



Quarkslab

SightHouse

Reverse Engineering with Function Similarity

Fenrisfulsur & MadSquirrels - 30/06/2026



Pass
the SALT

About Us



Benoît FORGETTE

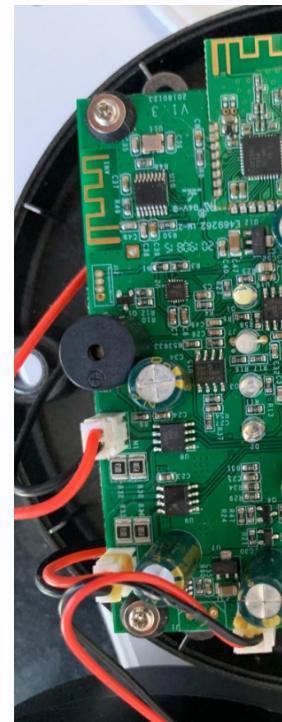
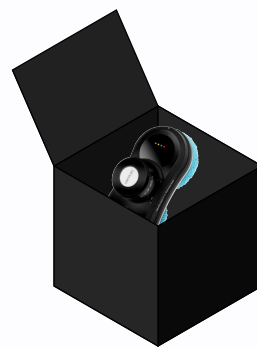
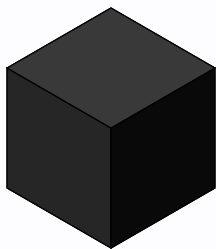
Software and hardware Security Researcher
topic (Hardware/Android)



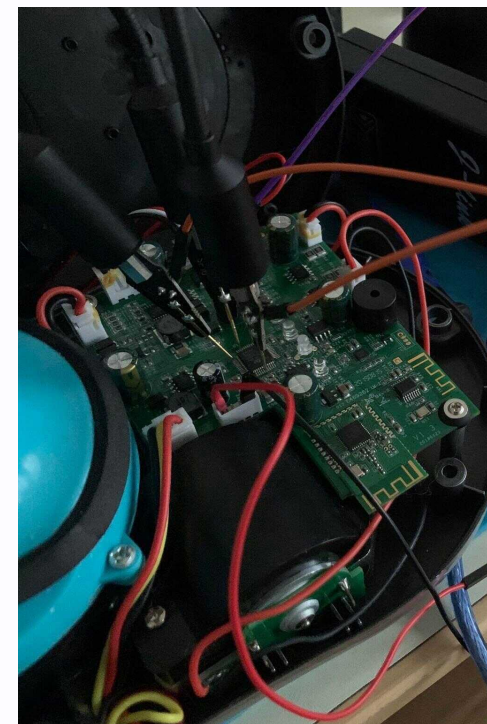
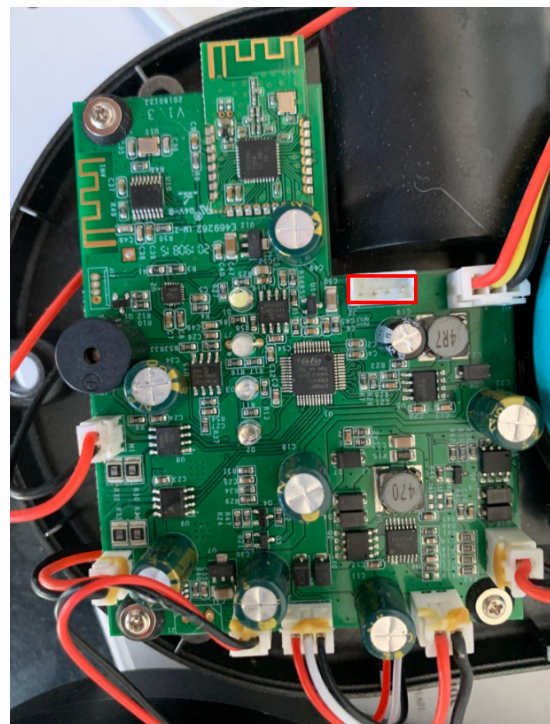
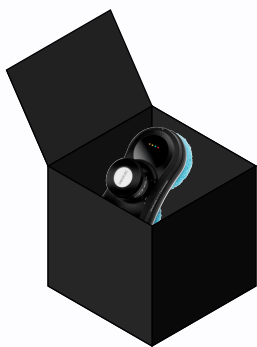
Sami BABIGEON

Software and hardware Security Researcher
topic (Hardware/CTF)

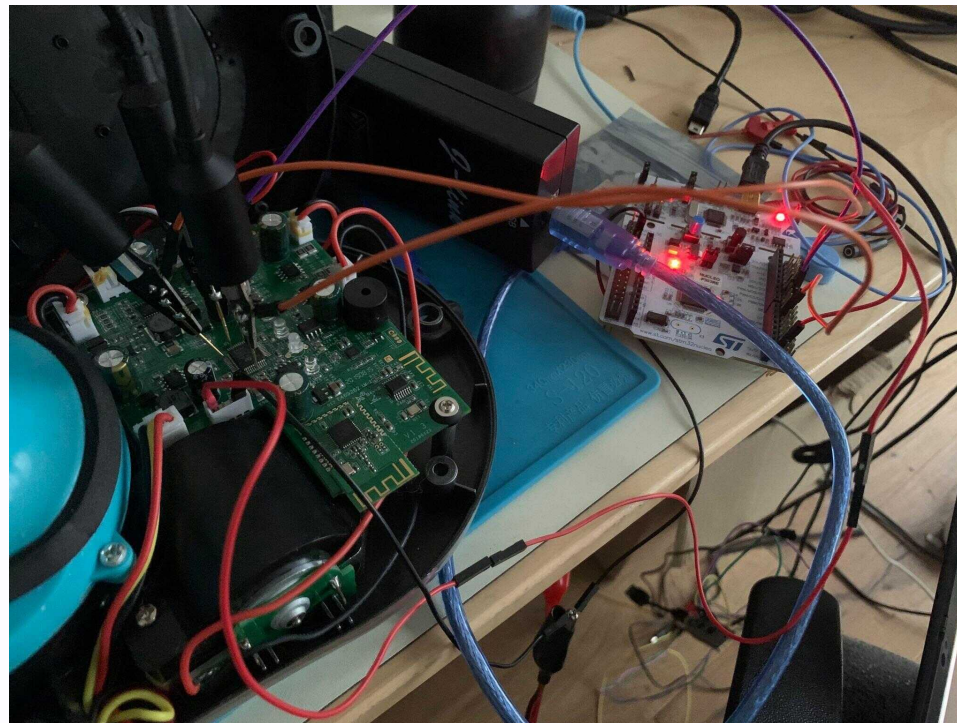
Our Workflow



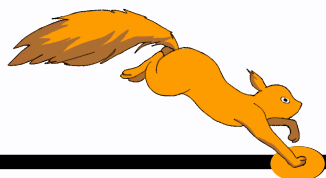
Our Workflow



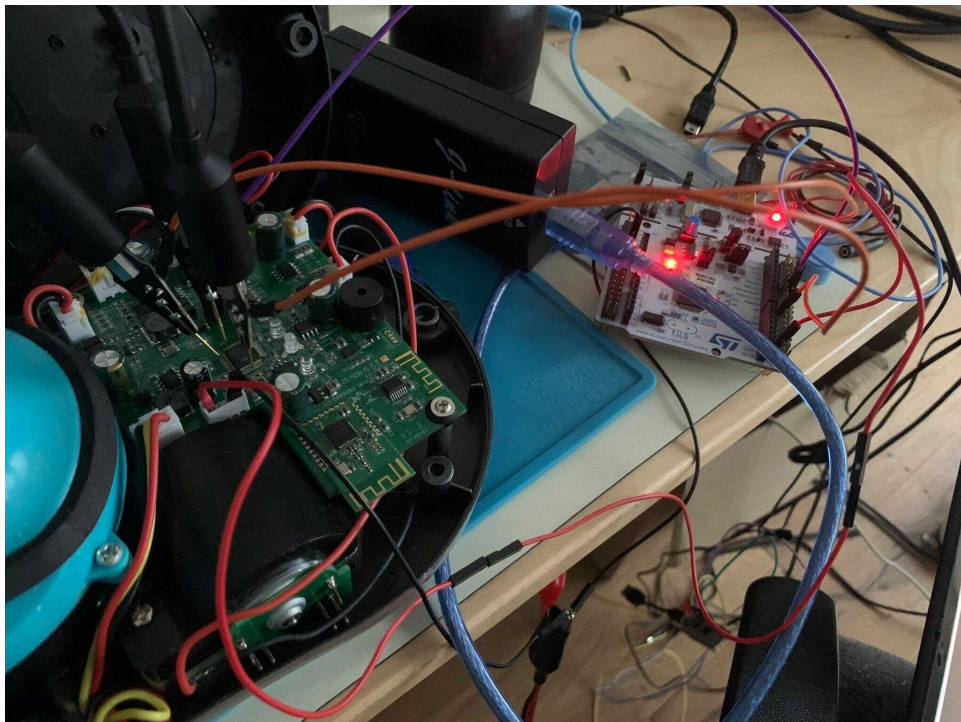
Our Workflow



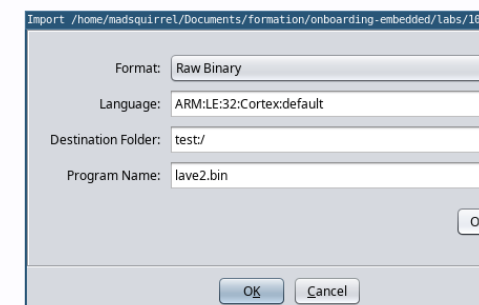
Address	00	01	02	03	04	05	06	07	08
00000000:	2D	A5	00	08	BB	04	00	08	00
00000010:	00	00	00	00	41	05	00	08	00
00000020:	00	00	00	00	5D	A5	00	08	5D
00000030:	5D	A5	00	08	99	A2	00	08	5D
00000040:	00	00	00	00	B9	0A	00	08	5D
00000050:	5D	A5	00	08	1F	17	00	08	00
00000060:	2D	18	A2	46	54	46	5D	46	00
00000070:	00	00	FB	1A	33	43	18	47	A0
00000080:	78	C1	FB	D8	30	C1	00	D5	1F
00000090:	F7	FF	00	F0	50	FB	03	B4	03
000000A0:	01	21	41	70	55	F8	18	21	00
000000B0:	01	70	41	70	07	F0	44	F8	01
000000C0:	C0	F9	01	21	BC	F9	01	21	B8
000000D0:	B0	F9	01	21	BA	F9	01	21	A8
000000E0:	A0	F9	10	BD	00	20	01	90	00
000000F0:	00	F0	8E	FE	00	F0	70	FF	27
00000100:	05	F0	A6	FA	00	19	84	B2	01
00000110:	94	49	88	8A	93	FA	68	46	84
00000120:	40	89	00	19	08	88	03	A9	68
00000130:	05	F0	76	FA	83	49	88	42	C0
00000140:	05	F0	07	FC	00	21	05	F0	C0
00000150:	40	89	00	12	68	46	40	89	68
00000160:	64	20	00	F0	05	FB	00	F0	C8
00000170:	A3	FB	01	F0	00	F0	40	FC	64
00000180:	64	49	08	70	3F	E0	00	F0	78
00000190:	00	F0	0C	FC	00	F0	20	FC	00
000001A0:	04	F0	3E	FB	11	FC	04	F0	80
000001B0:	A5	F9	01	25	00	F0	6A	FE	F0
000001C0:	04	F0	E9	FF	08	70	01	20	5A
000001D0:	04	F0	A0	FA	07	46	0A	28	7F
000001E0:	38	49	08	70	00	28	03	D1	C3
000001F0:	1E	D0	03	28	01	21	49	02	20
00000200:	00	90	1A	E0	28	48	05	F0	C0
00000210:	04	F0	94	FB	07	E0	00	20	08



Our Workflow



```
Address 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
00000000: 2D A5 00 08 BB 04 00 08 00 00 00 00 00 00 00 00 .....A...E...
00000010: 00 00 00 00 41 05 00 08 00 00 00 00 45 05 00 08 .....]...].
00000020: 00 00 00 00 5D A5 00 08 5D A5 00 08 5D A5 00 08 .....]...].
00000030: 5D A5 00 08 99 A2 00 08 5D A5 00 08 00 00 00 00 .....]...].
00000040: 00 00 00 00 B9 0A 00 08 5D A5 00 08 5D A5 00 08 .....]...].
00000050: 5D A5 00 08 1F 17 00 08 00 F0 02 F8 0C A0 30 C8 .....]...].
00000060: 2D 18 A2 46 54 46 5D 46 00 F0 22 F8 0F CC B6 46 .....FTF]F...".F
00000070: 00 00 F8 1A 33 43 18 47 A0 CF 00 00 00 25 00 26 .....3C.G....%.&
00000080: 78 C1 F8 08 30 C1 00 D5 1F B5 1F 8D 0B F0 38 FB x...0.....8.
00000090: F7 FF 00 F0 50 F8 03 B4 03 BC 08 F0 08 B5 13 21 .....P.....!
000000A0: 01 21 41 70 55 F8 1B 21 00 21 41 70 07 F0 4C F8 !ApU...!Ap.L.
000000B0: 01 70 41 70 07 F0 44 F8 01 21 23 20 B6 F9 01 21 pAp.D...!#...!
000000C0: C0 F9 01 21 BC F9 01 21 B8 F9 01 21 C2 F9 01 21 !!!!!!!...!
000000D0: B0 F9 01 21 BA F9 01 21 A8 F9 01 21 96 F9 01 21 !!!!!!!...!
000000E0: A0 F9 10 B0 00 20 01 90 00 24 00 27 FF F7 C9 FF .....$. '.....
000000F0: 00 F0 8E FE 00 F0 70 FF 27 FF 07 F0 DA FA 9E 49 .....p.'...I
00000100: 05 F0 A6 FA 00 19 84 B2 01 A9 02 31 68 46 C0 88 .....1hF.....
00000110: 94 49 88 8A 93 FA 68 46 84 B2 90 49 02 31 05 F0 .I...hF...I.1.
00000120: 40 89 00 19 08 88 03 A9 68 46 80 89 86 49 48 8B @.....hF...IH.
00000130: 05 F0 76 FA 83 49 88 42 C0 89 E1 43 47 D1 7E 49 .v.I.B...CG~I
00000140: 05 F0 07 FC 00 21 05 F0 C0 88 7A 49 00 89 79 49 .....!...zI...yI
00000150: 40 89 00 12 68 46 40 89 68 46 80 89 08 80 01 20 @...hF@.hF....
00000160: 64 20 00 F0 05 FB 00 F0 C8 F9 00 F0 31 FC 00 F0 d.....1...
00000170: A3 FB 01 F0 00 F0 40 FC 64 20 00 F0 FA FC 00 F0 .....@.d.....
00000180: 64 49 08 70 3F E0 00 F0 7B F9 00 F0 94 F9 05 20 dI.p?...{.....
00000190: 00 F0 0C FC 00 F0 20 FC 00 F0 53 F0 01 F0 76 F8 .....S...v...
000001A0: 04 F0 3E FB 11 FC 04 F0 80 FF 00 20 02 20 4F 49 .>.....OI
000001B0: A5 F9 01 25 00 F0 6A FE FD F8 68 1C F5 0D 04 20 ...%.j...h...
000001C0: 04 F0 E9 FF 08 70 01 20 5A E0 43 48 0D 00 00 20 .....p.Z.CH...
000001D0: 04 F0 A0 FA 07 46 0A 28 7F 20 08 F0 00 78 00 28 .....F.(...x.(
000001E0: 38 49 08 70 00 28 03 D1 C3 FD 33 E0 06 0D 01 28 8I.p.(...3...
000001F0: 1E D0 03 28 01 21 49 02 20 F0 70 1C 05 28 02 D0 ...(!.I...p.(
00000200: 00 90 1A E0 28 48 05 F0 C0 B2 06 46 00 26 02 20 ...(.H....F.&
00000210: 04 F0 94 FB 07 E0 00 20 08 70 02 E0 00 BF 00 BF .....d.....
```



Our Workflow

```

Address  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
00000000: 2D A5 00 08 BB 04 00 08 00 00 00 00 00 00 00 00 .....
00000010: 00 00 00 00 41 05 00 08 00 00 00 00 45 05 00 08 .....A...E...
00000020: 00 00 00 00 5D A5 00 08 5D A5 00 08 5D A5 00 08 .....]...]]...
00000030: 5D A5 00 08 99 A2 00 08 5D A5 00 08 00 00 00 00 .....]...
00000040: 00 00 00 00 B9 0A 00 08 5D A5 00 08 5D A5 00 08 .....]...
00000050: 5D A5 00 08 1F 17 00 08 00 F0 02 F8 0C A0 30 C8 .....]...
00000060: 2D 18 A2 46 54 46 5D 46 00 F0 22 F8 0F CC B6 46 .....FTF]F..."F
00000070: 00 00 F8 1A 33 43 18 47 A0 CF 00 00 00 25 00 26 .....3C.G....%&
00000080: 78 C1 F8 D8 30 C1 00 D5 1F B5 1F B0 0B F0 38 F8 x...0.....8
00000090: F7 FF 00 F0 50 F8 03 B4 03 BC 08 F0 08 B5 13 21 .....P.....!
000000A0: 01 21 41 70 55 F8 1B 21 00 21 41 70 07 F0 4C F8 !ApU...!Ap..L
000000B0: 01 70 41 70 07 F0 44 F8 01 21 23 20 B6 F9 01 21 pAp..D...!#...!
000000C0: C0 F9 01 21 BC F9 01 21 B8 F9 01 21 C2 F9 01 21 .....!.....!
000000D0: B0 F9 01 21 BA F9 01 21 A8 F9 01 21 96 F9 01 21 .....!.....!
000000E0: A0 F9 10 BD 00 20 01 90 00 24 00 27 FF F7 C9 FF .....$. '...!
000000F0: 00 F0 8E FE 00 F0 70 FF 27 FF 07 F0 DA FA 9E 49 .....p...'...I
00000100: 05 F0 A6 FA 00 19 84 B2 01 A9 02 31 68 46 C0 88 .....1hF...
00000110: 94 49 88 8A 93 FA 68 46 84 B2 90 49 02 31 05 F0 I...hF...I 1
00000120: 40 89 00 19 08 88 03 A9 68 46 80 89 86 49 48 8B @.....hF...IH
00000130: 05 F0 76 FA 83 49 88 42 C0 89 E1 43 47 D1 7E 49 v..I.B...CG~I
00000140: 05 F0 07 FC 00 21 05 F0 C0 88 7A 49 00 89 79 49 .....!.....zI...yI
00000150: 40 89 00 12 68 46 40 89 68 46 80 89 08 80 01 20 @...hF@.hF....
00000160: 64 20 00 F0 05 F8 00 F0 C8 F9 00 F0 31 FC 00 F0 d.....1...
00000170: A3 F8 01 F0 00 F0 40 FC 64 20 00 F0 FA FC 00 F0 .....@.d.....
00000180: 64 49 08 70 3F E0 00 F0 7B F9 00 F0 94 F9 05 20 dI.p?...{.....
00000190: 00 F0 0C FC 00 F0 20 FC 00 F0 53 F0 01 F0 76 F8 .....S...v...
000001A0: 04 F0 3E FB 11 FC 04 F0 80 FF 00 20 02 20 4F 49 >.....OI
000001B0: A5 F9 01 25 00 F0 6A FE FD F8 68 1C F5 D0 04 20 ...%.j...h...
000001C0: 04 F0 E9 FF 08 70 01 20 5A E0 43 48 00 D0 00 20 .....p..Z.CH...
000001D0: 04 F0 A0 FA 07 46 0A 28 7F 20 08 F0 00 78 00 28 .....F.(...x.(
000001E0: 38 49 08 70 00 28 03 D1 C3 F0 33 E0 06 D0 01 28 8I.p.(...3...
000001F0: 1E D0 03 28 01 21 49 02 20 F0 70 1C 05 28 02 D0 ...(.I...p.(...
00000200: 00 90 1A E0 28 48 05 F0 C0 B2 06 46 00 26 02 20 ...(.H....F.&...
00000210: 04 F0 94 FB 07 E0 00 20 08 70 02 E0 00 BF 00 BF .....d.....

```



Import /home/madsquirrel/Documents/formation/onboarding-embedded/labs/10_identify_...

Format: Raw Binary

Language: ARMv8:LE32:Cortex:default

Destination Folder: test/

Program Name: lave2.bin

Options...

Options

Block Name: RAM

Base Address: 0x08000000 Hex

File Offset: 0x0 Hex

Length: 0x4000 Hex

Apply Processor Defined Labels ☒

Anchor Processor Defined Labels ☒

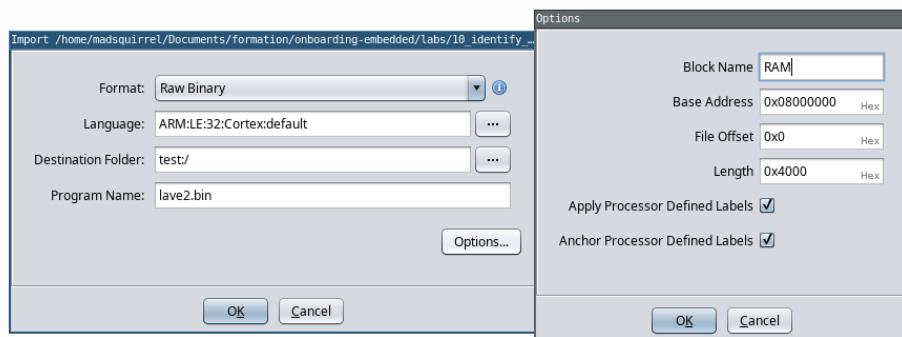
OK Cancel

```

*****
***** FUNCTION *****
*****
undefined FUN_08000e8c()
<UNASSIGNED> <RETURN>
FUN_08000e8c
08000e8c 01 68 ldr
08000e8e 20 46 mov
08000e90 04 46 mov
08000e92 0c 99 ldr
08000e94 ed fe 07 90 cdp2
08000e98 4f fe 11 90 mcr2
08000e9c 0a f0 e4 fe bl
08000ea0 0a f0 46 fe bl
08000ea4 08 98 ldr
08000ea6 0a f0 07 90 b.w
08000eaa 0a f0 40 48 and
08000eae 01 68 ldr
08000eb0 0a f0 d0 fe bl
08000eb4 0a f0 cc fe bl
08000eb8 01 68 ldr
08000eba 3f 20 movs
08000ebc c5 fe 07 90 cdp2
08000ec0 c1 fe 12 90 mcr2
08000ec4 3f 20 movs
08000ec6 00 06 lsls
08000ec8 21 46 mov
08000eca 07 90 str
08000ecc 04 46 mov
08000ece 17 48 ldr
08000ed0 07 68 ldr
08000ed2 17 48 ldr
08000ed4 21 46 mov
08000ed6 16 48 ldr
08000ed8 a9 fe 06 90 cdp2
08000edc 0a f0 a4 fe bl
08000ee0 c0 07 lsls
08000ee2 78 40 eors
08000ee4 0a f0 9c fe bl
08000ee8 0a f0 28 ff bl
08000eec 0a f0 24 ff bl

```

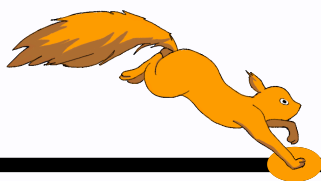
Our Workflow



```

*****
*                               *
*                               *
*****
FUNCTION
*****
undefined FUN_08000e8c()
<UNASSIGNED> <RETURN>
FUN_08000e8c
08000e8c 01 68      ldr     XREF[1]: FUN_080001ac:080001b4(c)
08000e8e 20 46      mov     r1, [r0, #0x0]
08000e90 04 46      mov     r0, r4
08000e92 0c 99      mov     r4, r0
08000e94 ed fe 07 90  ldr     r1, [sp, #Stack[0x30]]
08000e98 4f fe 11 90  cdp2    p0, 0xe, cr9, cr13, cr7, 0x0
08000e9c 0a f0 e4 fe  mcr2    p0, 0x2, r9, cr15, cr1, 0x0
08000ea0 0a f0 46 fe  bl      SUB_0800bc68
08000ea4 08 98      bl      SUB_0800bb30
08000ea6 0a f0 07 90  ldr     r0, [sp, #Stack[0x20]]
08000eaa 0a f0 40 48  b.w     LAB_08c0aeb8
08000eae 01 68      and     r8, r10, #0xc0000000
08000eb0 0a f0 d0 fe  ldr     r1, [r0, #0x0]
08000eb4 0a f0 cc fe  bl      SUB_0800bc54
08000eb8 01 68      bl      SUB_0800bc50
08000eba 3f 20      ldr     r1, [r0, #0x0]
08000ebc 3f 20      movs    r0, #0x3f
08000ebd c5 fe 07 90  cdp2    p0, 0xc, cr9, cr5, cr7, 0x0
08000ec0 c1 fe 12 90  mcr2    p0, 0x6, r9, cr1, cr2, 0x0
08000ec4 3f 20      movs    r0, #0x3f
08000ec6 00 06      lsls    r0, r0, #0x18
08000ec8 21 46      mov     r1, r4
08000eca 07 90      str     r0, [sp, #0x1c]
08000ecc 04 46      mov     r4, r0
08000ece 17 48      ldr     r0, [DAT_08000f2c]
08000ed0 07 68      ldr     r7, [r0, #0x0] => DAT_4ab71b00
08000ed2 17 48      ldr     r0, [DAT_08000f30]
08000ed4 21 46      mov     r1, r4
08000ed6 16 48      ldr     r0, [DAT_08000f30]
08000ed8 a9 fe 06 90  cdp2    p0, 0xa, cr9, cr9, cr6, 0x0
08000edc 0a f0 a4 fe  bl      SUB_0800bc28
08000ee0 c0 07      lsls    r0, r0, #0x1f
08000ee2 78 40      eors    r0, r7
08000ee4 0a f0 9c fe  bl      SUB_0800bc20
08000ee8 0a f0 28 ff  bl      SUB_0800bd3c
08000eec 0a f0 24 ff  bl      SUB_0800bd38

```



Our Workflow

```

*****
*                               *
*                               *
*****
FUNCTION
*****
undefined FUN_08000e8c()
<RETURN>
FUN_08000e8c
XREF[1]: FUN_080001ac:080001b4(c)
08000e8c 01 68      ldr    r1,[r0,#0x0]
08000e8e 20 46      mov    r0,r4
08000e90 04 46      mov    r4,r0
08000e92 0c 99      ldr    r1,[sp,#Stack[0x30]]
08000e94 ed fe 07 90 cdp2    p0,0xe,cr9,cr13,cr7,0x0
08000e98 4f fe 11 90 mcr2    p0,0x2,r9,cr15,cr1,0x0
08000e9c 0a f0 e4 fe bl      SUB_0800bc68
08000ea0 0a f0 46 fe bl      SUB_0800bb30
08000ea4 08 98      ldr    r0,[sp,#Stack[0x20]]
08000ea6 0a f0 07 90 b.w     LAB_08c0aeb8
08000eaa 0a f0 40 48 and     r8,r10,#0xc0000000
08000eae 01 68      ldr    r1,[r0,#0x0]
08000eb0 0a f0 d0 fe bl      SUB_0800bc54
08000eb4 0a f0 cc fe bl      SUB_0800bc50
08000eb8 01 68      ldr    r1,[r0,#0x0]
08000eba 3f 20      movs   r0,#0x3f
08000ebc c5 fe 07 90 cdp2    p0,0xc,cr9,cr5,cr7,0x0
08000ec0 c1 fe 12 90 mcr2    p0,0x6,r9,cr1,cr2,0x0
08000ec4 3f 20      movs   r0,#0x3f
08000ec6 00 06      lsls   r0,r0,#0x18
08000ec8 21 46      mov    r1,r4
08000eca 07 90      str    r0,[sp,#0x1c]
08000ecc 04 46      mov    r4,r0
08000ece 17 48      ldr    r0,[DAT_0800f2c]
08000ed0 07 68      ldr    r7,[r0,#0x0] =>DAT_4ab71b00
08000ed2 17 48      ldr    r0,[DAT_0800f30]
08000ed4 21 46      mov    r1,r4
08000ed6 16 48      ldr    r0,[DAT_0800f30]
08000ed8 a9 fe 06 90 cdp2    p0,0xa,cr9,cr9,cr6,0x0
08000edc 0a f0 a4 fe bl      SUB_0800bc28
08000ee0 c0 07      lsls   r0,r0,#0x1f
08000ee2 78 40      eors   r0,r7
08000ee4 0a f0 9c fe bl      SUB_0800bc20
08000ee8 0a f0 28 ff bl      SUB_0800bd3c
08000eec 0a f0 24 ff bl      SUB_0800bd38

```



What does this function do?

```
int FUN_0806c160(uint param_1) {
    int iVar1;
    uint *puVar2;
    uint uVar3;
    puVar2 = (uint *) (param_1 & 0xffffffffc);
    iVar1 = -(param_1 & 3);
    uVar3 = *puVar2;
    if ((param_1 & 3) != 0) {
        uVar3 = uVar3 | 0xffffffffU >> ((iVar1 + 4U & 0x1f) << 3);
    }
    while( true ) {
        puVar2 = puVar2 + 1;
        uVar3 = uVar3 + 0xfefefeff & ~uVar3 & 0x80808080;
        if (uVar3 != 0) break;
        uVar3 = *puVar2;
        iVar1 = iVar1 + 4;
    }
    return iVar1 + (0x1fU - LZCOUNT(uVar3 & -uVar3) >> 3);
}
```

What does this function do?

```
undefined4 FUN_0400eede5(undefined4 *param_1) {  
    *param_1 = 0;  
    param_1[1] = 0;  
    param_1[2] = 0x6a09e667;  
    param_1[3] = 0xbb67ae85;  
    param_1[4] = 0x3c6ef372;  
    param_1[5] = 0xa54ff53a;  
    param_1[6] = 0x510e527f;  
    param_1[7] = 0x9b05688c;  
    param_1[8] = 0x1f83d9ab;  
    param_1[9] = 0x5be0cd19;  
    return 0;  
}
```

What does this function do?

```
void FUN_08032ce4(undefined1 *param_1, undefined1 *param_2, uint param_3) {
    uint uVar1;
    int iVar2;

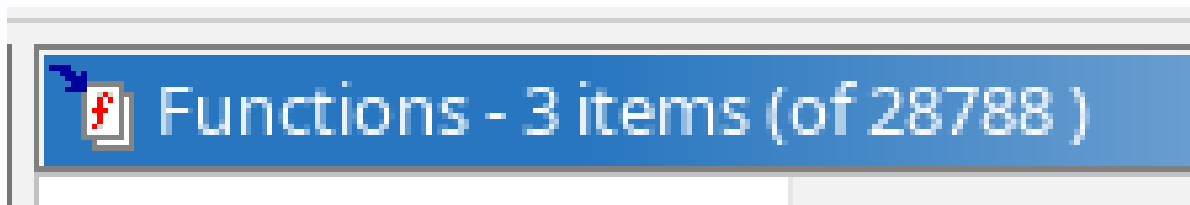
    if (param_1 == param_2) {
        do { } while( true );
    }
    if (((uint)param_1 ^ (uint)param_2) & 3) == 0) {
        while( true ) {
            if (param_3 == 0) { return; }
            iVar2 = 0;
            if (((uint)param_1 & 3) == 0) break;
            param_3 = param_3 - 1;
            *param_1 = *param_2;
            param_2 = param_2 + 1;
            param_1 = param_1 + 1;
        }
        for (; 3 < param_3 + iVar2; iVar2 = iVar2 + -4) {
            *(undefined4 *)(param_1 + -iVar2) = *(undefined4 *)(param_2 + -iVar2);
        }
        uVar1 = param_3 >> 2;
        param_3 = uVar1 * -4 + param_3;
        iVar2 = uVar1 * 4;
        param_1 = param_1 + iVar2;
        param_2 = param_2 + iVar2;
    }
    for (uVar1 = 0; param_3 != uVar1; uVar1 = uVar1 + 1) {
        param_1[uVar1] = param_2[uVar1];
    }
}
```

Let's continue (or not)

- Those functions were "easy"
- Reversing each function takes some time and effort
- No information on provenance / SDK

Let's continue (or not)

- Those functions were "easy"
- Reversing each function takes some time and effort
- No information on provenance / SDK
- A **little** scaling problem



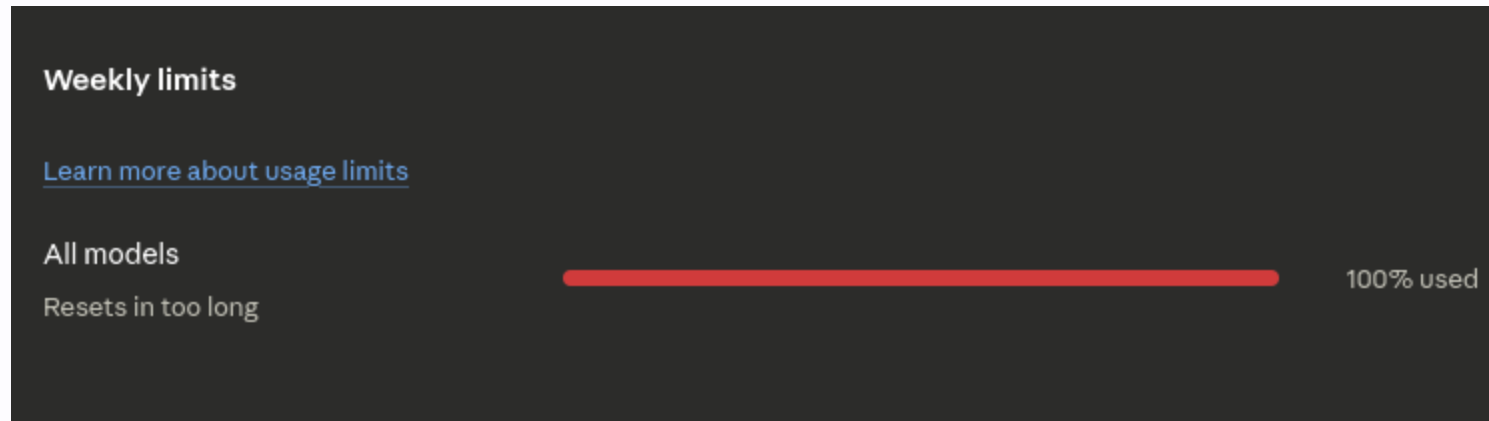
Renaming automatically in 2026

1. Open a chat with your favorite frontier model
2. Send all your data, boot up MCP / Tools / SKILLS / etc.
3. Set your favorite prompt:

Reverse this program. Find all the vulnerabilities. Make no mistakes.

Renaming automatically in 2026

One small problem (among others: privacy / environmental / political issues)



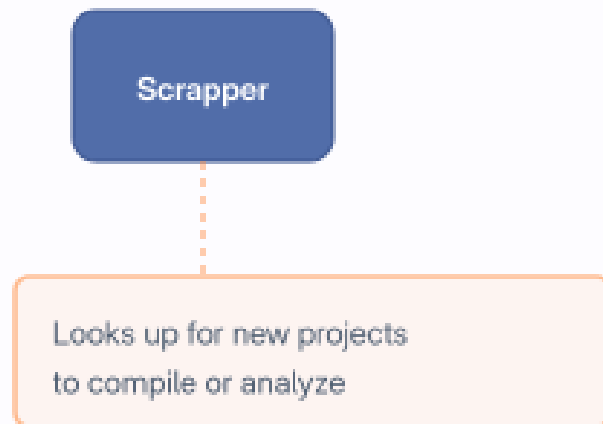
What is SightHouse?

SightHouse is a tool designed to assist reverse engineers by **collecting** information and **metadata** from programs and recognizing **similar** functions.

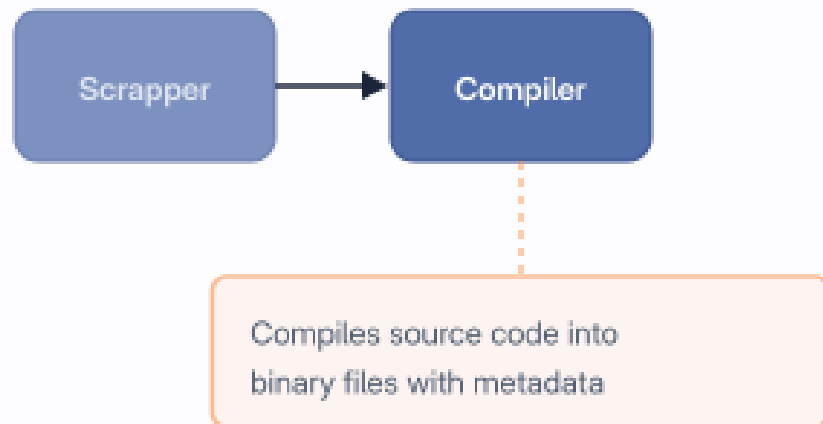
What is SightHouse?



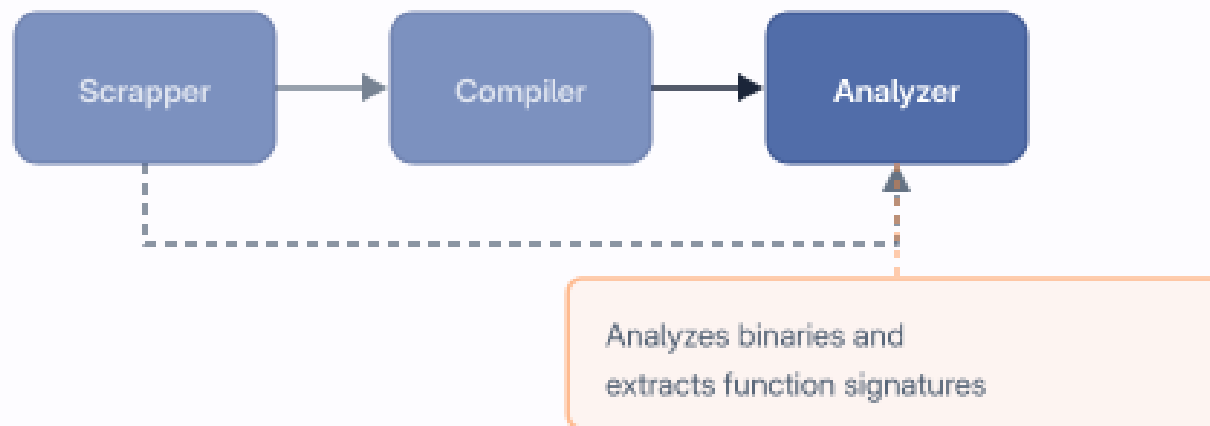
SightHouse Workflow



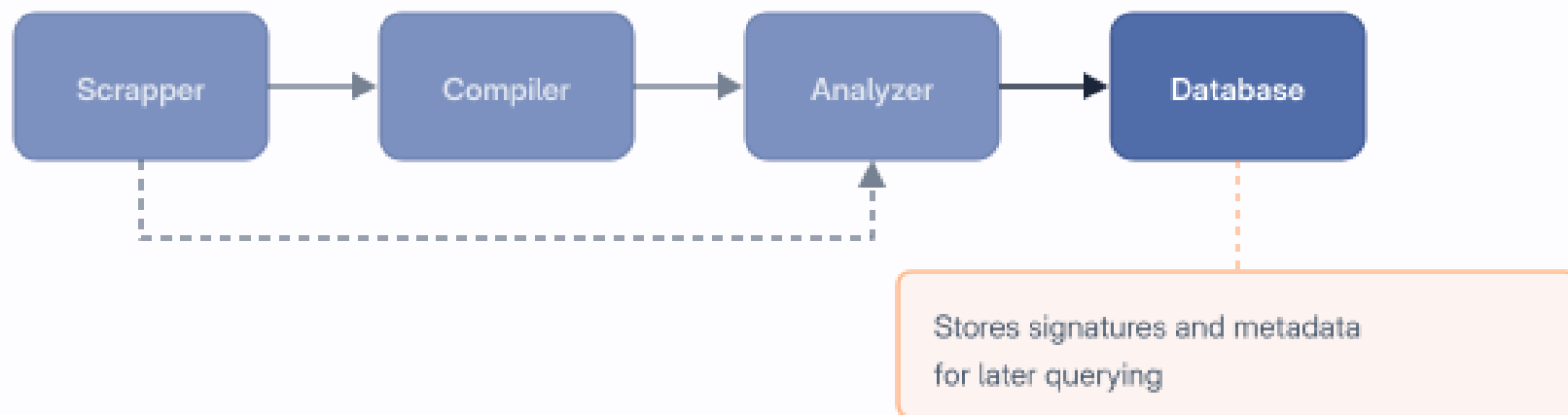
SightHouse Workflow



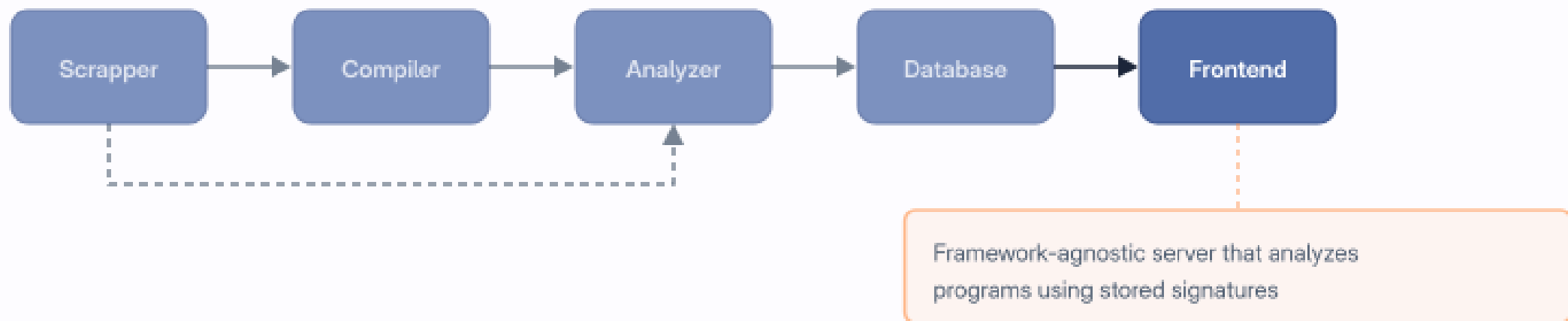
SightHouse Workflow



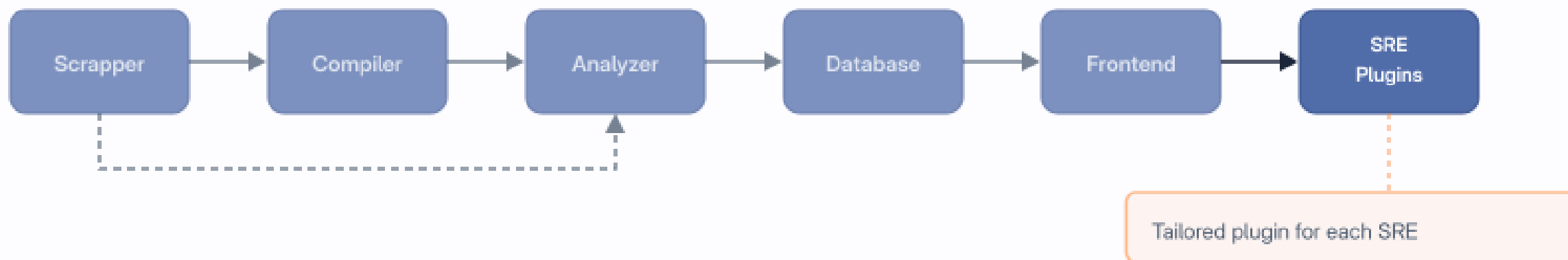
SightHouse Workflow



SightHouse Workflow



SightHouse Workflow



Demo - Pwn2Own 2025

Firmware analysis

Recon:

- Loading address `0x08010000`
(bootloader not part of FOTA?, secureboot?)

Used internal tool for function similarity ⇒ *Recognized all known FreeRTOS functions*

- OS: **FreeRTOS**

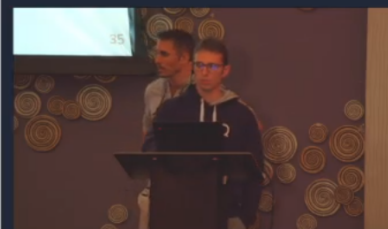
- No symbols available
- **No mitigations/protections** (ASLR, NX..)
- Task-based OS: identified interesting ones

Wifi_Ble_HAL_TASK

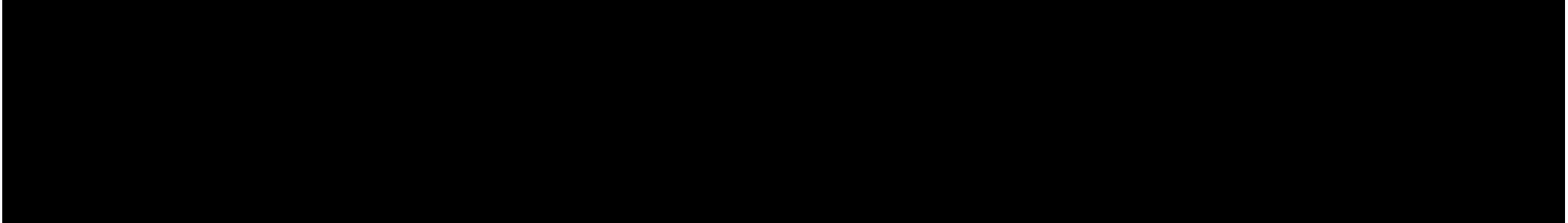
App_Business_Task

Module_Wifi_Ble_Task

UsbCommTask



Demo - Pwn2Own 2025



Wanna learn more?

- See how SightHouse can help you accelerate your Reverse Engineering workflow
- Learn how to create your own workers

Material Prerequisites:

- A Linux laptop
- Docker installed and working
- A supported Software Reverse Engineering (SRE): Ghidra / Binary Ninja / IDA

Technical Prerequisites:

- Basic reverse engineering knowledge
- Basic Python development experience

See you tomorrow from 09:30 to 12:30, Room LW112!



Quarkslab

Questions?

Documentation & GitHub

quarkslab.github.io/sighthouse
github.com/quarkslab/sighthouse



Pass
the SALT