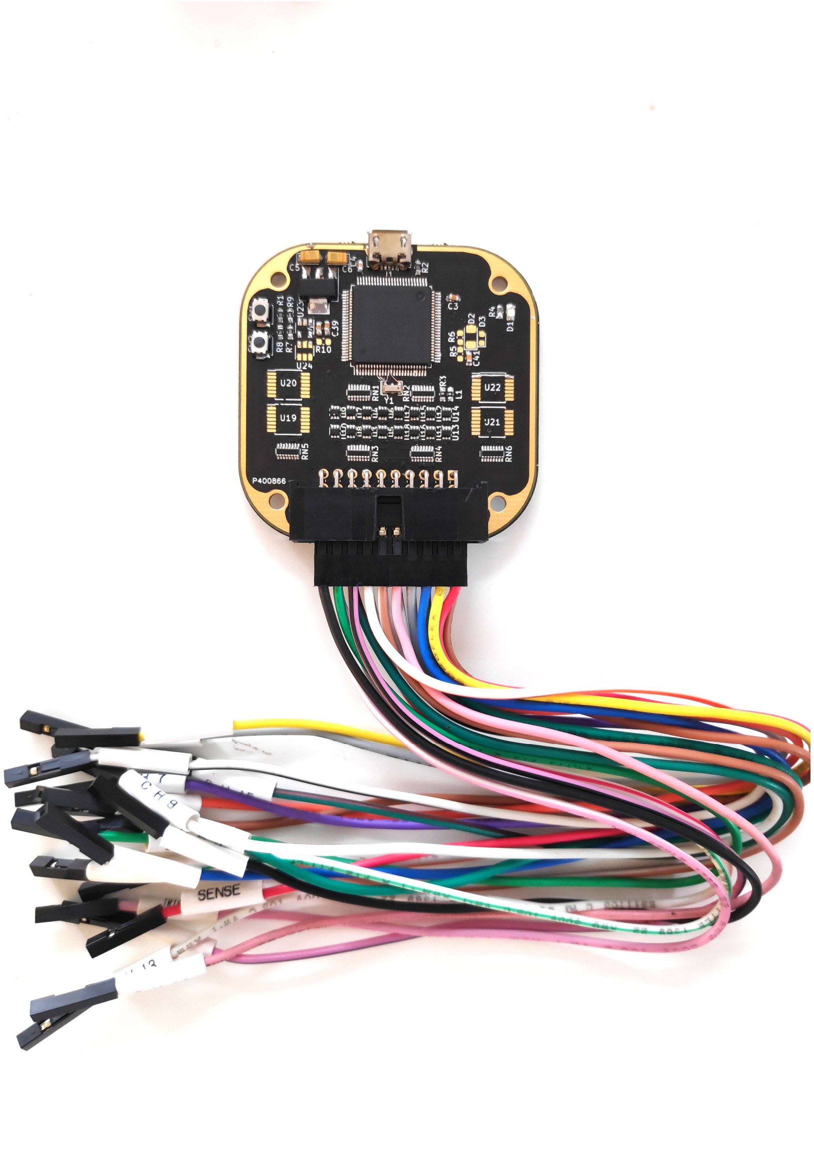
Bus Auditor
Getting Started Guide

EXPLIoT
www.expliot.io



Welcome to the Bus Auditor, quick start guide. This guide is designed to help you through initial setup of hardware and EXPLIoT Framework.

1. System Requirements

- Linux
- Python 3
- One USB port available

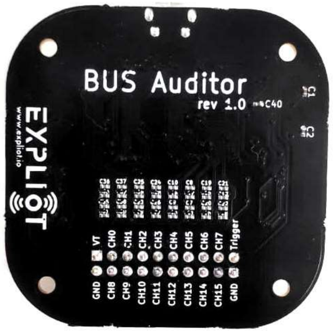
2. Hardware

BUS Auditor is a compact multi-protocol tool used to identify debugging and communication interfaces of unknown hardware devices. It can brute force several hardware protocols including JTAG, arm SWD, UART and I2C.

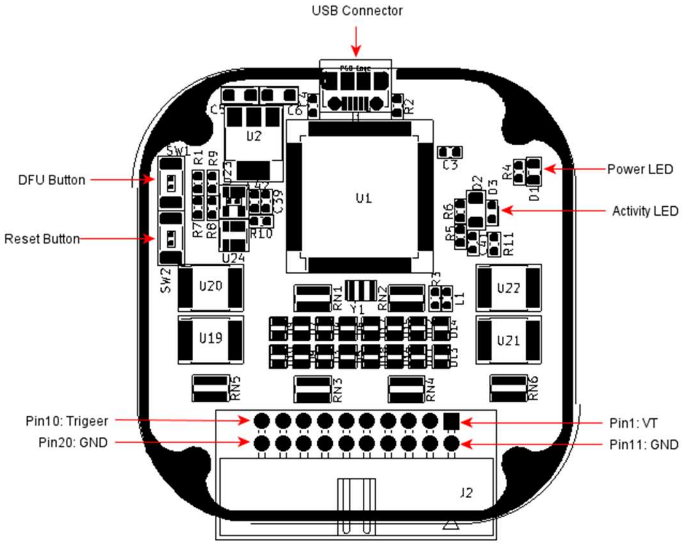
The device has 16 channels, every channel can be used to interface with the target.

The Inbuilt USB port can be used for interface with EXPLIoT framework (Internet of Things Exploitation framework - open source).

EXPLIoT framework (v0.9.5 onwards) provides plugins for JTAG, arm SWD, UART and I2C pin scan.



2.1. Description



2.2. LED Descriptions

Part Name	Description	Functionality
D1	Power LED (RED)	Indicate device is powered up
D3	Activity LED (Blue)	Indicate channel scan is active

2.3. Button Descriptions

Part Name	Description	Functionality
SW2	Reset Button	Device reset
SW1	DFU Button	Activate DFU mode

2.4. Pin Descriptions

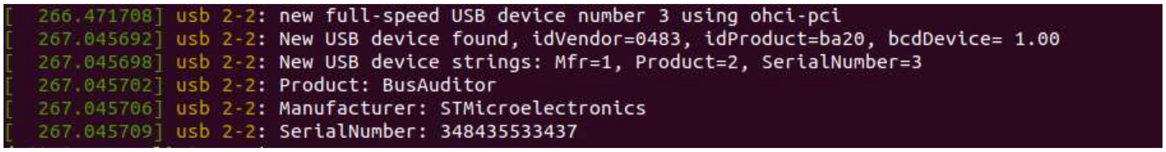
Pin Name	Channel Name	Description	Functionality
Pin 1	Target Voltage (VT)	Target voltage out	Voltage out for test. Supported voltages are 3.3v, 1.8v, and 1.2v
Pin 11, and 20	Ground (GND)	Ground	Ground
Pin 2 to 9, and Pin 12 to 19	Channel 0 to 15	Test Channels	Channel 0 to 15 for protocol scan
Pin 10	Trigger	Trigger	Reserved for future use

2.5. What's included

- Bus Auditor hardware
- 20 Pin connector * 2
- Micro-USB connector

3. Getting Started

1. Download and install EXPLIoT Framework using the instruction given here - https://expliot.readthedocs.io/en/latest/installation/intro.html
2. Connect USB cable between Bus Auditor and the computer where EXPLIoT framework is installed. The Power LED will light up.
3. To verify USB communication with Bus Auditor is working correctly, run '***dmesg***' command. This command will display below information about Bus Auditor device
   a. $ dmesg

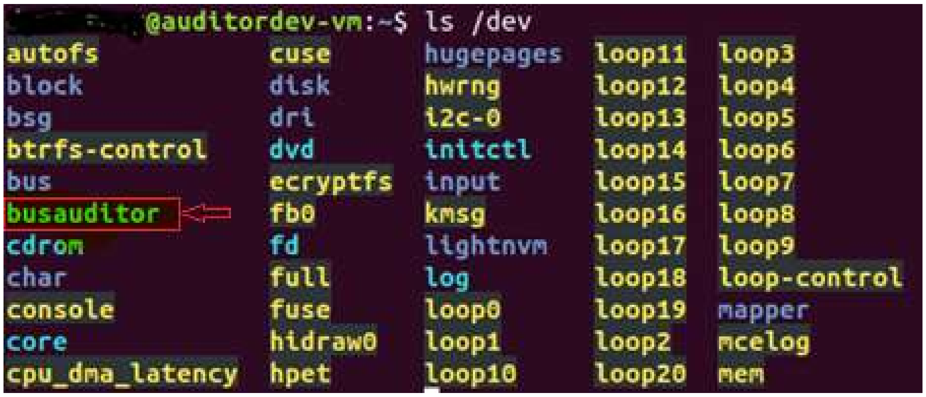


```
[  266.471708] usb 2-2: new full-speed USB device number 3 using ohci-pci
[  267.045692] usb 2-2: New USB device found, idVendor=0483, idProduct=ba20, bcdDevice= 1.00
[  267.045698] usb 2-2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[  267.045702] usb 2-2: Product: BusAuditor
[  267.045706] usb 2-2: Manufacturer: STMicroelectronics
[  267.045709] usb 2-2: SerialNumber: 348435533437
```

4. Add udev rule for Bus Auditor device to grant user level access to USB communication. If udev rule is not added, you will have to run expliot as root for accessing and using Bus Auditor.
   Example:

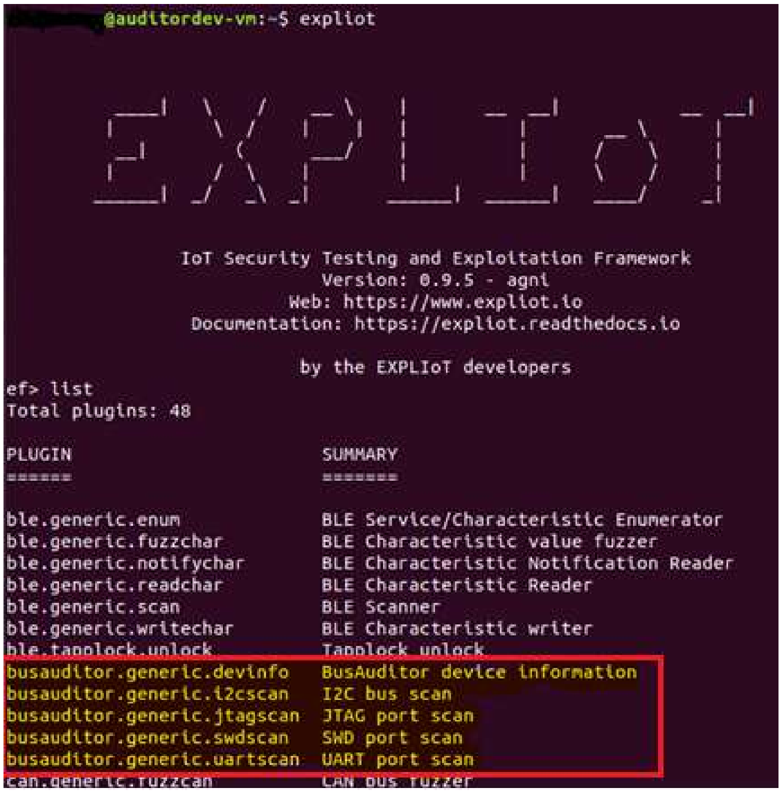
SUBSYSTEM=="usb", ATTRS{idVendor}=="0483", ATTRS{idProduct}=="ba20", OWNER="username", SYMLINK+="busauditor", MODE="0666"

5. To verify udev rule, disconnect and re-connect Bus Auditor to PC and run '***ls /dev***' command. This command will display '***busauditor***' as a new device in device configuration database.
   a. $ ls /dev



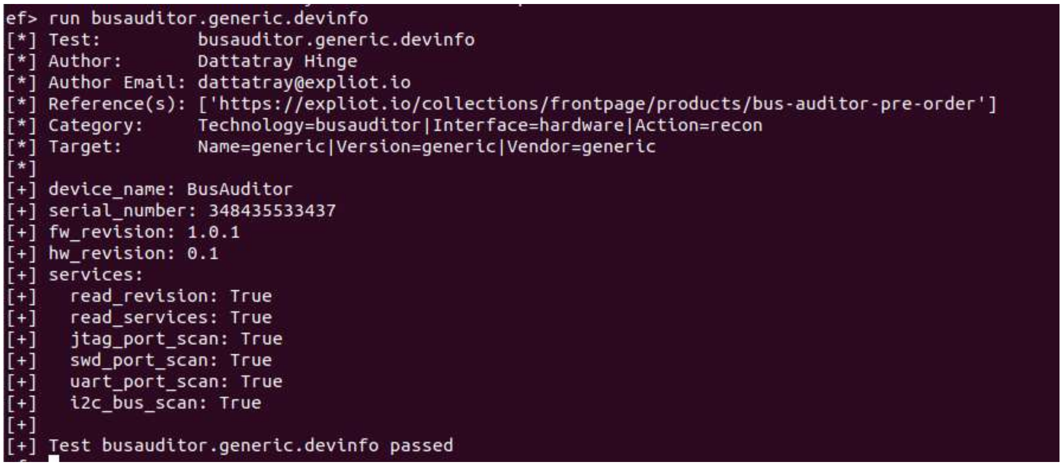
```
[redacted]@auditordev-vm:~$ ls /dev
autofs            cuse       hugepages  loop11  loop3
block             disk       hwrng      loop12  loop4
bsg               dri        i2c-0      loop13  loop5
btrfs-control     dvd        initctl    loop14  loop6
bus               ecryptfs   input      loop15  loop7
busauditor        fb0        kmsg       loop16  loop8
cdrom             fd         lightnvm   loop17  loop9
char              full       log        loop18  loop-control
console           fuse       loop0      loop19  mapper
core              hidraw0    loop1      loop2   mcelog
cpu_dma_latency   hpet       loop10     loop20  mem
```

6. Now run EXPLIoT framework using below command:
   a. $ expliot



```
[redacted]@auditordev-vm:~$ expliot

 ____| \ \  /  _ \  |      _ _|         __ __|
 __|    \  /  |   | |        |    _ \      |
 |         \  ___/  |        |   (   |     |
_____| _/\_\ _|    _____|  ___| \___/     _|

              IoT Security Testing and Exploitation Framework
                           Version: 0.9.5 - agni
                        Web: https://www.expliot.io
               Documentation: https://expliot.readthedocs.io

                         by the EXPLIoT developers
ef> list
Total plugins: 48

PLUGIN                        SUMMARY
======                        =======

ble.generic.enum              BLE Service/Characteristic Enumerator
ble.generic.fuzzchar          BLE Characteristic value fuzzer
ble.generic.notifychar        BLE Characteristic Notification Reader
ble.generic.readchar          BLE Characteristic Reader
ble.generic.scan              BLE Scanner
ble.generic.writechar         BLE Characteristic writer
ble.tapplock.unlock           Tapplock unlock
busauditor.generic.devinfo    BusAuditor device information
busauditor.generic.i2cscan    I2C bus scan
busauditor.generic.jtagscan   JTAG port scan
busauditor.generic.swdscan    SWD port scan
busauditor.generic.uartscan   UART port scan
can.generic.fuzzcan           CAN bus fuzzer
```

7. Now run Device information plugin from EXPLIoT framework:
   a. ef> run busauditor.generic.devinfo



```
ef> run busauditor.generic.devinfo
[*] Test:         busauditor.generic.devinfo
[*] Author:       Dattatray Hinge
[*] Author Email: dattatray@expliot.io
[*] Reference(s): ['https://expliot.io/collections/frontpage/products/bus-auditor-pre-order']
[*] Category:     Technology=busauditor|Interface=hardware|Action=recon
[*] Target:       Name=generic|Version=generic|Vendor=generic
[*]
[+] device_name: BusAuditor
[+] serial_number: 348435533437
[+] fw_revision: 1.0.1
[+] hw_revision: 0.1
[+] services:
[+]   read_revision: True
[+]   read_services: True
[+]   jtag_port_scan: True
[+]   swd_port_scan: True
[+]   uart_port_scan: True
[+]   i2c_bus_scan: True
[+]
[+] Test busauditor.generic.devinfo passed
```

4. EXPLIoT Framework Plugins Supported

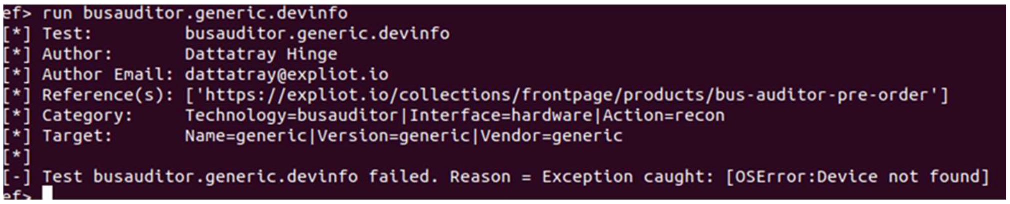
1. JTAG scan:	busauditor.generic.jtagscan
2. SWD scan:	busauditor.generic.swdscan
3. UART scan:	busauditor.generic.uartscan
4. I2C scan:	busauditor.generic.i2cscan

5. Help Tips

1. Identify Vcc and Ground pins in on target hardware headers
2. Avoid connecting target Vcc to Bus Auditor channels, this may lead to incorrect test result or damage the Bus Auditor channels circuit.
3. Connect Bus Auditor channels in a sequential range to target hardware header pins
4. Use exact start and end channels for plugin input that are connected to target hardware header pins.

6. Troubleshoot

1. “OS Error: Device not found”



```
ef> run busauditor.generic.devinfo
[*] Test:         busauditor.generic.devinfo
[*] Author:       Dattatray Hinge
[*] Author Email: dattatray@expliot.io
[*] Reference(s): ['https://expliot.io/collections/frontpage/products/bus-auditor-pre-order']
[*] Category:     Technology=busauditor|Interface=hardware|Action=recon
[*] Target:       Name=generic|Version=generic|Vendor=generic
[*]
[-] Test busauditor.generic.devinfo failed. Reason = Exception caught: [OSError:Device not found]
ef>
```

Troubleshoot steps:

- Check the USB cable for correct working
- Connect Bus Auditor to PC and verify Power LED is on
- Run ‘***dmesg’*** to see if the device was recognized by system driver.

7. References:

1. IoT Security-Part 13 (Introduction To Hardware Recon)
2. IoT Security-Part 14 (Introduction To And Identification Of Hardware Debug Ports)