

BOSSA PLATFORM

Spring 2018 IPRO

Motivation

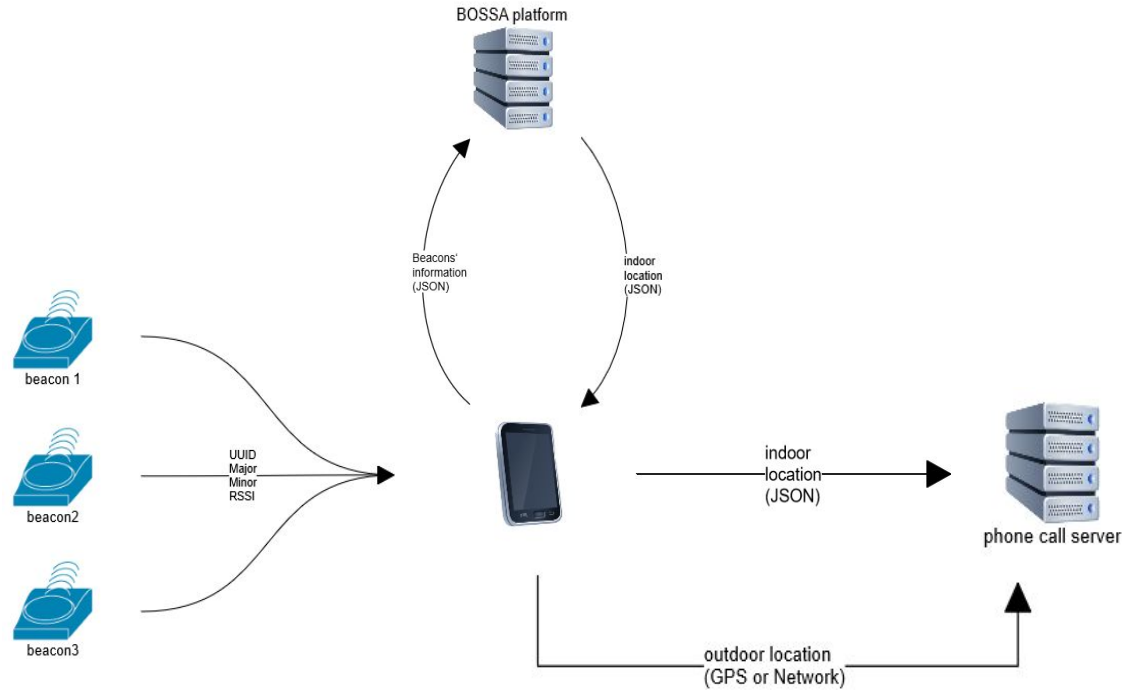
- In California, more than half of cellphone calls didn't transmit location to 911 from 2011 to 2013, and it's getting worse. Last year, about 12.4 million, or 63%, of California's cellphone calls to 911 didn't share location.
- In Texas, two-thirds of cellphone calls in a sample of calls from major cities – including Austin and Houston – reached 911 without an instant fix on location from 2010 through 2013.

- *USA Today*

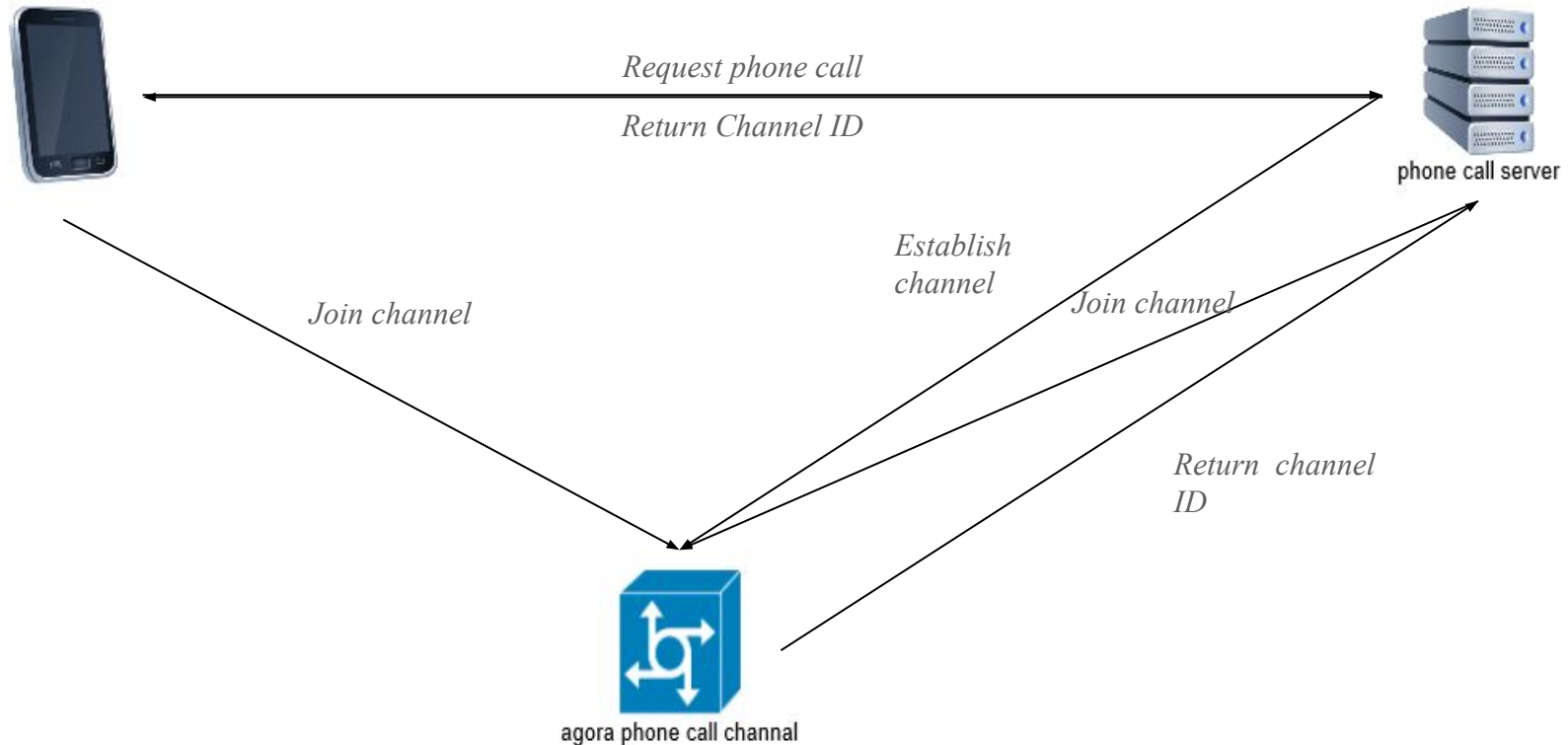
*“More than **10,000 people**, who would otherwise be saved, **die every year** when calling 911 from a cellphone because emergency dispatchers can’t **get a quick and accurate location on them**”*

Our Solution

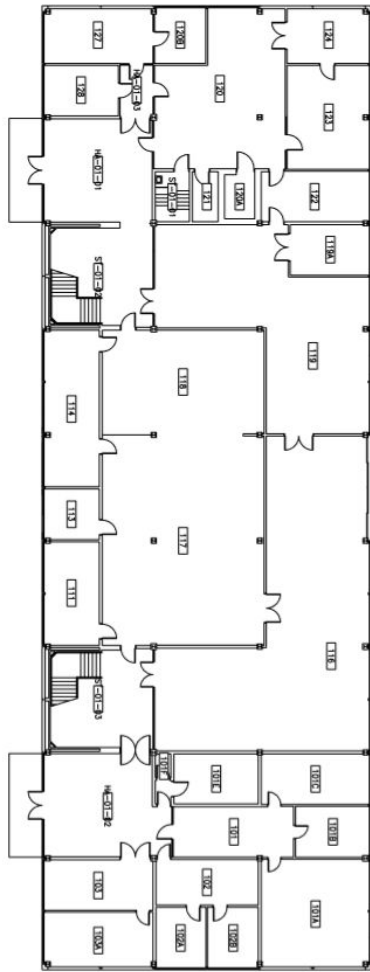
WebRTC PSAP Application



WebRTC PSAP Application

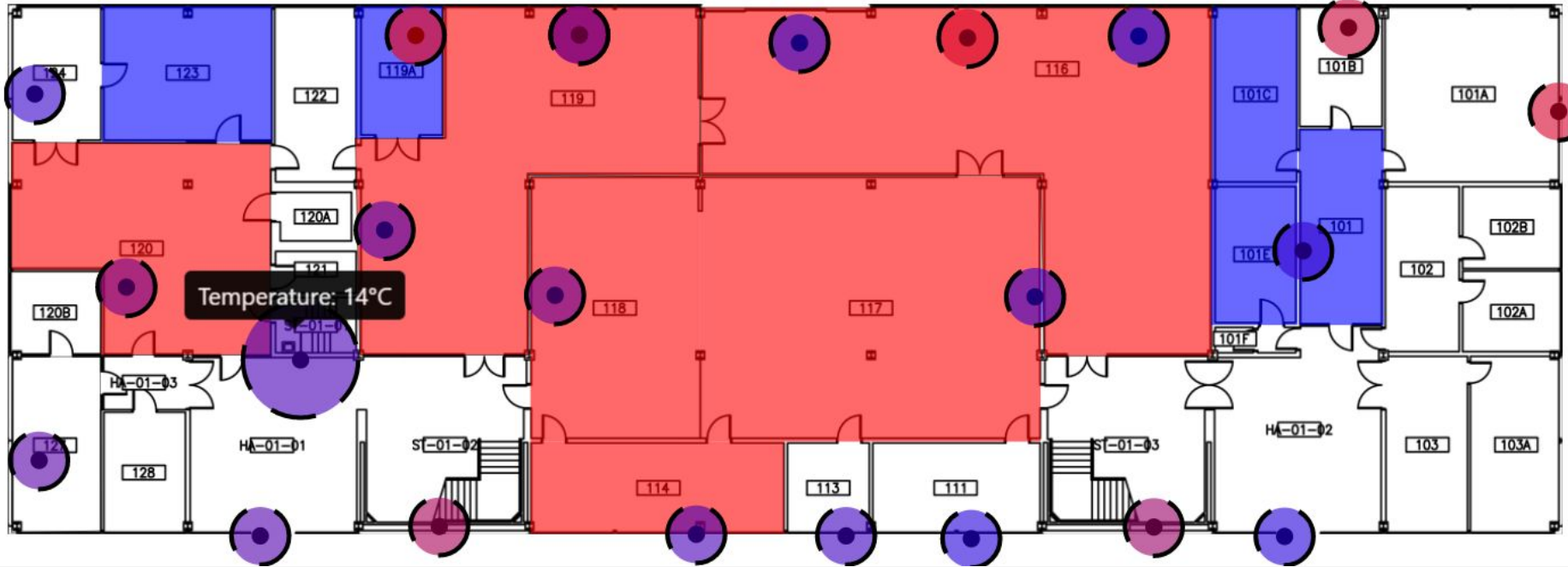


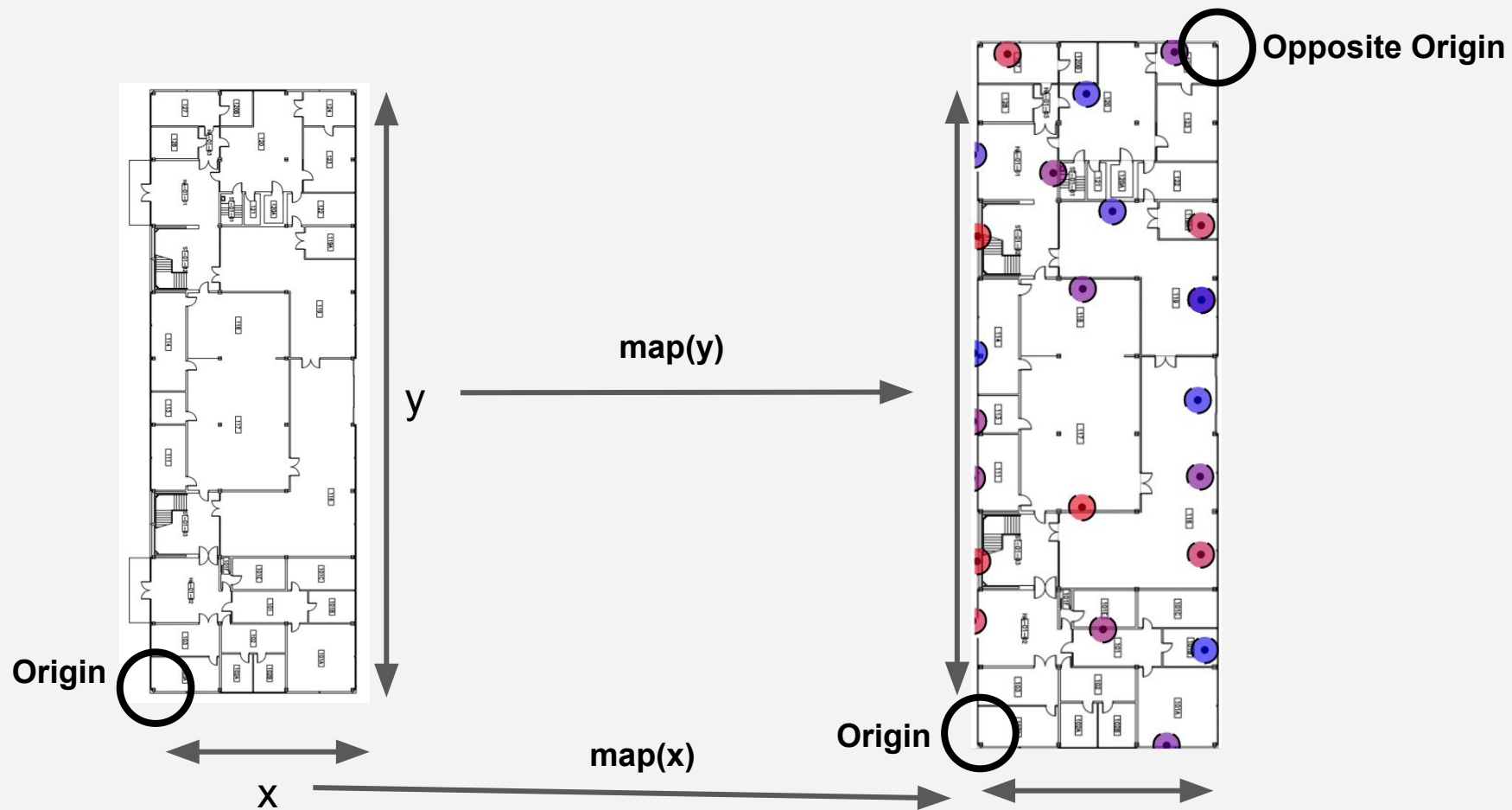
Mapping



Convert static
PNG/PDF/JPG of floor plan
to something that can be
used for visualization.

Scalable Vector Graphics (SVG)



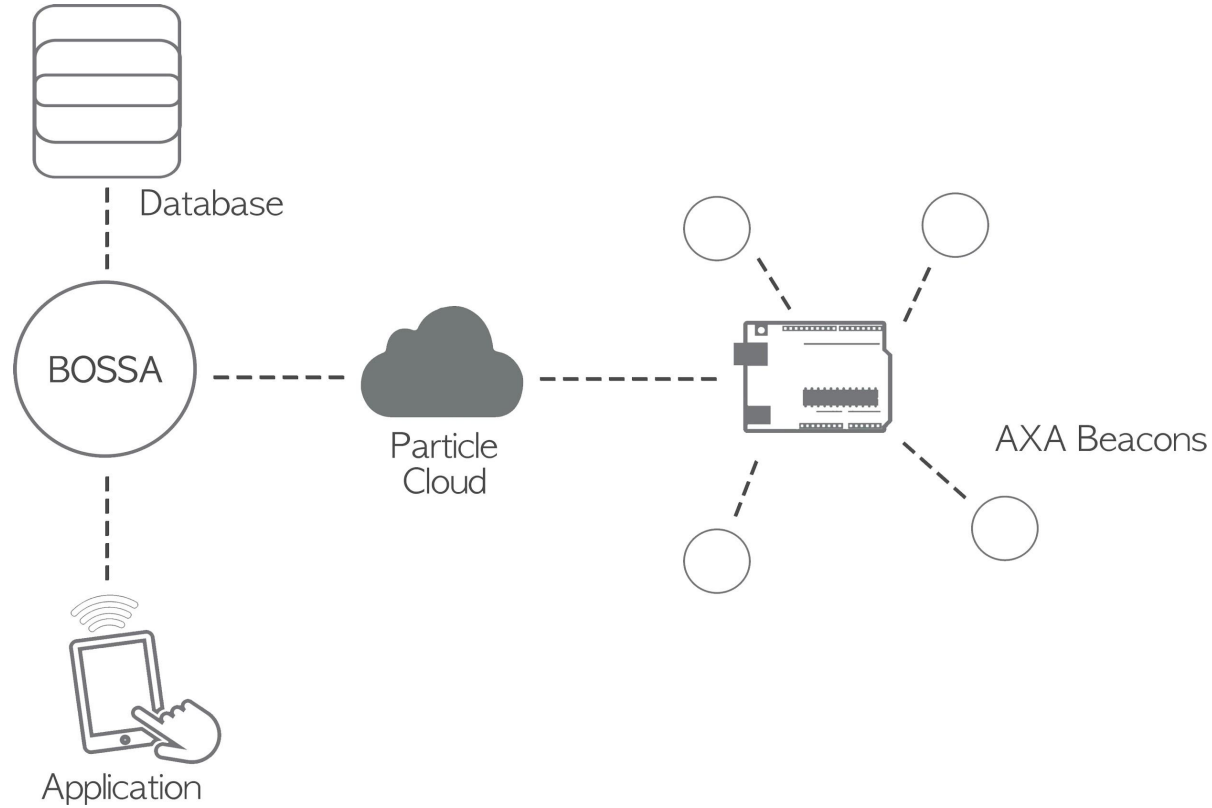


Facilities Application Demo

API / DATABASE

api

database





`https://api.iitrtclab.com/deployment/beacon`

```
{  
  "loc_id": 169,  
  "id": "A0:E6:F8:69:8F:F6",  
  "major": 1000,  
  "minor": 540  
},
```

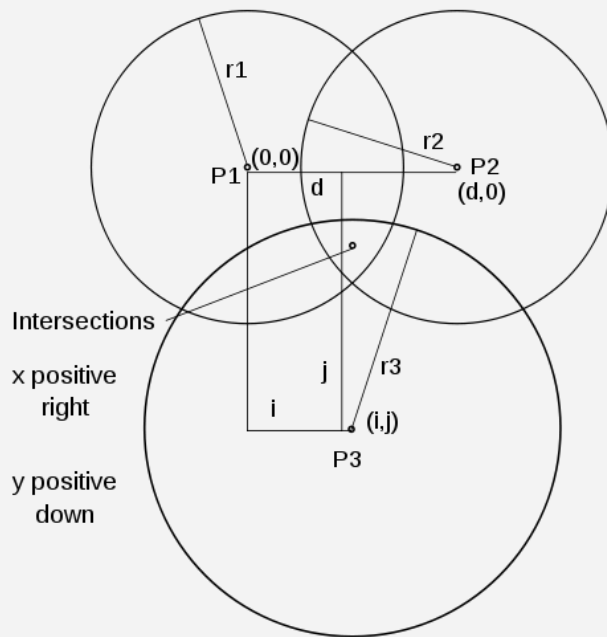
`https://api.iitrtclab.com/map/location?id=169`

```
{  
  "building_id": 4,  
  "id": 169,  
  "floor": 2,  
  "room_type": null,  
  "room_number": null,  
  "nearest_wall": null,  
  "comment": null,  
  "x": 21.856458725400003,  
  "y": 18.734667788400003,  
  "z": null  
}
```

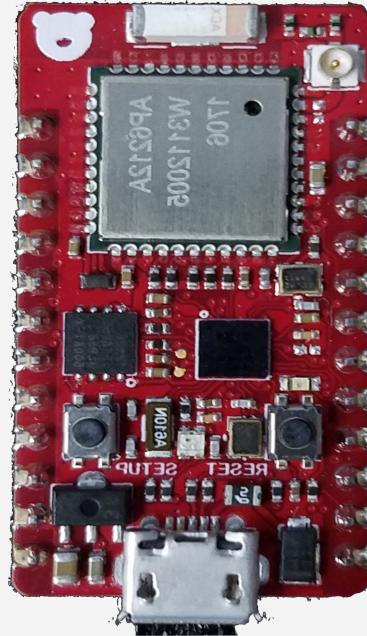

Location Algorithm

Trilateration

Nonlinear Least Squares Fitting



REDBEAR



Important JSON

Redbear Configuration
Version Information Sleeptime Battery (Voltage)

Beacon Update
Beacon MAC Address Temperature Humidity

RSSI Update
Beacon MAC Address RSSI

Algorithm

- Redbear tries to connect to wifi
- Redbear sends its core ID to BOSSA through the Particle cloud and receives a list of MAC addresses of the beacons
- Redbear sends its version and battery to BOSSA
- Redbear connects to the beacons and reports its information to BOSSA

Ubertooth Sniffing

Ubertooth-one : powerful testing tool for sniffing packets from BLE connections.



ActivitiesWireshark

Thu 02:54

stuff.pcapng

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

GATT and ATT packets captured

btl2cap.cid == 0x0004

No.	Time	Source	Destination	Protocol	Length	Info
6	0.101196300	unknown_0x50655c6a	unknown_0x50655c6a	ATT	40	UnknownDirection Exchange MTU Request, Client Rx MTU: 48
9	0.131425600	unknown_0x50655c6a	unknown_0x50655c6a	ATT	40	UnknownDirection Exchange MTU Response, Server Rx MTU: 23
10	0.161260000	unknown_0x50655c6a	unknown_0x50655c6a	ATT	46	UnknownDirection Find By Type Value Request, GATT Primary Service Decla
13	0.221228500	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Read By Type Request, GATT Characteristic Declaration,
15	0.251584200	unknown_0x50655c6a	unknown_0x50655c6a	ATT	60	UnknownDirection Read By Type Response, Attribute List Length: 3, Unkno
16	0.281227700	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Read By Type Request, GATT Characteristic Declaration,
17	0.311487700	unknown_0x50655c6a	unknown_0x50655c6a	ATT	46	UnknownDirection Read By Type Response, Attribute List Length: 1, Unkno
18	0.341230000	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Read By Type Request, GATT Characteristic Declaration,
21	0.371454500	unknown_0x50655c6a	unknown_0x50655c6a	ATT	42	UnknownDirection Error Response - Attribute Not Found, Handle: 0x0028, M
24	0.431454500	unknown_0x50655c6a	unknown_0x50655c6a	ATT	42	UnknownDirection Read Response
140	863.087496800	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Handle Value Notification, Handle: 0x0027 (Unknown: Unl
142	863.567513000	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Handle Value Notification, Handle: 0x0027 (Unknown: Unl
143	864.047530400	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Handle Value Notification, Handle: 0x0027 (Unknown: Unl
230	894.288182600	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Handle Value Notification, Handle: 0x0027 (Unknown: Unl

DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)

Bluetooth Low Energy Link Layer

Access Address: 0x50655c6a

[Master Address: AmpakTec_11:c2:2f (b0:f1:ec:11:c2:2f)]

[Slave Address: TexasIns_69:f9:85 (a0:e6:f8:69:f9:85)]

Data Header: 0x0b06

CRC: 0x1fa8a9

Bluetooth L2CAP Protocol

00000000000018009300000036750c00009a0900.....6u.....

00106bc77346020200006a5c6550060b0700k.sF....j\ep....

002004001b2700161c171bf81595...'.....

DLT User (user_dlt), 20 bytes

Packets: 291 · Displayed: 14 (4.8%) · Load time: 0:0.5 · Profile: Default

GATT PACKET A DEEPER LOOK

Expression...

Time	Source	Destination	Protocol	Length	Info
0.251584200	unknown_0x50655c6a	unknown_0x50655c6a	ATT	60	UnknownDirection Read By Type Response, Attribute List Length: 3, Unknown
0.281227700	unknown_0x50655c6a	unknown_0x50655c6a	ATT	44	UnknownDirection Read By Type Request, GATT Characteristic Declaration, ...
0.311487700	unknown_0x50655c6a	unknown_0x50655c6a	ATT	46	UnknownDirection Read By Type Response, Attribute List Length: 1, Unknown

```
[UUID: Unknown (0xfffd2)]
  UUID: Unknown (0xfffd2)
- Attribute Data, Handle: 0x0023, Characteristic Handle: 0x0024, UUID: Unknown
  - Handle: 0x0023: Unknown: GATT Characteristic Declaration
    [Characteristic UUID: Unknown (0xfffd2)]
    [UUID: GATT Characteristic Declaration (0x2803)]
  - Characteristic Properties: 0x00a, Write, Read
    0... .. = Extended Properties: False
    .0.. .. = Authenticated Signed Writes: False
    ..0. .... = Indicate: False
    ...0 .... = Notify: False
    .... 1... = Write: True
    .... .0.. = Write without Response: False
    .... ..1. = Read: True
    .... ...0 = Broadcast: False
  - Characteristic Value Handle: 0x0024: Unknown)
    [UUID: Unknown (0xfffd3)]
    UUID: Unknown (0xfffd3)
  [UUID: GATT Characteristic Declaration (0x2803)]
[Request in Frame: 13]
```

0000	00 00 18 00 93 00 00 00	36 75 0c 00 00 9a 09 00 6u.....
0010	cb 9e 90 31 02 02 00 00	6a 5c 65 50 0a 1b 17 00	...1.... j\ep....
0020	04 00 09 07 1d 00 0a 1e	00 f1 ff 20 00 10 21 00 !
0030	f2 ff 23 00 0a 24 00 f3	ff 1d be ca	..#..\$..

DID WE FINALLY DO IT?

Expression...

```

- Frame 24: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- PPI version 0, 24 bytes
  DLT: 147, Payload: btile (Bluetooth Low Energy Link Layer)
- Bluetooth Low Energy Link Layer
  Access Address: 0x50655c6a
  [Master Address: AmpakTec_11:c2:2f (b0:f1:ec:11:c2:2f)]
  [Slave Address: TexasIns_69:f9:85 (a0:e6:f8:69:f9:85)]
  Data Header: 0x090a
  CRC: 0x290e50
- Bluetooth L2CAP Protocol
  Length: 5
  CID: Attribute Protocol (0x0004)
- Bluetooth Attribute Protocol
  Opcode: Read Response (0x0b)
    0... .... = Authentication Signature: False
    .0.. .... = Command: False
    ..00 1011 = Method: Read Response (0x0b)
  Value: 161c1713

```

Packets: 291 · Displayed: 14 (4.8%) · Load time: 0:0.5 Profile: Default