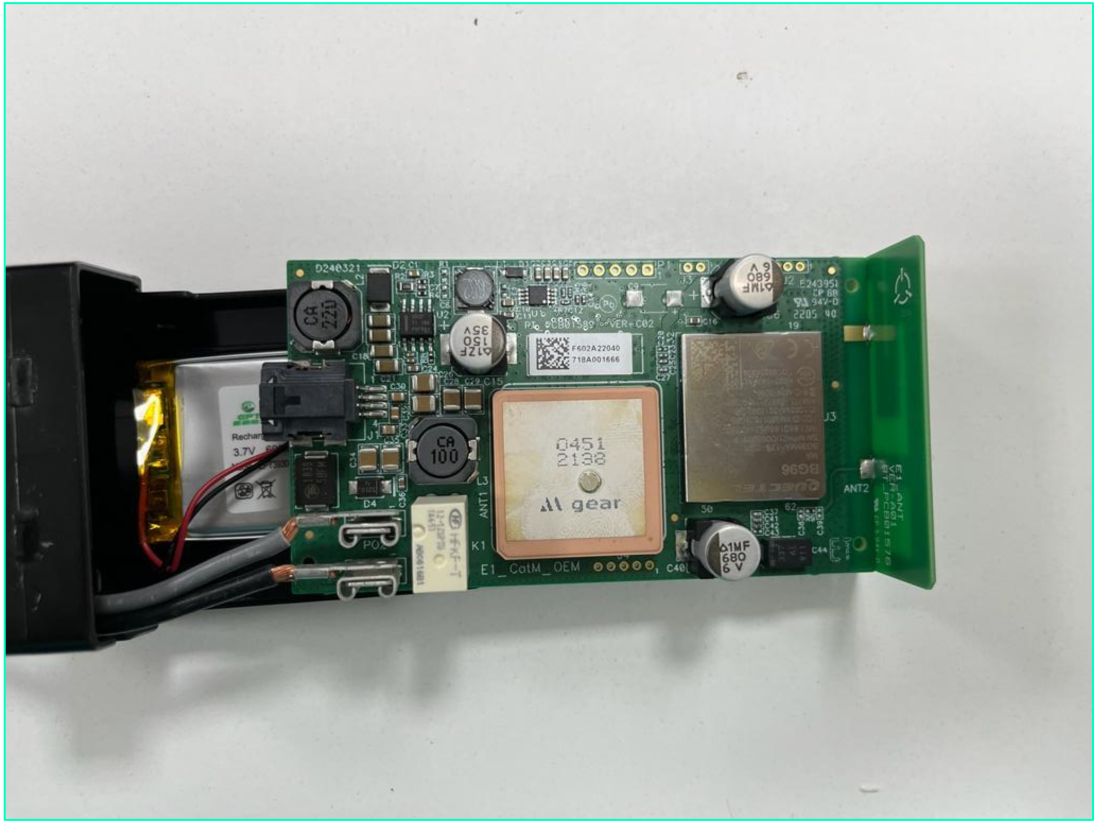
Packets: 7088 · Displayed: 1716 (24.2%) · Dropped: 0

Hardware

TAMPERING?

Before opening do we need to check that?

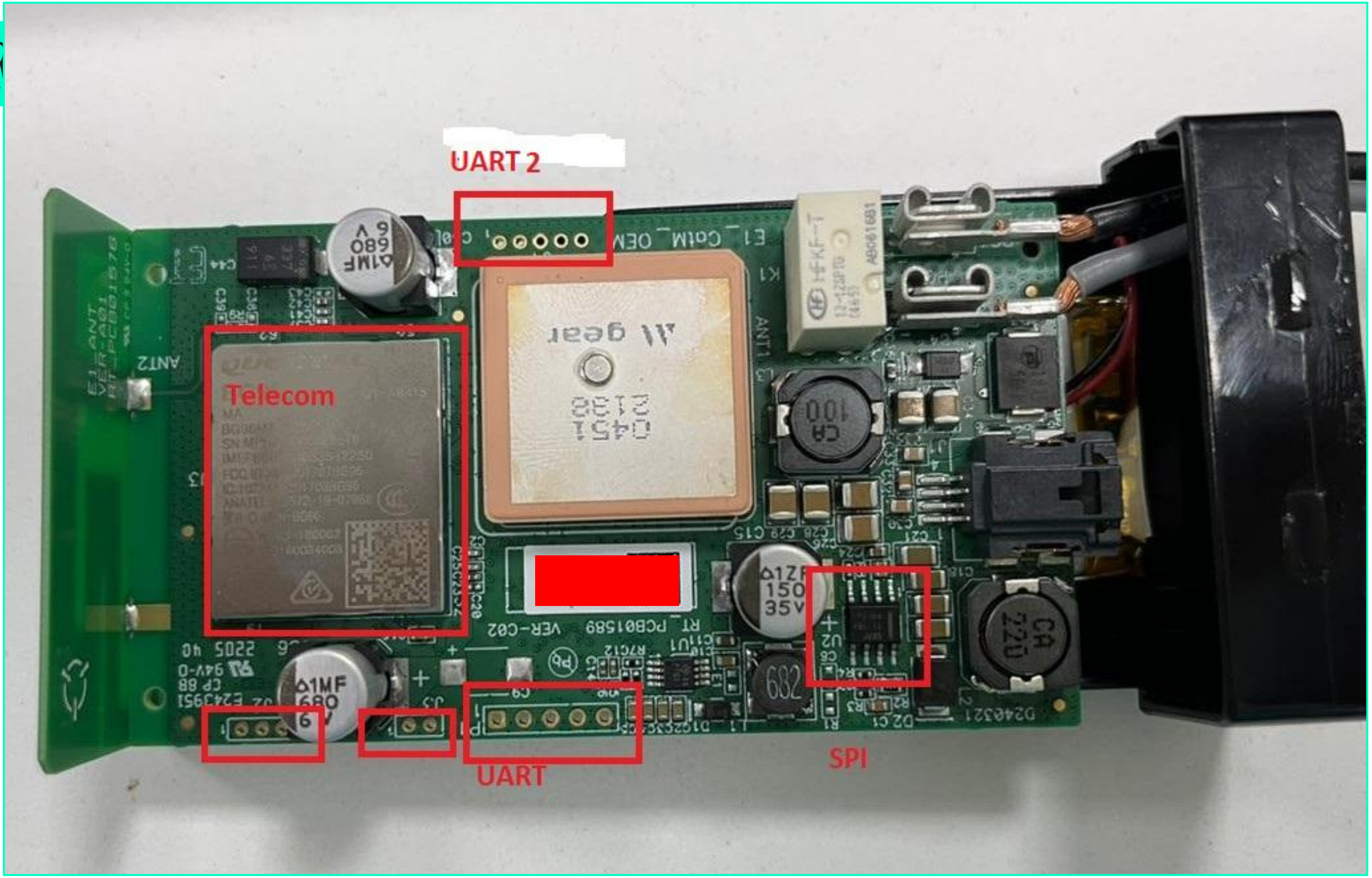
X-ray scans



Let's open it up!

Communication pr

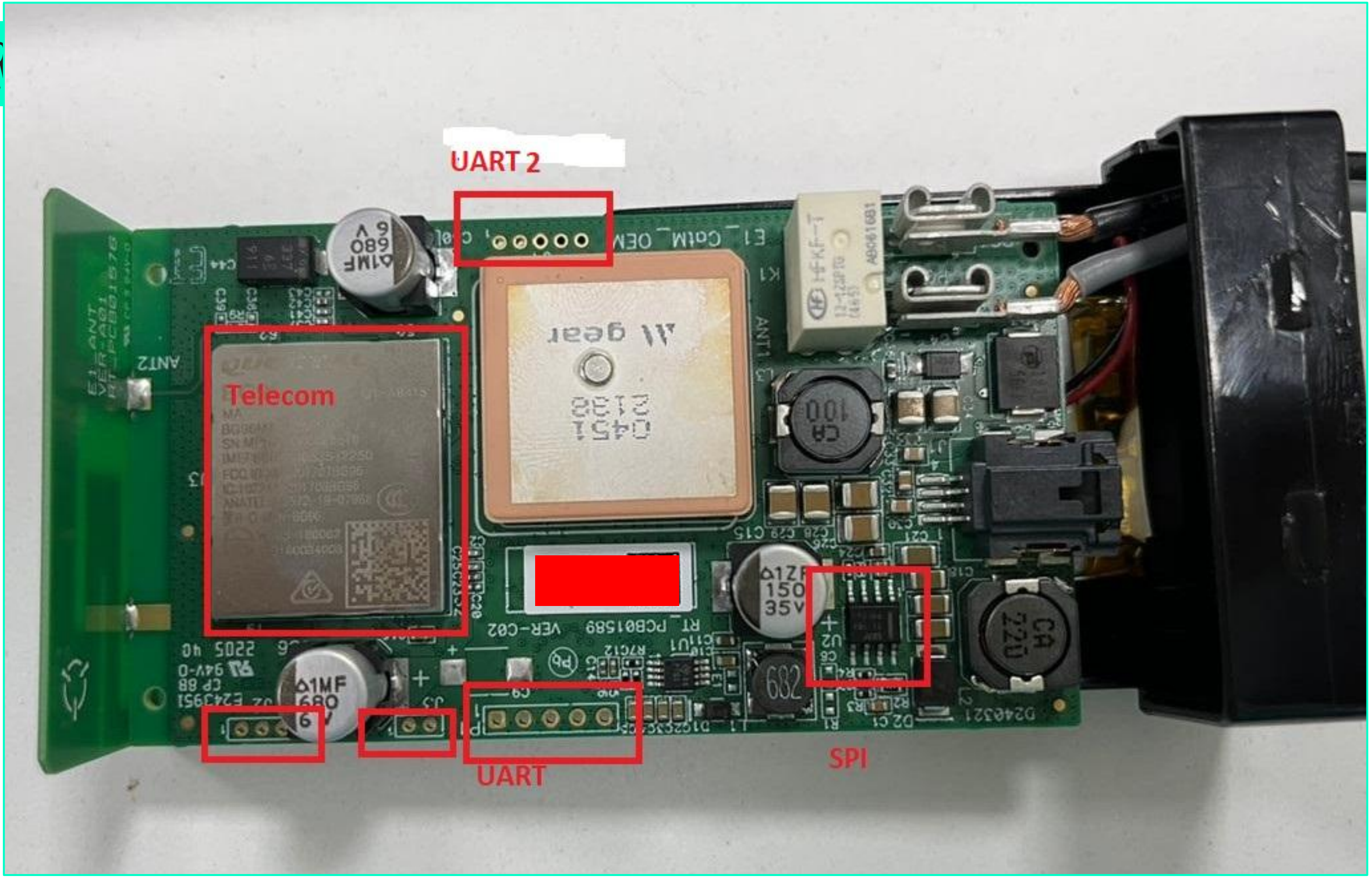
- Telecom Chip



[redacted]

Communication pr

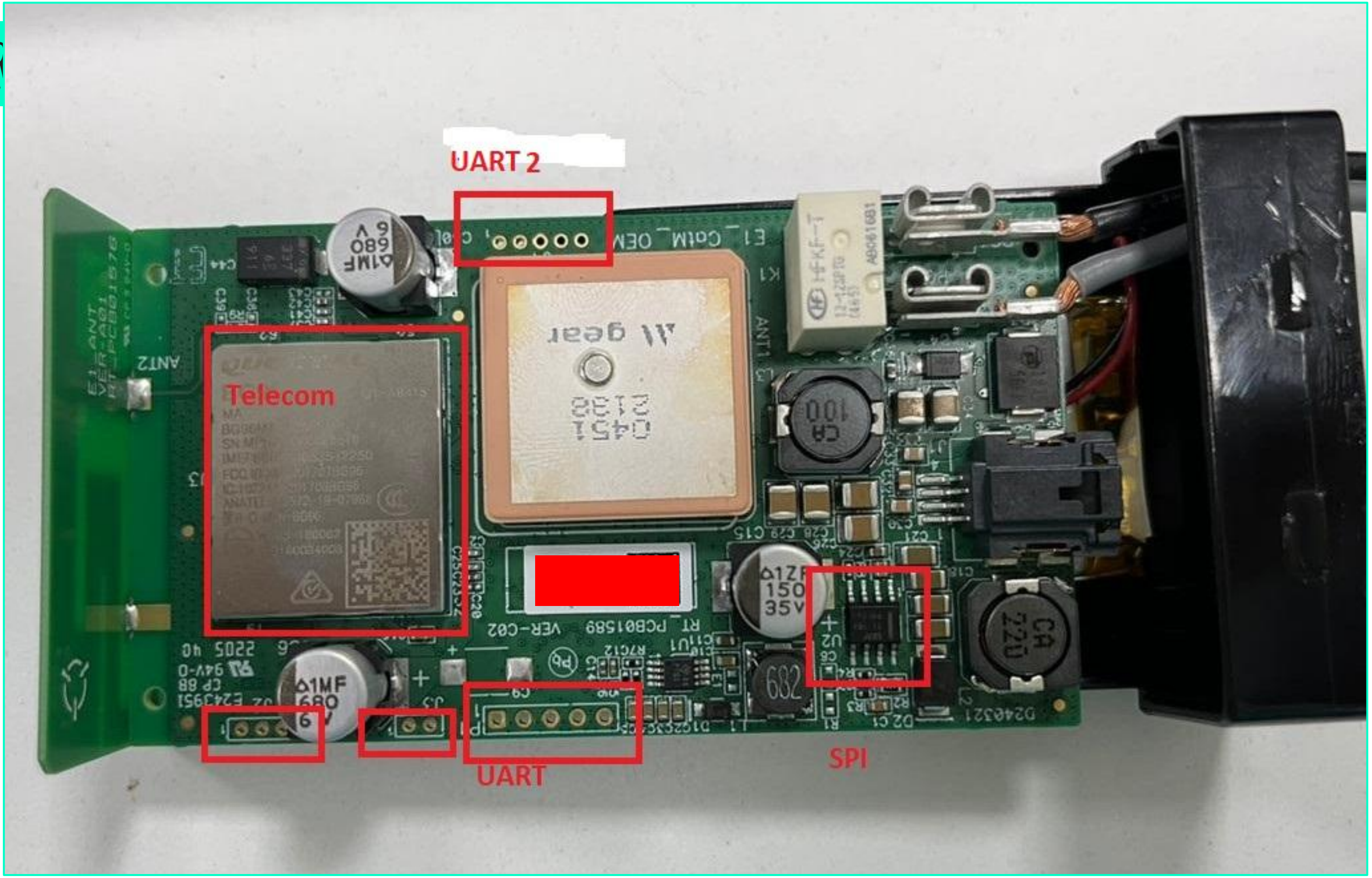
- Telecom Chip
- UART



[redacted]

Communication pr

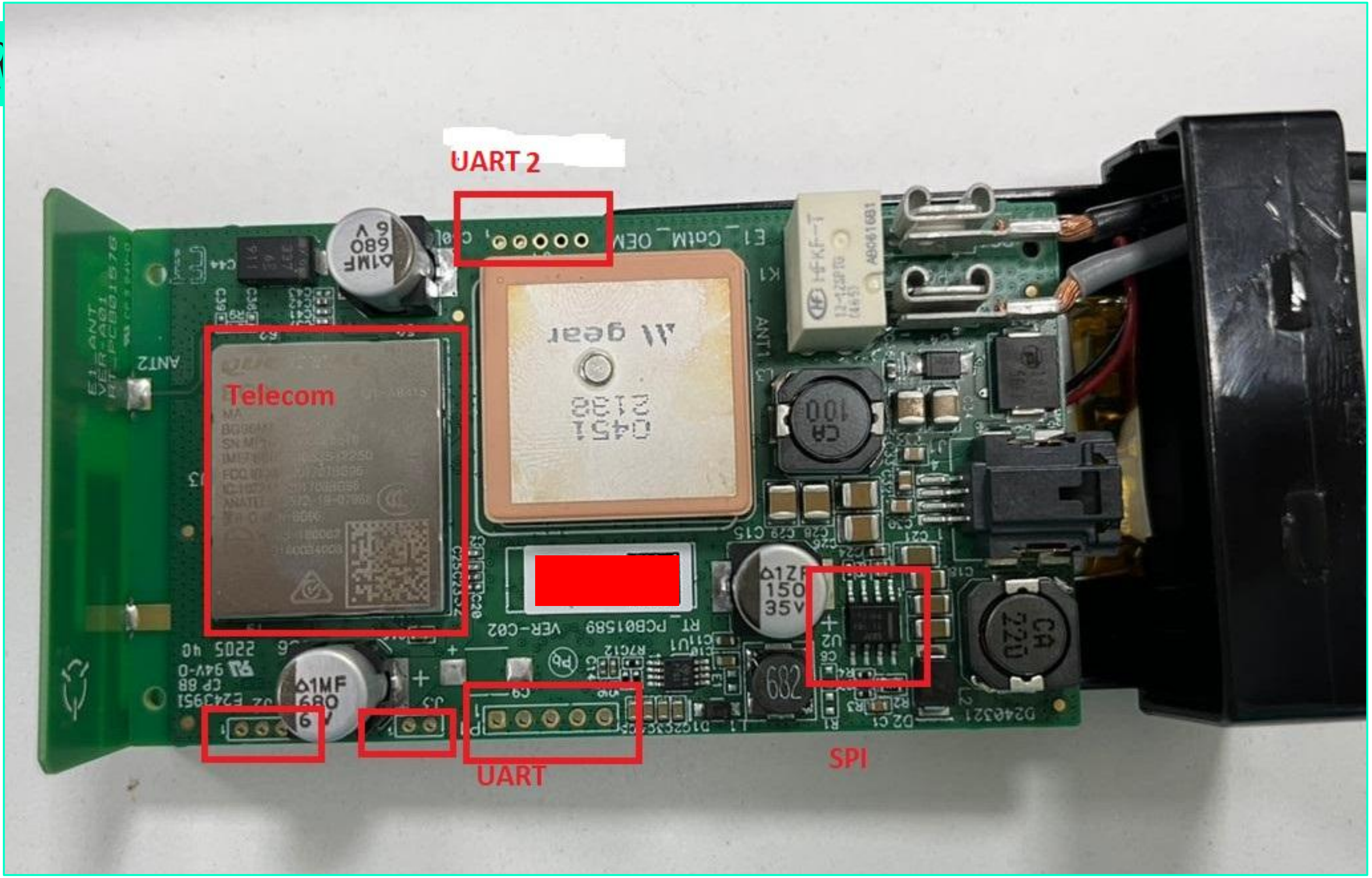
- Telecom Chip
- UART
- SPI



[redacted]

Communication pr

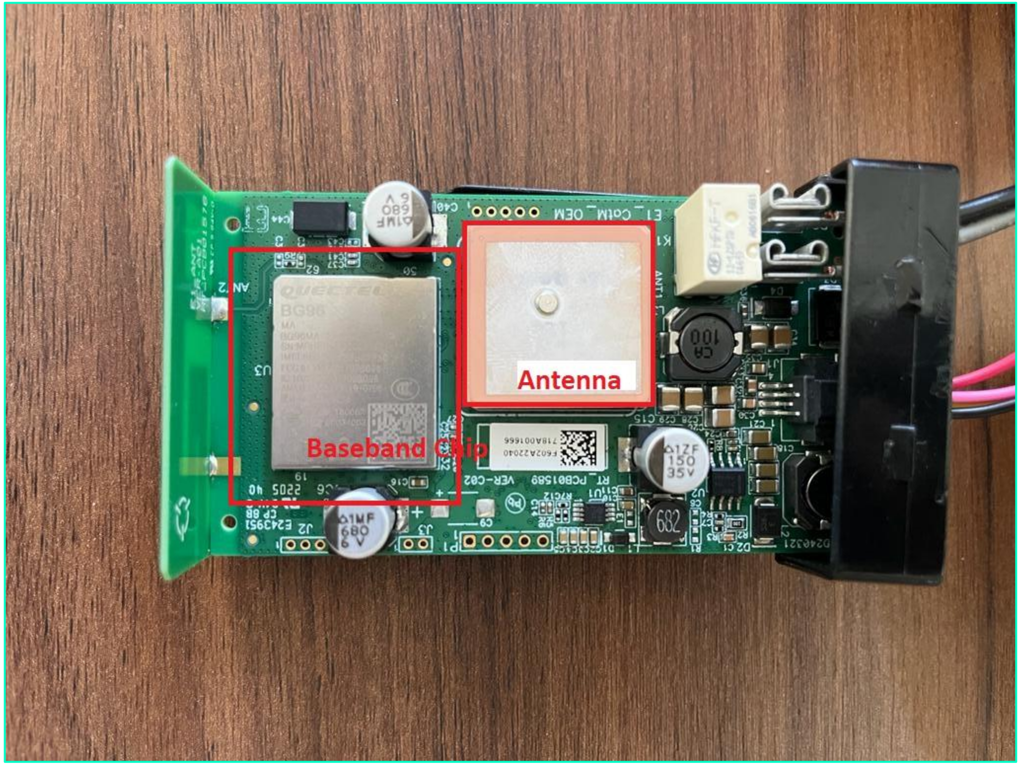
- Telecom Chip
- UART
- SPI
- SoC



[redacted]

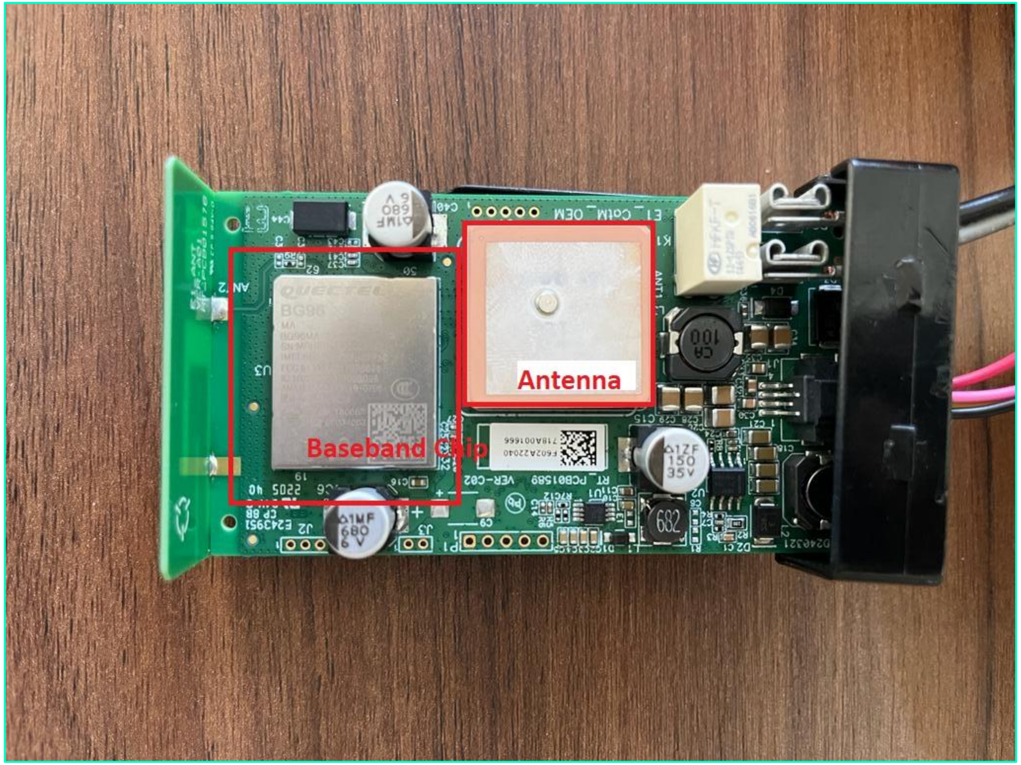
Communication protocol

- Antenna



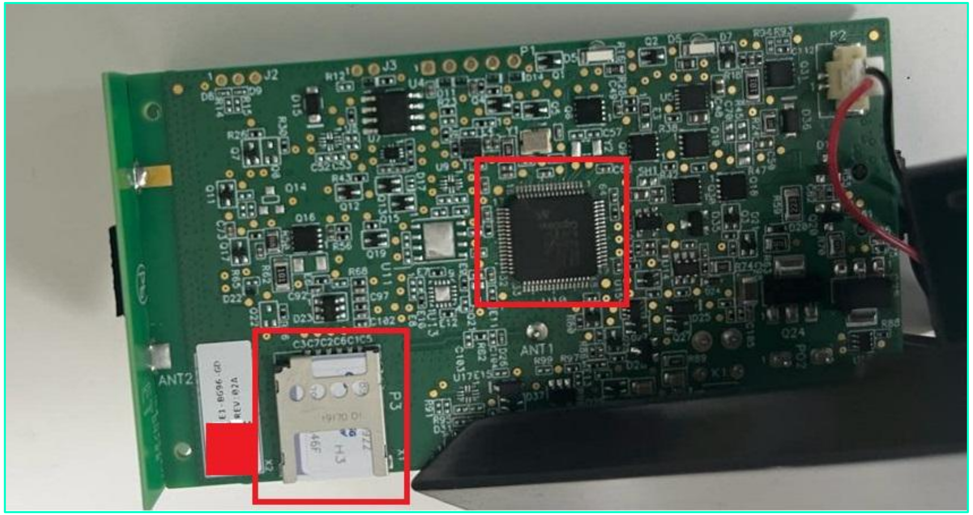
Communication protocol

- Antenna
- Baseband Chip



Communication protocol

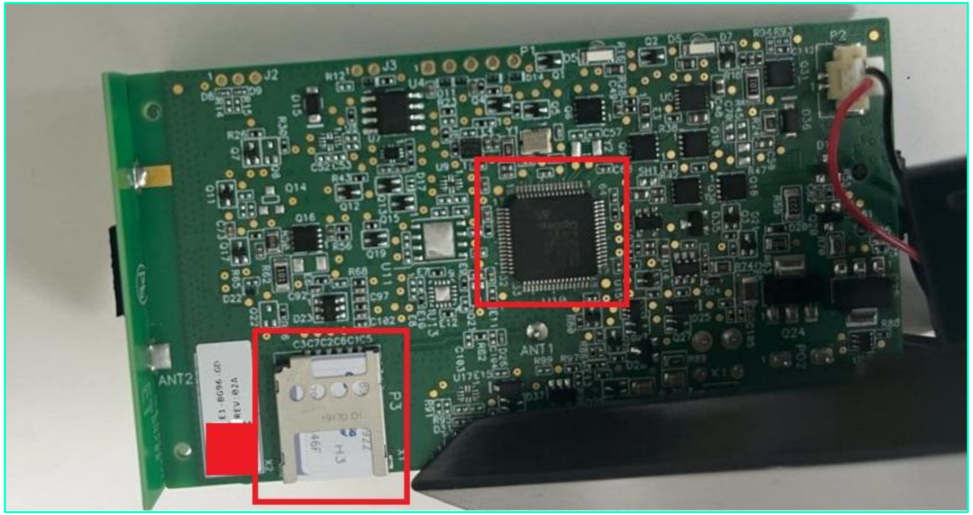
- System on Chip



Bottom View

Communication protocol

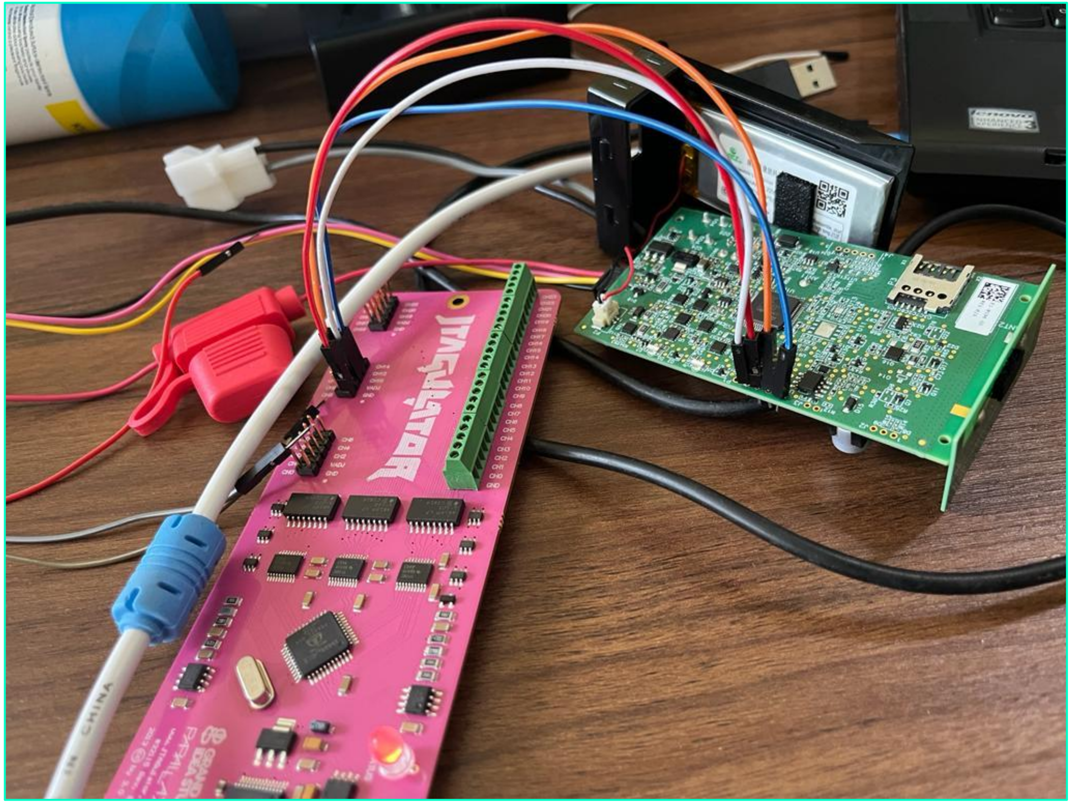
- System on Chip
- Plastic Sim



Bottom View

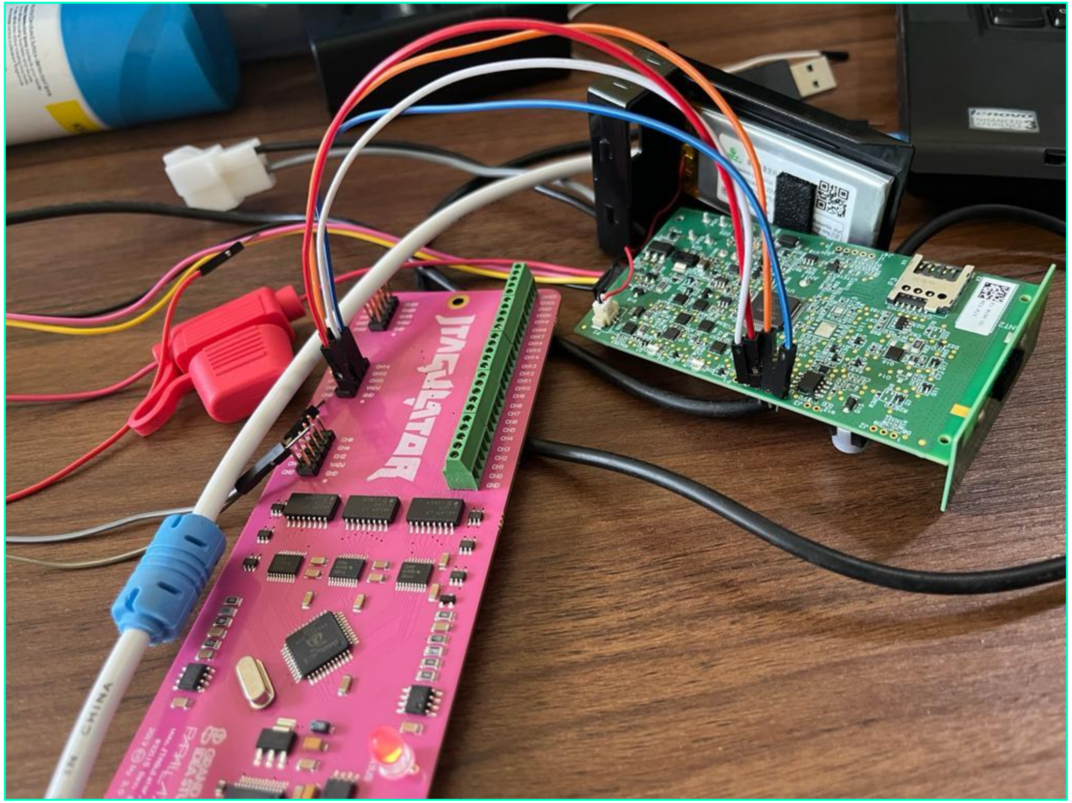
Hardware

- Jtagulator



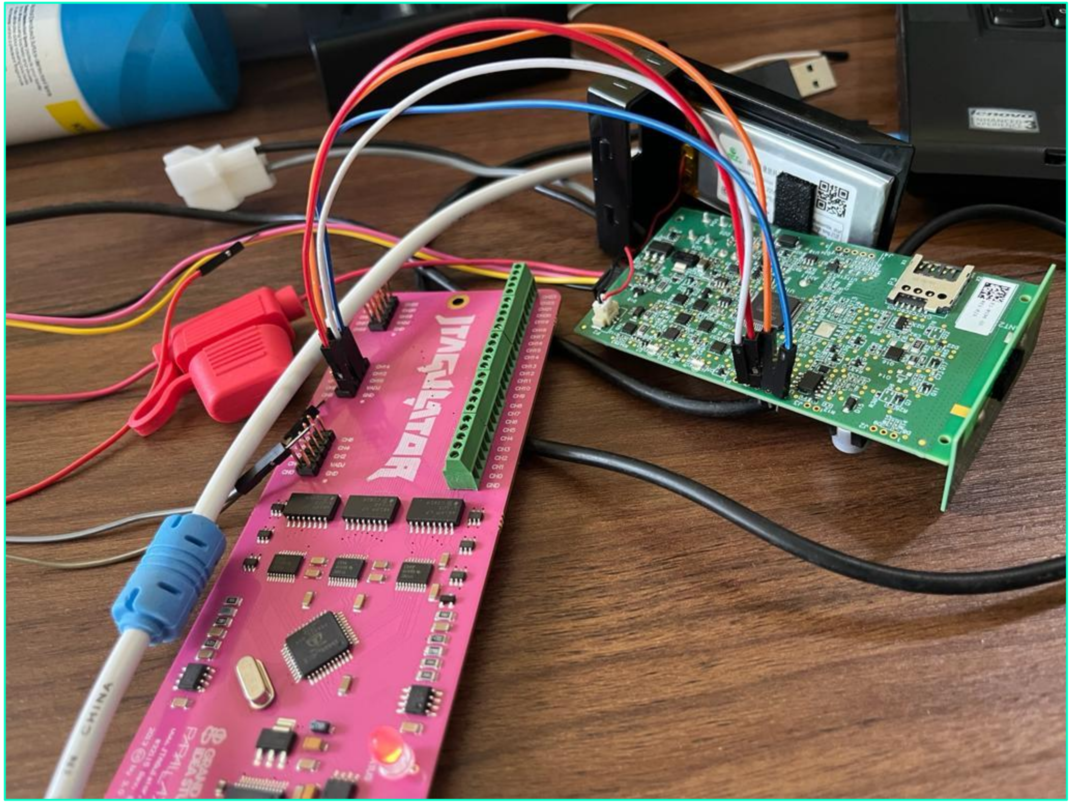
Hardware

- Jtagulator
- Finding pinouts



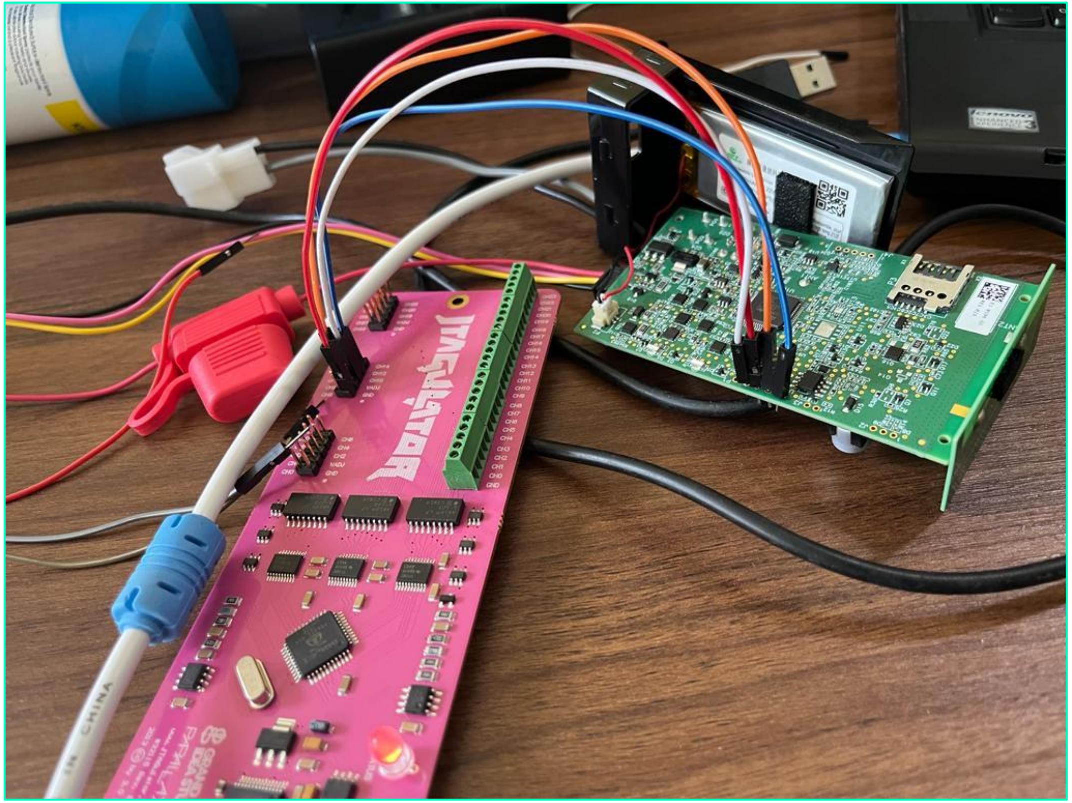
Hardware

- Jtagulator
- Finding pinouts
- Get a root!



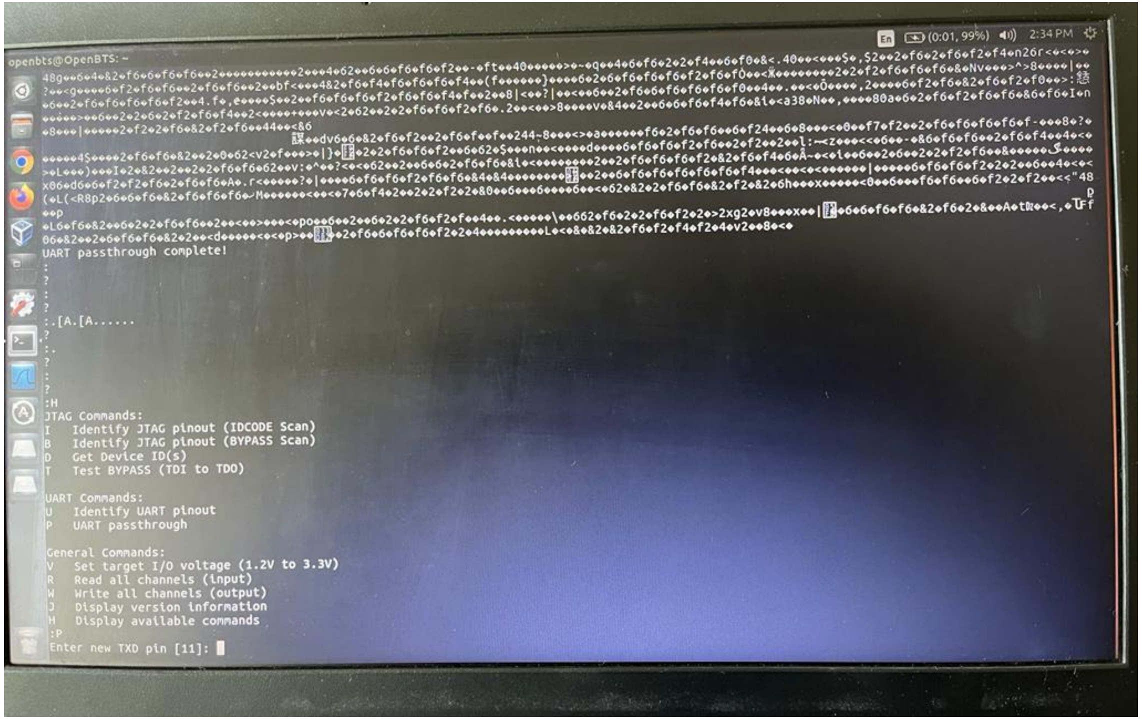
Hardware

- Jtagulator
- Finding pinouts
- Get a root!
- Beer ;)



Hardware

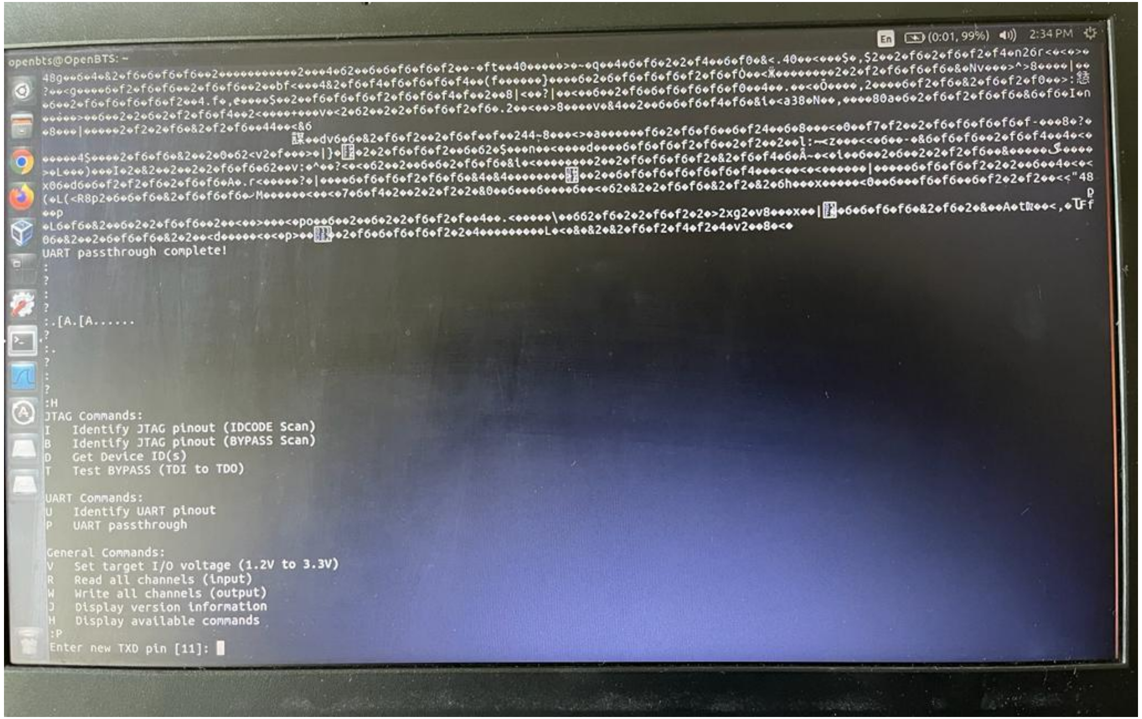
- Jtagulator



```
openbts@OpenBTS: ~
UART passthrough complete!
:
?
:
?
:.[A.[A......
?
:.
?
:
?
:H
JTAG Commands:
I   Identify JTAG pinout (IDCODE Scan)
B   Identify JTAG pinout (BYPASS Scan)
D   Get Device ID(s)
T   Test BYPASS (TDI to TDO)

UART Commands:
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target I/O voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
:P
Enter new TXD pin [11]: 
```

Hardware

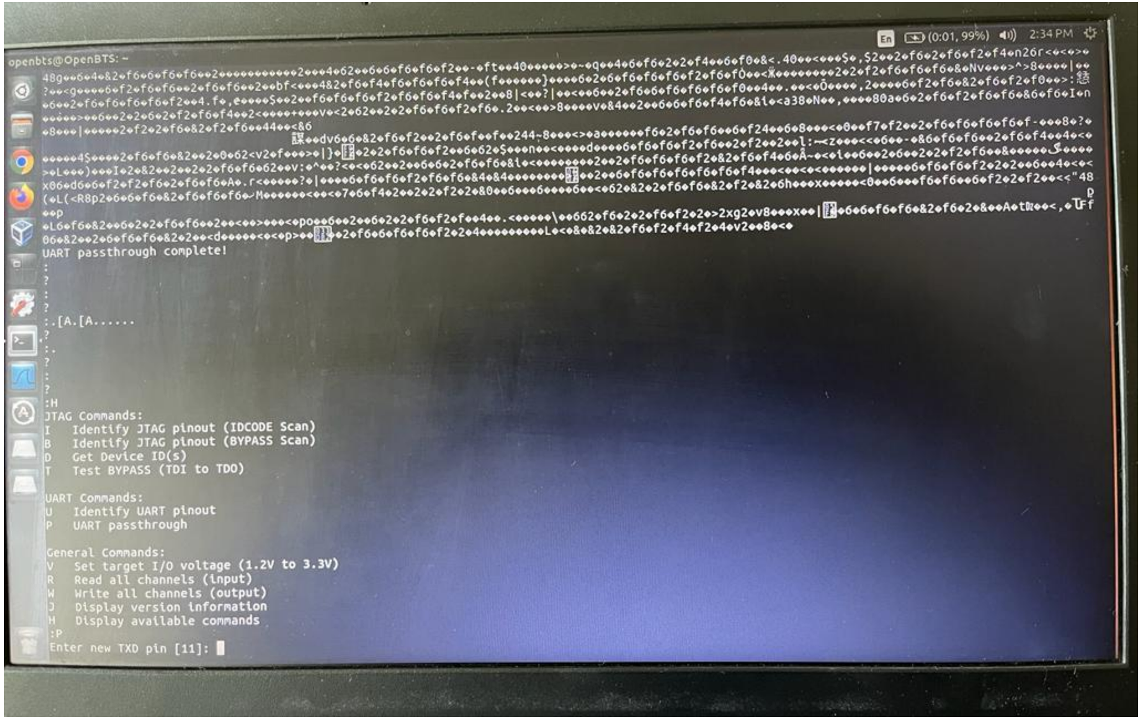
- Jtagulator
- Custom Baud Rate



```
openbts@OpenBTS: ~
UART passthrough complete!
:
?
:
?
:.[A.[A......
?
:.
?
:
?
:H
JTAG Commands:
I   Identify JTAG pinout (IDCODE Scan)
B   Identify JTAG pinout (BYPASS Scan)
D   Get Device ID(s)
T   Test BYPASS (TDI to TDO)

UART Commands:
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target I/O voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
:P
Enter new TXD pin [11]: 
```

Hardware

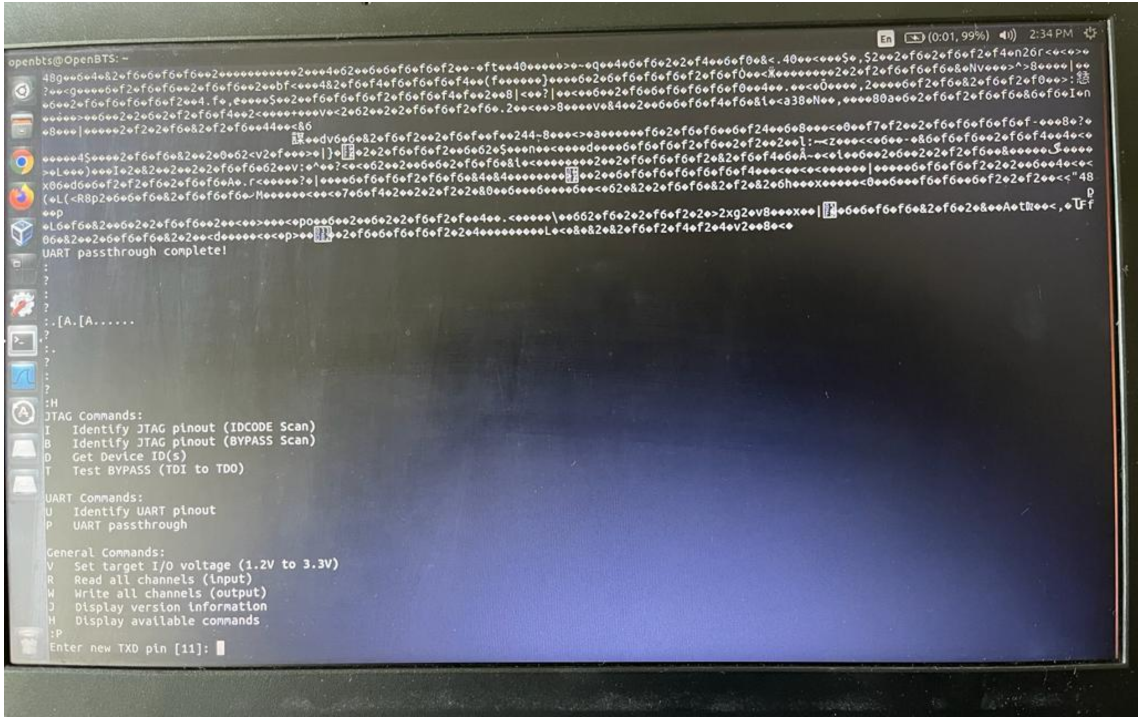
- Jtagulator
- Custom Baud Rate
- UART Passthrough



```
openbts@OpenBTS: ~
48g��6�4�&2�f6�6�f6�f6��2����������2���4�62��6�6�f6�f6�f2��-�ft��40�����>�~�q��4�6�f6�2�2�f4��6�f0�&<.40��<���$�,$2��2�f6�2�f6�f2�f4�n26r<�<�>�
?��<g�����6�f2�f6�f6��2�f6�f6��2��bf<���4&2�f6�f4�f6�f6�f6�f4��(f������}����6�2�6�f6�f6�f6�f2�f6�f0��<Ж��������2�2�f2�f6�f6�f6�&�Nv����>^>8����|��
�6��2�f6�f6�f6�f6�f2��4.f�,�����$��2��f6�f6�f6�f2�f6�f6�f4�f��2��8|<��?|��<��6��2�f6�6�f6�f6�f6�f0���4��.��<�Ō����,2�����6�f2�f6�&2�f6�f2�f0���>:
������>��6��2�2�6�2�f2�f6�f4��2<�����+���V�<2�62��2�2�f6�f6�f2�f6�.2��<��>8�����V�&4��2��6�6�f6�f4�f6�&l�<a38�N��,����80a�6�2�f6�f2�f6�f6�&6�f6�I�n
�8���|�����2�f2�2�f6�&2�f2�f6���44��<&6
        ��dv6�6�&2�f6�f2��2�f6�f��f��244-8���<>�a������f6�2�f6�f6���6�f24��6�8���<�0��f7�f2��2�f6�f6�f6�f6�f-���8�?�
�����4$�����2�f6�f6�&2��2�0�62<v2�f���>�|}��2�2�f6�f6�f2��6�62�$���n��<����d����6�f6�f6�f2�f6��2�f2��2��l:~<z���<<�6��-�&6�f6�f6��2�f6�f4��4�<�
>�L���)���I�2�&2��2��2�2�f6�f6�62��v:�^��?<�<�62��2��6�6�2�f6�f6�&l�<��������2��2�f6�f6�f6�f2�&2�f6�f4�6�Å~�<�l��6��2�6��2�2�f2�f6��&������$����
x06�d6�6�f2�f2�f6�2�f6�f6�A�.r<�����?�|����6�f6�f6�f2�f6�f6�&4�&4��������2��6�f6�f6�f6�f6�f6�f4���<��<�<������|�����6�f6�f6�f2�2�2��6��4�<�<
(�L(<R8p2�6�6�f6�&2�f6�f6�f6�~M������<��<�7�6�f4�2��2�2�f2�2�&0��6����6�����6��<�62�&2�2�f6�f6�&2�f2�&2�6h���x�����<0��6����f6�f6��6�f2�2�f2��<"48
��p
�L6�f6�&2��6�2�2�f6�f6��2��<��>���<�po��6��2��6�2�2�f6�f2�f��4��.<�����\��662�f6�2�2�f6�f2�2�>2xg2�v8���x��|�6�6�f6�f6�&2�f6�2�&��A�t��<,�Ff
06�&2��2�6�f6�f6�&2�2��<d�����<�<�p>����2�f6�6�f6�f6�f2�2�4���������L�<�&�&2�&2�f6�f2�f4�f2�4�v2��8�<�
UART passthrough complete!
:
?
:
?
:.[A.[A......
?
:.
?
:
?
:H
JTAG Commands:
I   Identify JTAG pinout (IDCODE Scan)
B   Identify JTAG pinout (BYPASS Scan)
D   Get Device ID(s)
T   Test BYPASS (TDI to TDO)

UART Commands:
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target I/O voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
:P
Enter new TXD pin [11]: 
```

Hardware

- Jtagulator
- Custom Baud Rate
- UART Passthrough
- Pinout Scan

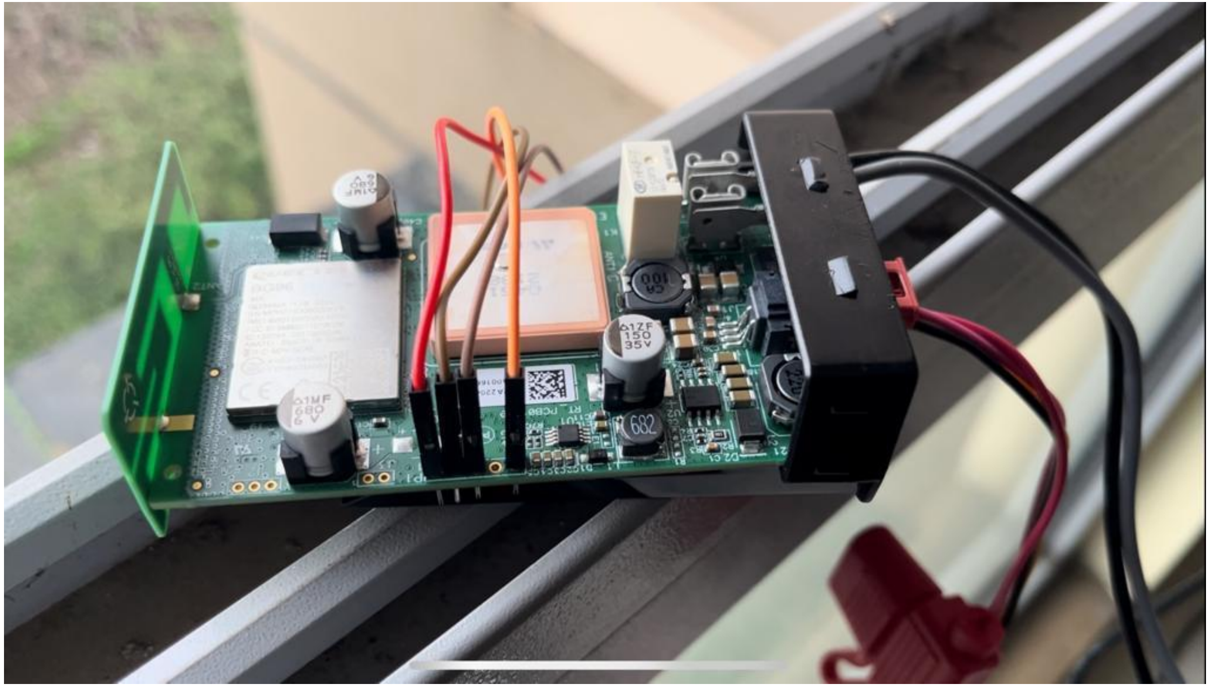


```
openbts@OpenBTS: ~
[illegible]
UART passthrough complete!
:
?
:
?
:.[A.[A......
?
:.
?
:
?
:H
JTAG Commands:
I   Identify JTAG pinout (IDCODE Scan)
B   Identify JTAG pinout (BYPASS Scan)
D   Get Device ID(s)
T   Test BYPASS (TDI to TDO)

UART Commands:
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target I/O voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
:P
Enter new TXD pin [11]: 
```

GPS

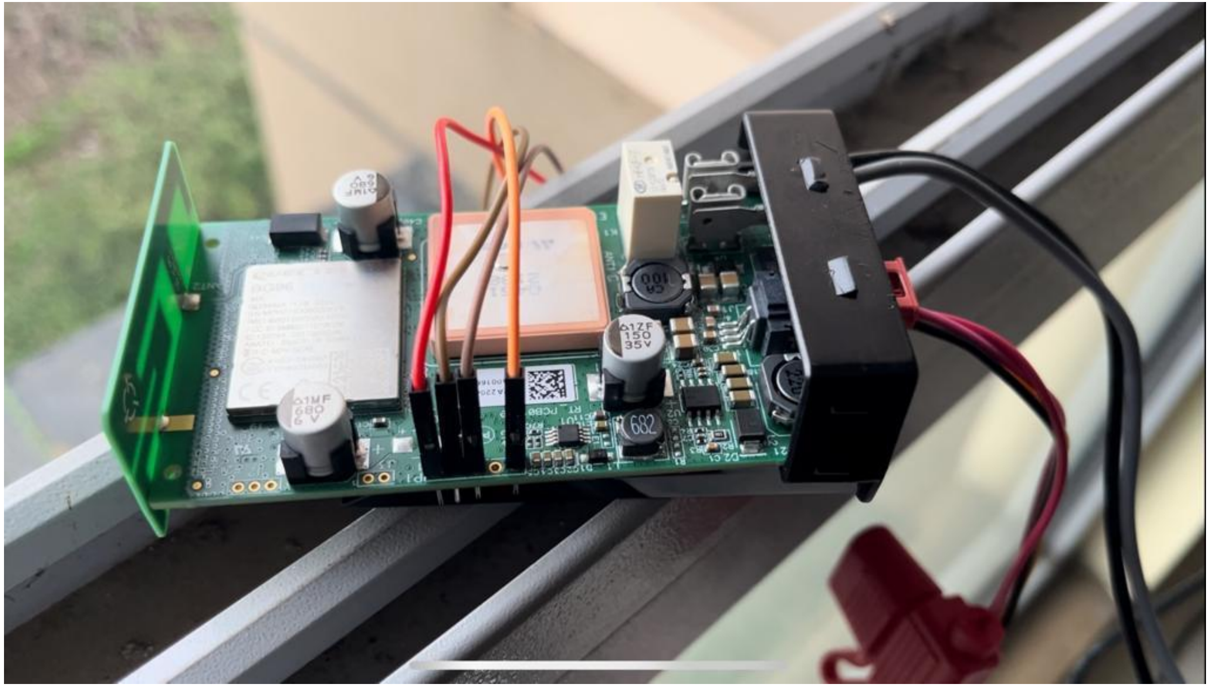
GPS

- GPS Spoofing



GPS

- GPS Spoofing
- GPS Jamming

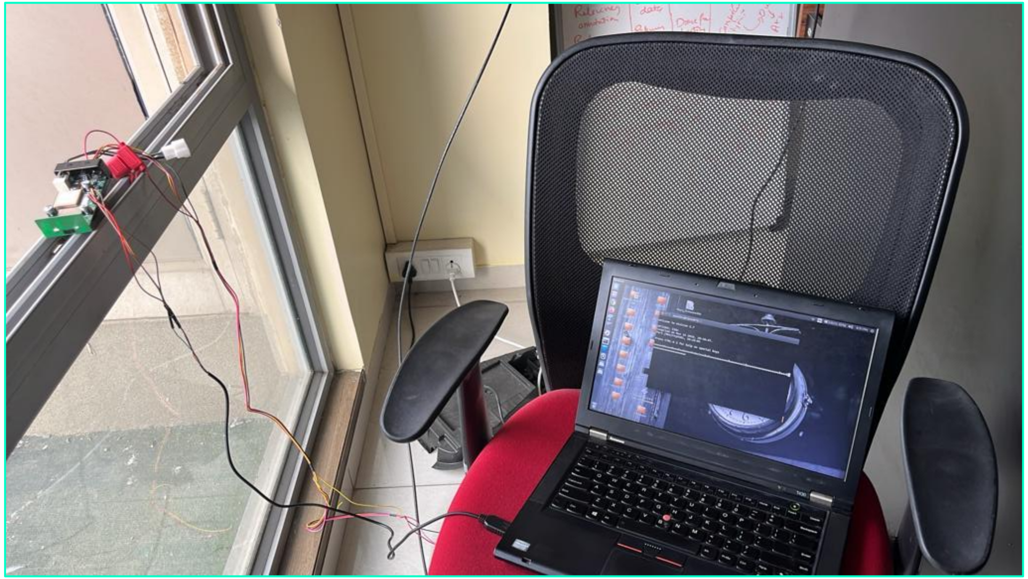


GPS

- Setup

GPS

- Setup
- TTL Data on UART

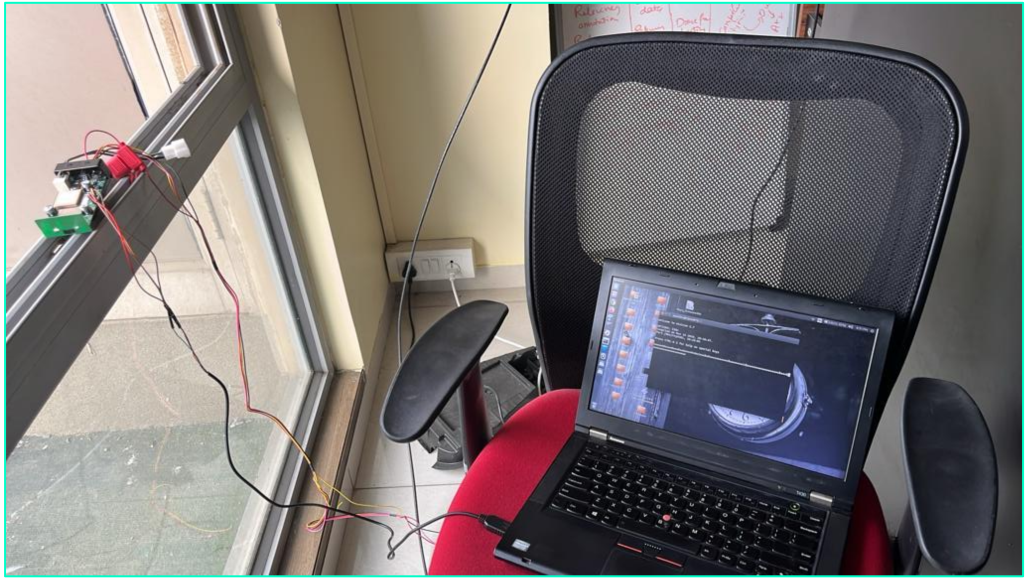


GPS

- Setup
- TTL Data on UART
- Custom baudrate

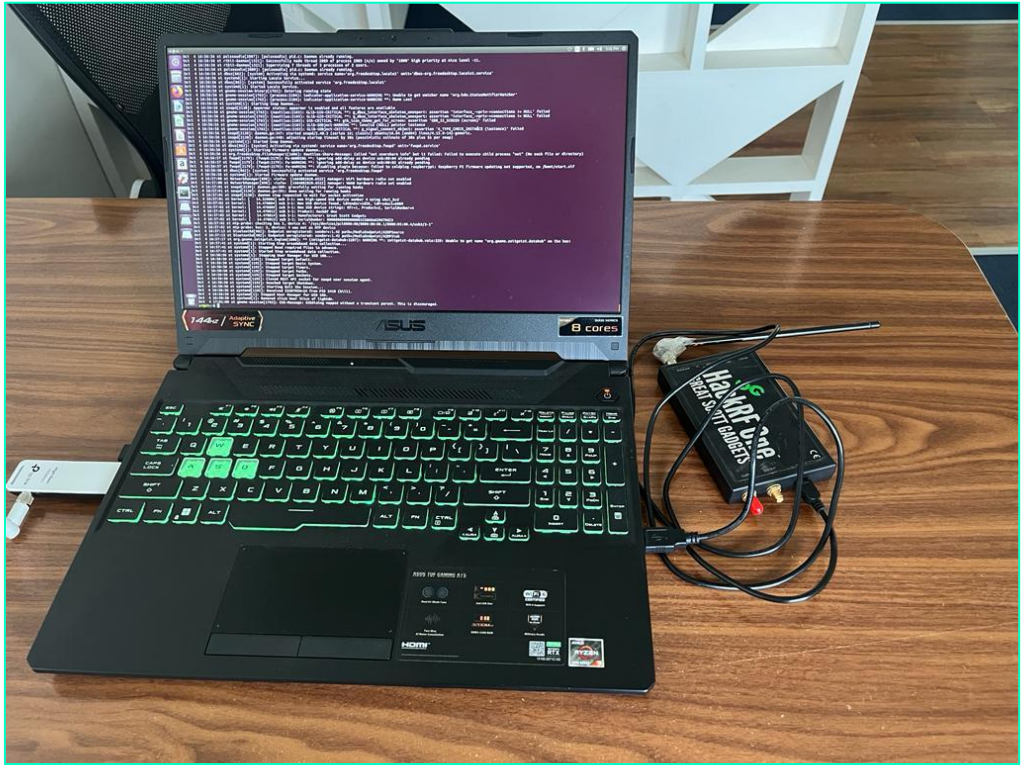
GPS

- Setup
- TTL Data on UART
- Custom baudrate
- Jtagulator



GPS

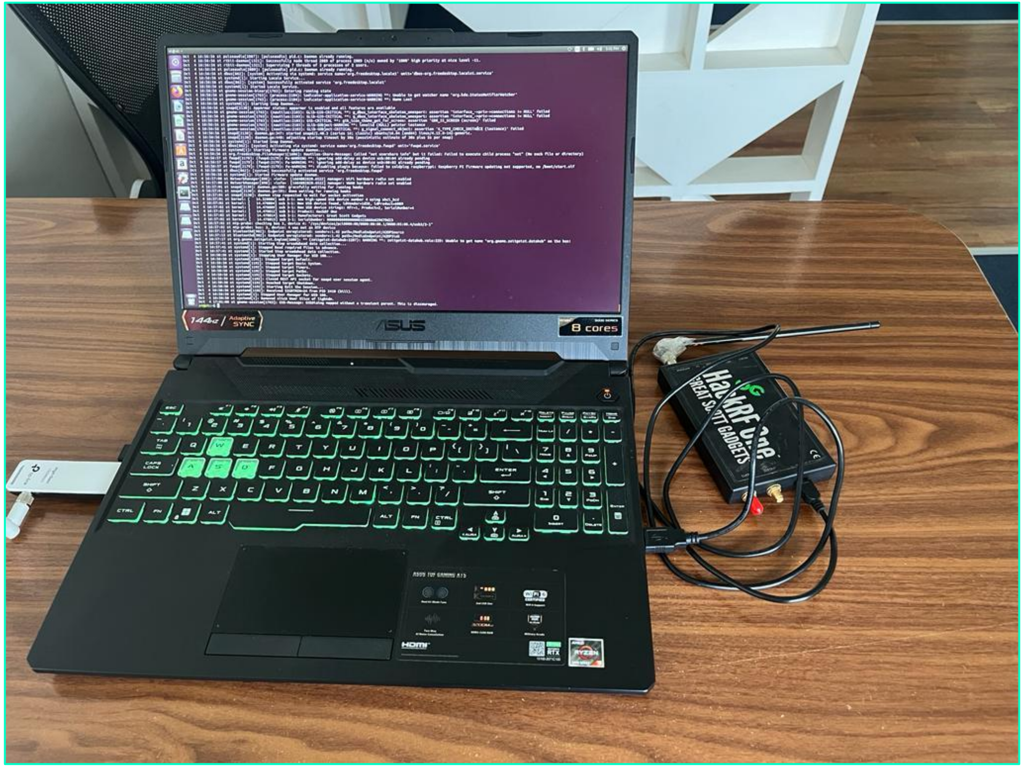
- Setup for GPS



Refer: https://www.rtl-sdr.com/using-a-hackrf-for-gps-spoofing-on-windows/

GPS

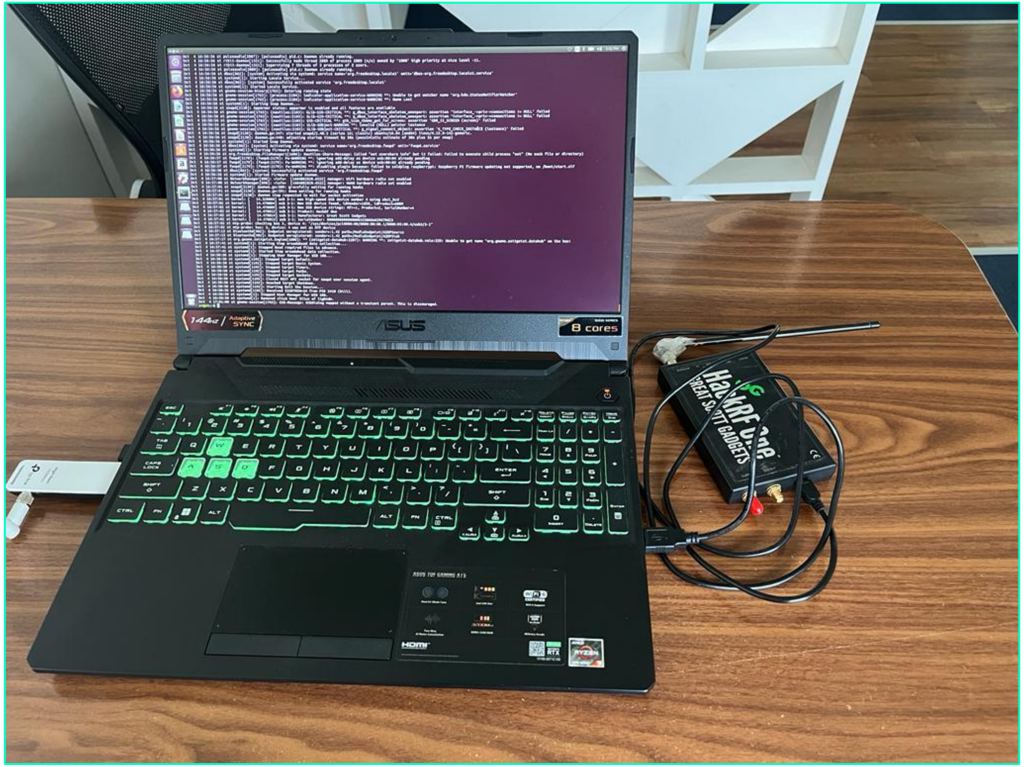
- Setup for GPS
- Jamming



Refer: https://www.rtl-sdr.com/using-a-hackrf-for-gps-spoofing-on-windows/

GPS

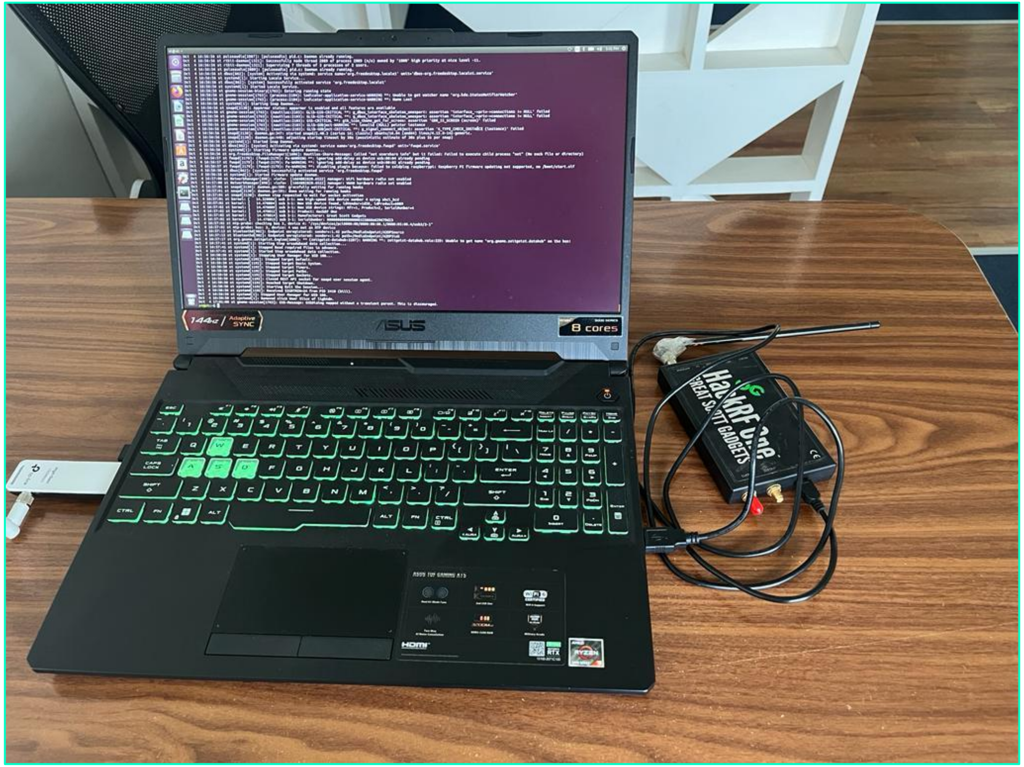
- Setup for GPS
- Jamming
- Spoofing



Refer: https://www.rtl-sdr.com/using-a-hackrf-for-gps-spoofing-on-windows/

GPS

- Setup for GPS
- Jamming
- Spoofing
- Simulation



Refer: https://www.rtl-sdr.com/using-a-hackrf-for-gps-spoofing-on-windows/

Conclusion

- Telematics plays a major role in Car Hacking

Conclusion

- Telematics plays a major role in Car Hacking
- Companies should focus some attention on this component which can lead to havocs!

Conclusion

- Telematics plays a major role in Car Hacking
- Companies should focus some attention on this component which can lead to havocs!
- Mitigation and security must be given a thought on this

Conclusion

- Telematics plays a major role in Car Hacking
- Companies should focus some attention on this component which can lead to havocs!
- Mitigation and security must be given a thought on this
- One must know the severity of these flaws.

Q/A

Lets talk?

THANKS!

That’s all folks,

Connect me on LinkedIn ;)