COMMENTES MOI ÇA!

Retex & WU of the ph0wn CTF 2024

by Philippe_Katerine & e1k

SUMMARY OF THIS TALK

01. IOT HACKING SOUS LE SOLEIL

02. WU STAGE 1 : HARDWARE

03. WU STAGE 2 : REVERSE

04. FINAL WORDS AND BEERS, Q&A

$WHOAREWE

Paul → Philippe_Katerine / ENSIBS
Emile → e1k / IMT Atlantique

iut Saint Malo réseaux & télécoms

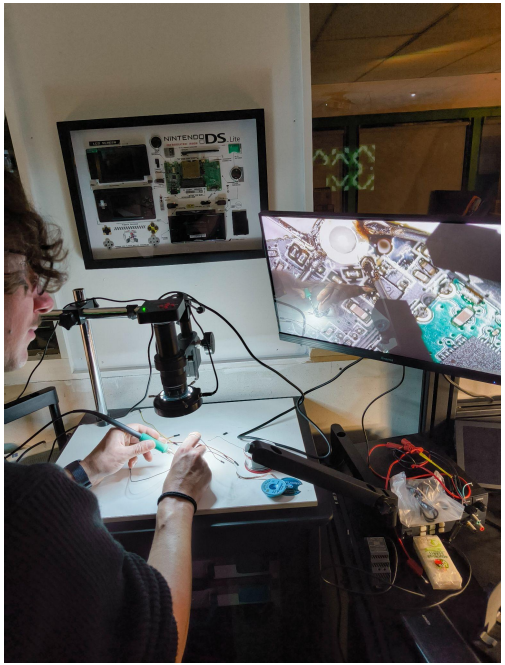
École d'ingénieurs ensibs : Université Bretagne Sud

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom


IOT HACKING SOUS LE SOLEIL
01.

POLYTECHNIQUE (EUH NICE**)

QUI ? QUOI ?



ph0wn

SHL

PICO PCB

Stage 1 : Hardware

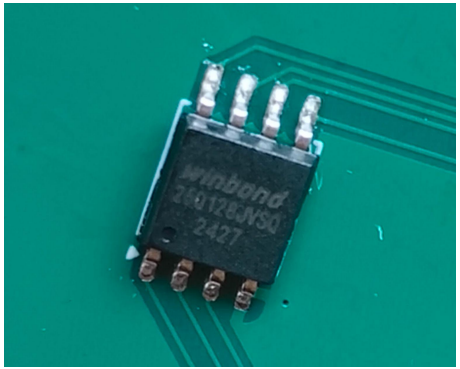
02.

LE CHALLENGE

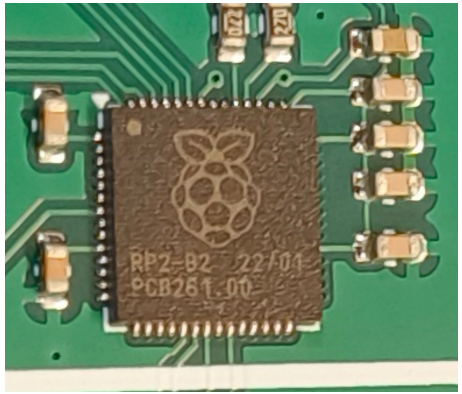
Pico lost a flag. He can’t remember where it is on the PCB. Stupid, isn’t it?

1. Locate Pico’s memory
2. Look under the carpet. The hot air stations might help you.
3. You’ll need to put everything back in place for stage 2.

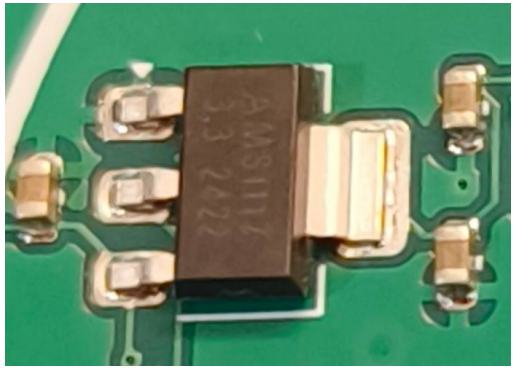
RETRO INGÉNIERIE DU PCB



W25Q128JVSJQ “SERIAL FLASH MEMORY - SPI”
-> La mémoire

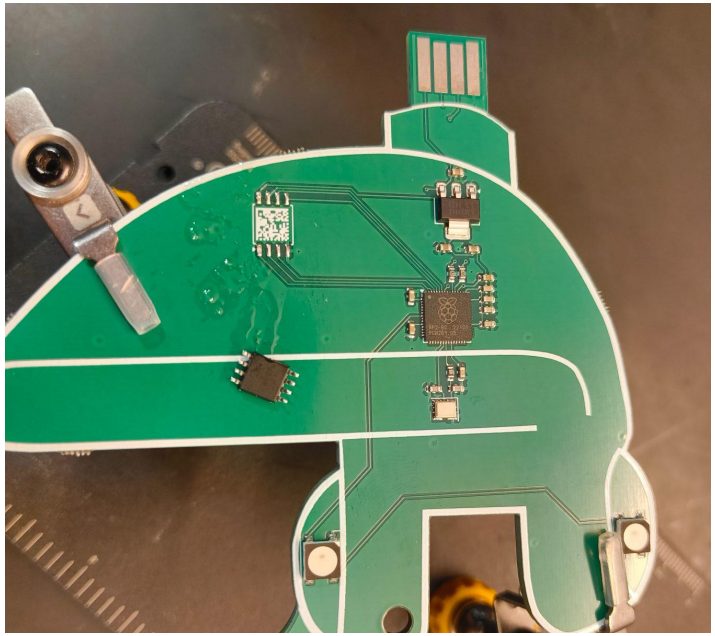


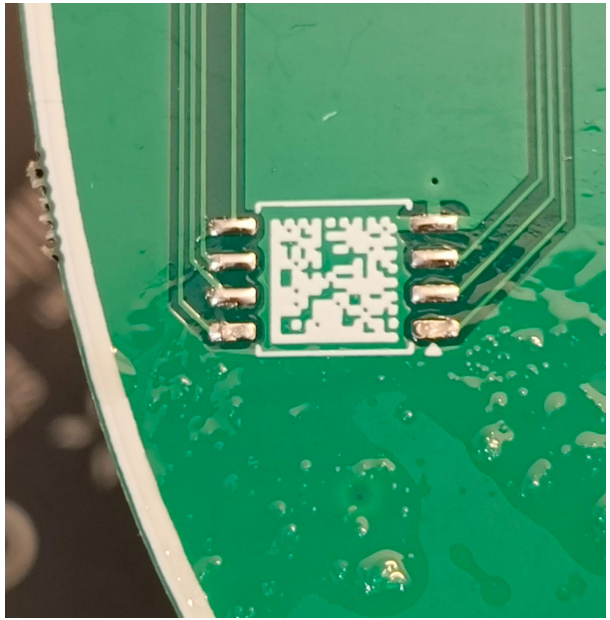
RP2-B2 22/01 PCB261
-> Le microcontroleur



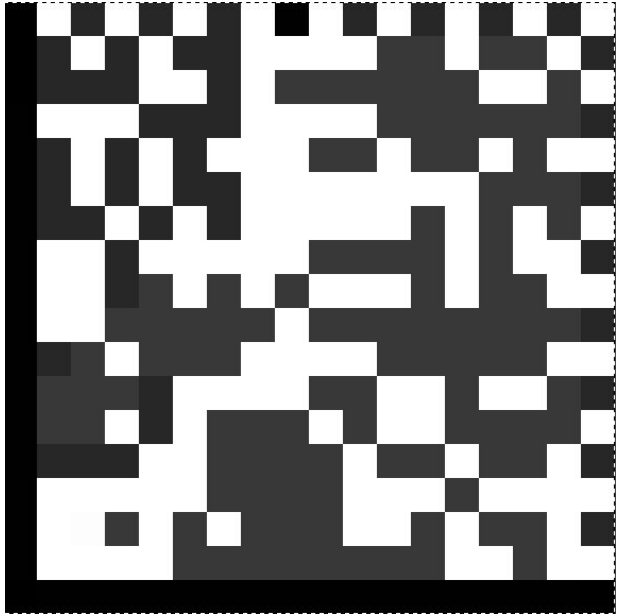
AMS1117 3,3
-> Le régulateur de tension

LOOKING UNDER THE CARPET

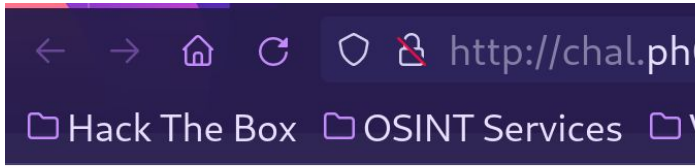




DATA MATRIX CODE

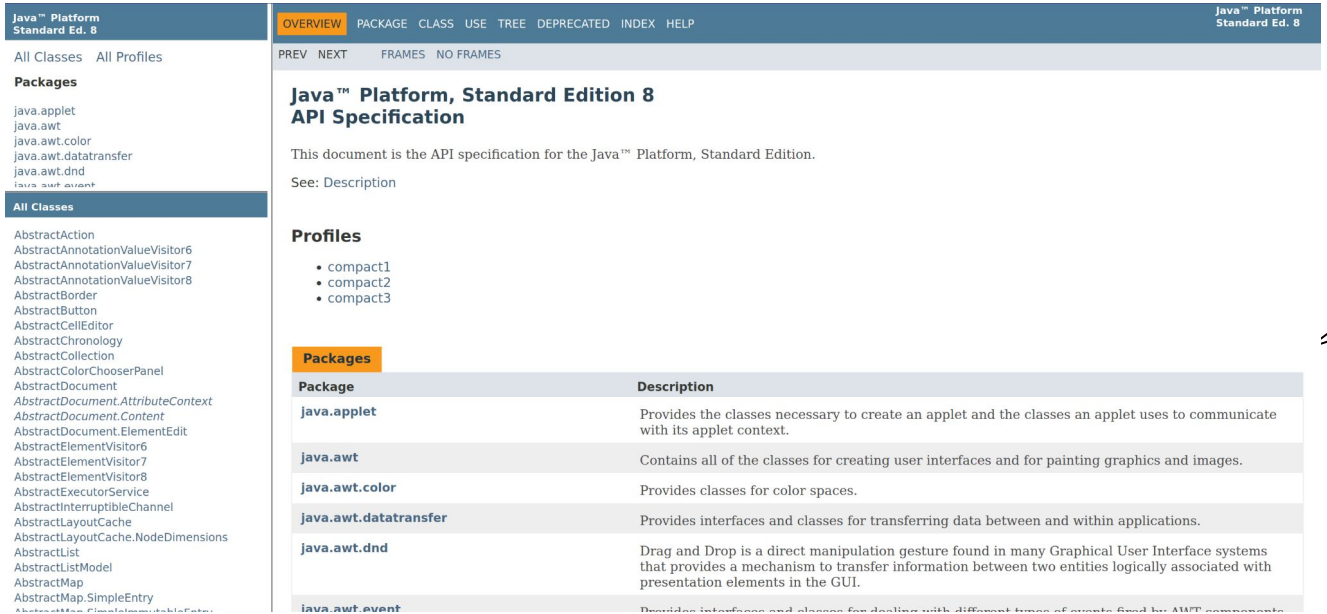


ph0wn.org/pcb-key




```
algo: AES-CBC
key:  thanks_to_balda!
IV:   butter_soldering
```

RTFM TU ME LIS LA DOC LA



Java™ Platform Standard Ed. 8

All Classes All Profiles

Packages

java.applet
java.awt
java.awt.color
java.awt.datatransfer
java.awt.dnd
java.awt.event

All Classes

AbstractAction
AbstractAnnotationValueVisitor6
AbstractAnnotationValueVisitor7
AbstractAnnotationValueVisitor8
AbstractBorder
AbstractButton
AbstractCellEditor
AbstractChronology
AbstractCollection
AbstractColorChooserPanel
AbstractDocument
AbstractDocument.AttributeContext
AbstractDocument.Content
AbstractDocument.ElementEdit
AbstractElementVisitor6
AbstractElementVisitor7
AbstractElementVisitor8
AbstractExecutorService
AbstractInterruptibleChannel
AbstractLayoutCache
AbstractLayoutCache.NodeDimensions
AbstractList
AbstractListModel
AbstractMap
AbstractMap.SimpleEntry

OVERVIEW PACKAGE CLASS USE TREE DEPRECATED INDEX HELP — Java™ Platform Standard Ed. 8

PREV NEXT FRAMES NO FRAMES

Java™ Platform, Standard Edition 8 API Specification

This document is the API specification for the Java™ Platform, Standard Edition.

See: Description

Profiles

- compact1
- compact2
- compact3

Packages

Package	Description
java.applet	Provides the classes necessary to create an applet and the classes an applet uses to communicate with its applet context.
java.awt	Contains all of the classes for creating user interfaces and for painting graphics and images.
java.awt.color	Provides classes for color spaces.
java.awt.datatransfer	Provides interfaces and classes for transferring data between and within applications.
java.awt.dnd	Drag and Drop is a direct manipulation gesture found in many Graphical User Interface systems that provides a mechanism to transfer information between two entities logically associated with presentation elements in the GUI.
java.awt.event	Provides interfaces and classes for dealing with different types of events fired by AWT components

RTFM TU ME LIS LA DOC LA

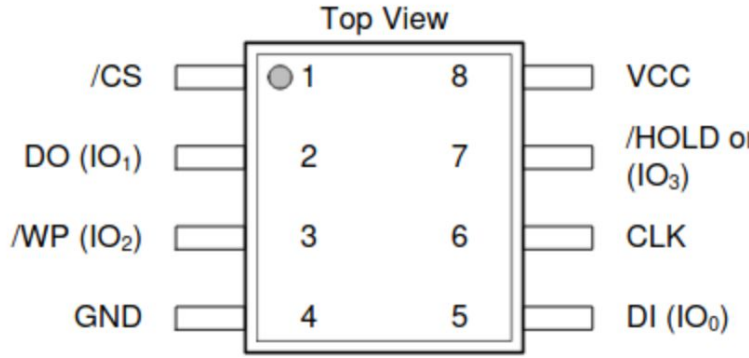
winbond

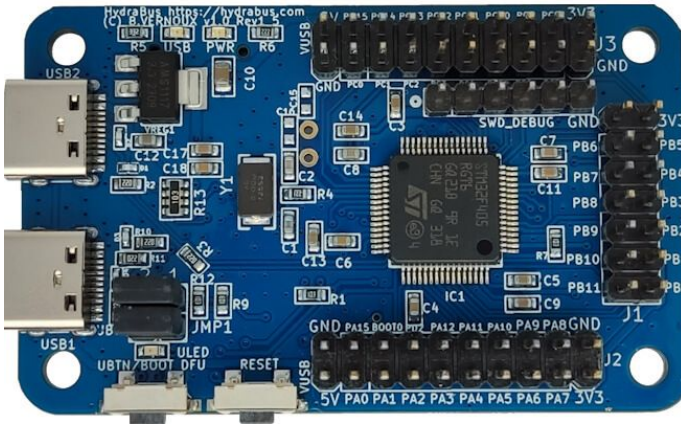
spiflash®

3V 128M-BIT
SERIAL FLASH MEMORY WITH
DUAL/QUAD SPI

For Industrial & Industrial Plus Grade

FIRMWARE EXTRACTION

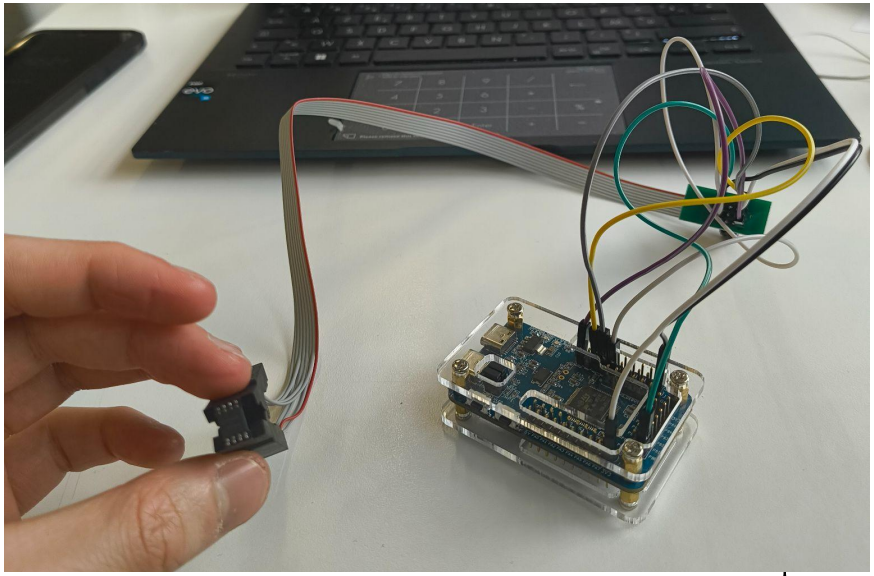




FIRMWARE EXTRACTION

Example connection SPIFlash WINBOND W25Q16DV / HydraBus

SPI Flash WINBOND W25Q16DV	HydraBus SPI2	Details
/CS Pin1	SPI2 CS: PC1	Chip Select
DO(IO1) Pin2	SPI2 MISO: PC2	SPI MISO
/WP(IO2) Pin3	3V3	Disable write protect
GND Pin4	GND	
DI(IO0) Pin5	SPI2 MOSI: PC3	SPI MOSI
CLK Pin6	SPI2 SCK: PB10	SPI CLK
/HOLD (IO3) Pin7	3V3	Disable hold
VCC Pin8	3V3	



FIRMWARE ANALYSIS

```
eddymalou@parrot:~/Documents/CTF/ph0wn/ctf/pico_hardware$ md5sum dump_first.bin
016030e6453350b399f9036c092b77a3  dump_first.bin
eddymalou@parrot:~/Documents/CTF/ph0wn/ctf/pico_hardware$ md5sum dump_second.bin
016030e6453350b399f9036c092b77a3  dump_second.bin
```

```
eddymalou@parrot:~/Documents/CTF/ph0wn/ctf/pico_hardware$ binwalk dump_first.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
29036         0x716C          Unix path: /home/axelle/softs/pico/pico-sdk/src/rp2040/pico_platform/platform.c
29240         0x7238          Unix path: /home/axelle/softs/pico/pico-sdk/src/rp2_common/hardware_irq/irq.c
31644         0x7B9C          Unix path: /home/axelle/softs/pico/pico-sdk/src/rp2_common/pico_stdio/stdio.c
32016         0x7D10          Unix path: /home/axelle/softs/pico/pico-sdk/src/rp2_common/pico_stdio_usb/stdio_usb.c
32320         0x7E40          Unix path: /home/axelle/softs/pico/pico-sdk/src/rp2_common/pico_unique_id/unique_id.c
33204         0x81B4          Unix path: /home/axelle/softs/pico/pico-sdk/lib/tinyusb/src/portable/raspberrypi/rp2040/rp2040_usb.c
33692         0x839C          Unix path: /home/axelle/softs/pico/pico-sdk/src/rp2_common/hardware_pio/pio.c
```

FLAG STAGE 1

```
00008f40: 0000 0000 a507 0010 4245 4749 4e20 454e  ........BEGIN EN
00008f50: 4352 5950 5445 4420 5354 4147 4531 2043  CRYPTED STAGE1 C
00008f60: 4f4e 5445 4e54 8329 0650 36b7 45b1 d225  ONTENT.).P6.E..%
00008f70: 5610 e8f2 ba7c 3b8b f3c8 6179 aa34 3c73  V....|;...ay.4<s
00008f80: 6ca3 16b7 88c4 51ac 324b 3cf5 fdfa ad9a  l.....Q.2K<.....
00008f90: 180c 9ca1 c0e1 14ee 37f9 d618 bf3e 1483  ........7....>..
00008fa0: 786b a2a1 ea23 5b9c 9765 e3b4 a138 b919  xk...#[..e...8..
00008fb0: 653b 546f ce78 1f0c b0d1 87c4 3a89 368b  e;To.x......:.6.
00008fc0: f785 cb4b 15b4 9ce0 ecef da2f f84d 3328  ...K......./.M3(
00008fd0: a334 2fa3 05ec fe49 3b7c c99a 6cb3 6bac  .4/....I;|..l.k.
00008fe0: e2af 0cac fd17 d549 1f3e d6dd 1389 01db  .......I.>......
00008ff0: 95ee 2a3b b5f6 436d e760 e628 8281 5626  ..*;..Cm.`.(..V&
00009000: cab7 6246 6c21 6c53 6806 66e2 48d2 b0e7  ..bFl!lSh.f.H...
00009010: fdd7 2d6c af66 810e f148 ee63 abfc b39e  ..-l.f...H.c....
00009020: 4c86 b2ef ca56 1a98 82aa 49bb 9316 1e46  L....V....I....F
00009030: 7882 9bd9 e60b 454e 4420 454e 4352 5950  x.....END ENCRYP
00009040: 5445 4420 5354 4147 4531 2043 4f4e 5445  TED STAGE1 CONTE
00009050: 4e54 1000 0000 0000 0000 0100 0000 0000  NT..............
```

```python
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import binascii

encrypted_data_hex = """
8329 0650 36b7 45b1 d225 5610 e8f2 ba7c 3b8b f3c8 6179 aa34 3c73
6ca3 16b7 88c4 51ac 324b 3cf5 fdfa ad9a 180c 9ca1 c0e1 14ee 37f9
d618 bf3e 1483 786b a2a1 ea23 5b9c 9765 e3b4 a138 b919 653b 546f
ce78 1f0c b0d1 87c4 3a89 368b f785 cb4b 15b4 9ce0 ecef da2f f84d
3328 a334 2fa3 05ec fe49 3b7c c99a 6cb3 6bac e2af 0cac fd17 d549
1f3e d6dd 1389 01db 95ee 2a3b b5f6 436d e760 e628 8281 5626 cab7
6246 6c21 6c53 6806 66e2 48d2 b0e7 fdd7 2d6c af66 810e f148 ee63
abfc b39e 4c86 b2ef ca56 1a98 82aa 49bb 9316 1e46 7882 9bd9 e60b
"""

encrypted_data = binascii.unhexlify(encrypted_data_hex.replace(" ", "").replace("\n

print(f"Length of encrypted data: {len(encrypted_data)} bytes")
print(f"Raw encrypted data (hex): {binascii.hexlify(encrypted_data).decode()}")

key = b"thanks_to_balda!"
iv = b"butter_soldering"

cipher = AES.new(key, AES.MODE_CBC, iv)

if len(encrypted_data) % AES.block_size != 0:
```

```
Decrypted Message:
Lesson to be learned: always look under the carpet!
This is your flag for the Pico PCB challenge: ph0wn{under_the_mag1c_karpet}
```

PICO PCB

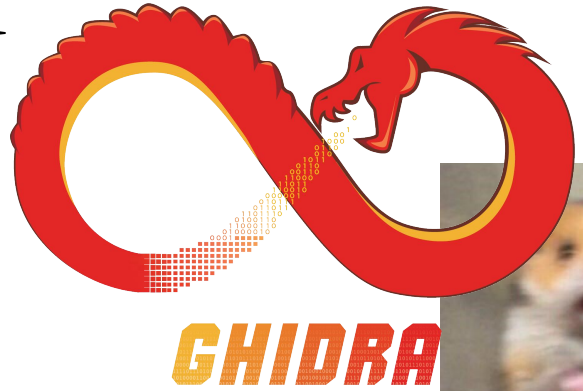
Stage 2 : Reverse

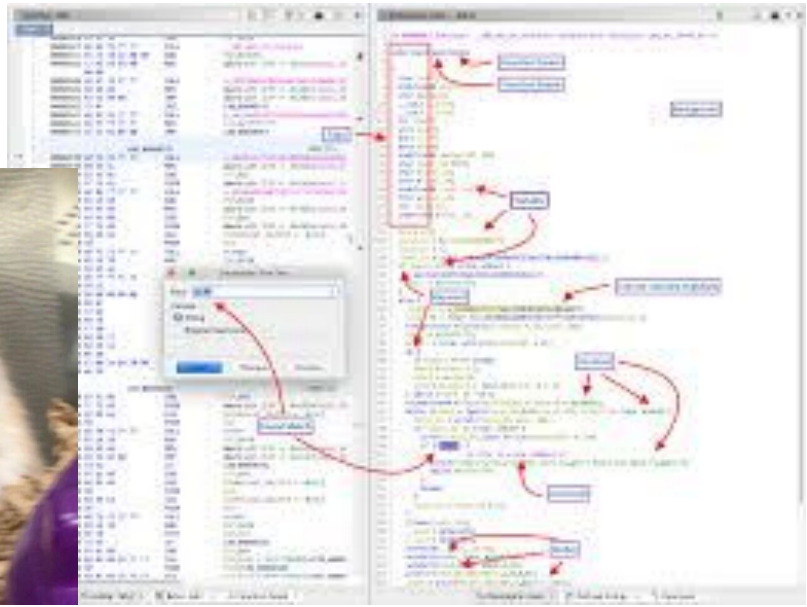
03.

THE CHALLENGE

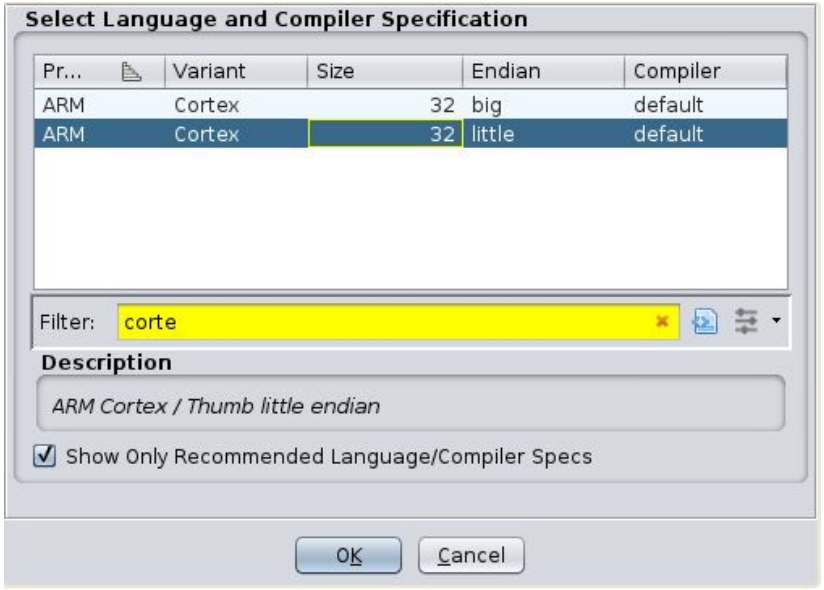
There's a flag in Pico's car.

LOAD THE MEMORY IN GHIDRA

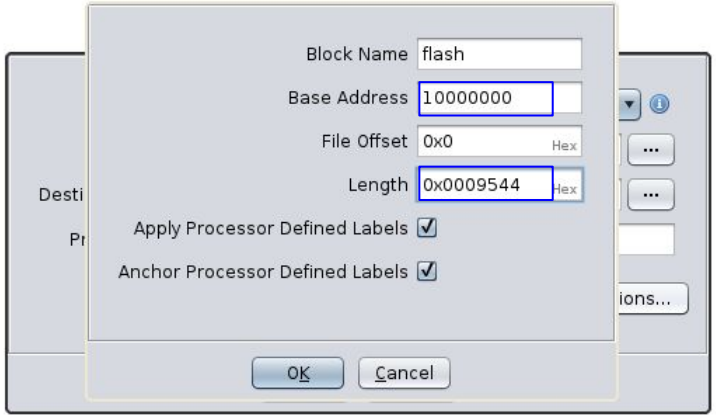




LOAD THE MEMORY IN GHIDRA



CHOOSE THE OFFSET



AND NOW ?

CTRL+F

WHAT ARE WE LOOKING FOR ?

Edit Help

String Search - 117 items - [dump.bin, Minimum size = 10, Align = 1]

...	Loc...	Label	Code Unit	String View	Stri...	Le...	Is Word
⚠	10001dc2		ldr r6,[DAT_10001edc]	"FN4nunwo6o"	string	11	false
⚠	10001df2		ldr r6,[DAT_10001edc]	":N4nunwo6o"	string	11	false
⚠	10002256		eors r0,r2	"P@B@P@Y@K@Y@"	string	13	false
⚠	10004e3b	FUN_1000...	movs r0,#0x0	" pGpGpGpGpG"	string	12	false
A	10006d38	s_Stage_...	ds "Stage %d: %s\n"	"Stage %d: %s\n"	string	14	true
A	10006d48	s_Select_...	ds "Select challenge: "	"Select challenge: "	string	19	true
A	10006d5c	s_STAGE_...	ds "STAGE 2 unlock! This...	"STAGE 2 unlock! This mess...	string	200	true
A	10006e24	s_Starting...	ds "\nStarting challenge...	"\nStarting challenge: %s\n"	string	25	true
A	10006e40	s_Invalid_...	ds "Invalid selection. P...	"Invalid selection. Please try...	string	37	true
A	10006e70	s_Pico_PC...	ds "Pico PCB Loader v%s....	"Pico PCB Loader v%s...\n"	string	24	true
A	10006e88	s_----------...	ds "----------...	"----------"	string	30	true
A	10006ea8	s_Welcom...	ds "Welcome to the Pico ...	"Welcome to the Pico PCB B...	string	30	true
A	10006ee0	s_Kudoz_t...	ds "Kudoz to Balda!"	"Kudoz to Balda!"	string	16	true
A	10006ef0	s_Pico_PC...	ds "Pico PCB challenge -...	"Pico PCB challenge ---------"	string	29	true
A	10006f10	s_Amnesi...	ds "Amnesia. Something i...	"Amnesia. Something is hid...	string	79	true
A	10006f60	s_Turn_lig...	ds "Turn lights ON"	"Turn lights ON"	string	15	true
A	10006f70	s_Turn_lig...	ds "Turn lights OFF"	"Turn lights OFF"	string	16	true

U REMEMBER ?

```
Pico PCB Loader v0.15...
----------------------------
Welcome to the Pico PCB Board
Stage 1: Hardware
Stage 2: Car
Select challenge: Invalid selection. Please try again.

Pico PCB Loader v0.15...
----------------------------
Welcome to the Pico PCB Board
Stage 1: Hardware
Stage 2: Car
Select challenge:
Starting challenge: Hardware
Pico PCB challenge ---------
Amnesia. Something is hidden deep down in my memory but I cant understand it.
```

ANYTHING MORE INTERESTING ?

```
s_______...  ds "\n       ______       +-...  "\n      _____     +------------+"  string
s___//_||_\_...  ds "    __//_||_\\__    |  ...  "  __//_||_\\__   | Pico      |"  string
s_|_||_|__|_...  ds "  |      ||     |__| Ca...  " |    ||    |__| Car Status |"  string
s_'--(_)--(_)...  ds "  '--(_)--(_)-'  +---...  " '--(_)--(_)-' +------------+\n"  string
s_Lights:_...  ds "Lights: %s"                  "Lights: %s"                      string
s_Motor:_...  ds " Motor: %s"                   " Motor: %s"                      string
s_------------...  ds "\n--------------------...  "\n-----------------------"      string
s_Enter_y...  ds "\nEnter your choice: "        "\nEnter your choice: "          string
s_===_H...  ds "\n=== H1dden Pic0 Men...  "\n=== H1dden Pic0 Menu =...  string
s_Passwo...  ds "Password (* to END): "         "Password (* to END): "           string
s_Congrat...  ds "Congrats! Flag is ph0...  "Congrats! Flag is ph0wn{%s...  string
s_Ouch!_T...  ds "Ouch! The engine stal...  "Ouch! The engine stalled!!!"      string
s_VROOO...  ds "\nVR0000000000000M! Y...  "\nVROOOOOOOOOOOOM! Yo...  string
s_Access_...  ds "\nAccess denied!"           "\nAccess denied!"                  string
DAT_1000...  undefined4 3726lA28h            "£7*£*$ $16($7*"                  string
```

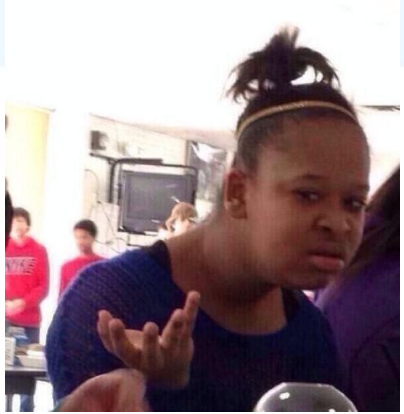
ANYTHING MORE INTERESTING ?

```
s_______...   ds "\n       ______       +-...   "\n     _____     +------------+"
s___//_||_\_...  ds "    __//_||_\\__    |  ...   "  __//_||_\\__  | Pico     |"
s_|_||_|__|_...  ds "  |      ||     |__| Ca...   " |   ||   |__| Car Status |"
s_'--(_)--(_)...  ds "  '--(_)--(_)-'  +---...   " '--(_)--(_)-' +------------+\n"
s_Lights:_...  ds "Lights: %s"                    "Lights: %s"
s_Motor:_...   ds " Motor: %s"                    " Motor: %s"
s_------------...  ds "\n--------------------...   "\n-----------------------"
s_Enter_y...   ds "\nEnter your choice: "         "\nEnter your choice: "
s_===_H...     ds "\n=== H1dden Pic0 Men...      "\n=== H1dden Pic0 Menu =...   string
s_Passwo...    ds "Password (* to END): "         "Password (* to END): "        string
s_Congrat...   ds "Congrats! Flag is ph0...      "Congrats! Flag is ph0wn{%s...  string
s_Ouch!_T...   ds "Ouch! The engine stal...      "Ouch! The engine stalled!!!"  string
s_VROOO...     ds "\nVR0000000000000M! Y...      "\nVROOOOOOOOOOOOM! Yo...   string
s_Access_...   ds "\nAccess denied!"             "\nAccess denied!"            string
DAT_1000...    undefined4 3726LA28h               "£7*£*$ $16($7*"              string
```

LET'S JUMP THERE !

```
                    s_Congrats!_Flag_is_ph0wn{%s}_100070b8          XREF[2]:     FUN_100007a4:100007b0(*),
                                                                                 FUN_100007a4:100007c6(*)
100070b8 43 6f 6e        ds         "Congrats! Flag is ph0wn{%s}\n"
         67 72 61
         74 73 21 ...
```

DOES IT EVEN MEAN SOMETHING ?



LET'S JUMP THERE !

ADDRESS

MEMORY CONTENT

CROSS-REFERENCE
(= USAGE)

AND NOW ?

```
                    *************************************************************
                    *                          FUNCTION                         *
                    *************************************************************
                    undefined FUN_100007a4()
      undefined         r0:1           <RETURN>
      undefined1        Stack[-0x4c]:1 local_4c                          XREF[1]:     100007ee(W)
      undefined4        Stack[-0x54]:4 local_54                          XREF[1]:     100007ea(W)
      undefined4        Stack[-0x60]:4 local_60                          XREF[1]:     100007e6(W)
                    FUN_100007a4
100007a4 f0 b5        push        {r4,r5,r6,r7,lr}
100007a6 c6 46        mov         lr,r8
100007a8 00 b5        push        {lr}
100007aa 92 b0        sub         sp,#0x48
100007ac 27 4d        ldr         r5,[DAT_1000084c]                        = 2000225Dh
100007ae 28 4e        ldr         r6,[DAT_10000850]                        = 100070D8h
100007b0 28 4b        ldr         r3=>s_Congrats!_Flag_is_phOwn{%s}_100070b8,[DA... = "Congrats! Flag is phOwn{%s}\n"
                                                                           = 100070B8h
100007b2 98 46        mov         r8,r3
100007b4 33 e0        b           LAB_1000081e

                    LAB_100007b6                                           XREF[1]:     10000828(j)
100007b6 2b 78        ldrb        r3,[r5,#0x0]=>DAT_2000225d
100007b8 01 2b        cmp         r3,#0x1
100007ba 03 d0        beq         LAB_100007c4
100007bc 30 00        movs        r0=>s_Ouch!_The_engine_stalled!!!_100070d8,r6 = "Ouch! The engine stalled!!!"
100007be 03 f0 99 fd  bl          FUN_100042f4                             undefined FUN_100042f4()
100007c2 2c e0        b           LAB_1000081e

                    LAB_100007c4                                           XREF[1]:     100007ba(j)
100007c4 0c a9        add         r1,sp,#0x30
100007c6 40 46        mov         r0=>s_Congrats!_Flag_is_phOwn{%s}_100070b8,r8 = "Congrats! Flag is phOwn{%s}\n"
100007c8 03 f0 c4 fd  bl          FUN_10004354                             undefined FUN_10004354()
100007cc 1f 4b        ldr         r3=>DAT_2000225d,[DAT_1000084c]          = 2000225Dh
```

LET'S HAVE A DEEPER LOOK

```
void FUN_100007a4(void)

{
  char *pcVar1;
  undefined4 uVar2;
  undefined4 uVar3;
  char cVar4;
  int iVar5;
  undefined4 local_60;
  undefined4 uStack_5c;
  undefined4 uStack_58;
  undefined4 local_54;
  undefined4 uStack_50;
  undefined local_4c;
  undefined auStack_48 [24];
  undefined auStack_30 [24];

  uVar3 = DAT_10000854;
  uVar2 = DAT_10000850;
  pcVar1 = DAT_1000084c;
  do {
    while( true ) {
      cVar4 = FUN_1000064c();
      if (cVar4 != '2') break;
      if (*pcVar1 == '\x01') {
        FUN_10004354(uVar3,auStack_30);
        *DAT_1000084c = '\0';
        FUN_10002bcc(auStack_30,0,0x16);
      }
      else {
        FUN_100042f4(uVar2);
      }
    }
    if (cVar4 == '3') {
      local_60 = *DAT_10000858;
      uStack_5c = DAT_10000858[1];
      uStack_58 = DAT_10000858[2];
      local_54 = DAT_10000858[3];
      uStack_50 = DAT_10000858[4];
      local_4c = *(undefined *)(DAT_10000858 + 5);
      iVar5 = FUN_10000724(auStack_30,0x16);
      FUN_1000078c(auStack_48,auStack_30,0x45,0x16);
      if ((iVar5 == 0x15) && (iVar5 = FUN_10006b40(auStack_48,&local_60,0x15), iVar5 == 0)) {
        FUN_100042f4(DAT_10000864);
        *DAT_1000084c = '\x01';
      }
      else {
        FUN_100042f4(DAT_1000085c);
      }
    }
    else if (cVar4 == '1') {
      *DAT_10000860 = *DAT_10000860 == '\0';
    }
  } while( true );
}
```

```
if (cVar4 == '3') {
  local_60 = *DAT_10000858;
  uStack_5c = DAT_10000858[1];
  uStack_58 = DAT_10000858[2];
  local_54 = DAT_10000858[3];
  uStack_50 = DAT_10000858[4];
  local_4c = *(undefined *)(DAT_10000858 + 5);
  iVar5 = FUN_10000724(auStack_30,0x16);
  FUN_1000078c(auStack_48,auStack_30,0x45,0x16);
  if ((iVar5 == 0x15) && (iVar5 = FUN_10006b40(auStack_48,&local_60,0x15), iVar5 == 0)) {
    FUN_100042f4(DAT_10000864);
    *DAT_1000084c = '\x01';
  }
```

LET'S HAVE A DEEPER LOOK

```
void FUN_100007a4(void)

{
  char *pcVar1;
  undefined4 uVar2;
  undefined4 uVar3;
  char cVar4;
  int iVar5;
  undefined4 local_60;
  undefined4 uStack_5c;
  undefined4 uStack_58;
  undefined4 local_54;
  undefined4 uStack_50;
  undefined local_4c;
  undefined auStack_48 [24];
  undefined auStack_30 [24];

  uVar3 = DAT_10000854;
  uVar2 = DAT_10000850;
  pcVar1 = DAT_1000084c;
  do {
    while( true ) {
      cVar4 = FUN_1000064c();
      if (cVar4 != '2') break;
      if (*pcVar1 == '\x01') {
        FUN_10004354(uVar3,auStack_30);
        *DAT_1000084c = '\0';
        FUN_10002bcc(auStack_30,0,0x16);
      }
      else {
        FUN_100042f4(uVar2);
      }
    }
    if (cVar4 == '3') {
      local_60 = *DAT_10000858;
      uStack_5c = DAT_10000858[1];
      uStack_58 = DAT_10000858[2];
      local_54 = DAT_10000858[3];
      uStack_50 = DAT_10000858[4];
      local_4c = *(undefined *)(DAT_10000858 + 5);
      iVar5 = FUN_10000724(auStack_30,0x16);
      FUN_1000078c(auStack_48,auStack_30,0x45,0x16);
      if ((iVar5 == 0x15) && (iVar5 = FUN_10006b40(auStack_48,&local_60,0x15), iVar5 == 0)) {
        FUN_100042f4(DAT_10000864);
        *DAT_1000084c = '\x01';
      }
      else {
        FUN_100042f4(DAT_1000085c);
      }
    }
    else if (cVar4 == '1') {
      *DAT_10000860 = *DAT_10000860 == '\0';
    }
  } while( true );
}
```

```
if (cVar4 == '3') {
  local_60 = *DAT_10000858;
  uStack_5c = DAT_10000858[1];
  uStack_58 = DAT_10000858[2];
  local_54 = DAT_10000858[3];
  uStack_50 = DAT_10000858[4];
  local_4c = *(undefined *)(DAT_10000858 + 5);
  iVar5 = FUN_10000724(auStack_30,0x16);
  FUN_1000078c(auStack_48,auStack_30,0x45,0x16);
  if ((iVar5 == 0x15) && (iVar5 = FUN_10006b40(auStack_48,&local_60,0x15), iVar5 == 0)) {
    FUN_100042f4(DAT_10000864);
    *DAT_1000084c = '\x01';
  }
```

FUN6B40

```
int FUN_10006b40(int *param_1,int *param_2,uint param_3)

{
  int iVar1;
  int iVar2;
  bool bVar3;

  if (3 < param_3)
    iVar2 = param_
    if ((((uint)pa
    do {
      if (*param_1
      param_3 = pa
      param_1 = pa
      param_2 = pa
    } while (3 < p
  }
  iVar2 = param_3 - 1;
  if (param_3 == 0) {
    return 0;
  }
LAB_10006b50:
  iVar1 = 0;
  do {
    if ((uint)*(byte *)((int)param_1 + iVar1) != (uint)*(byte *)((int)param_2 + iVar1)) {
      return (uint)*(byte *)((int)param_1 + iVar1) - (uint)*(byte *)((int)param_2 + iVar1);
    }
    bVar3 = iVar2 != iVar1;
    iVar1 = iVar1 + 1;
  } while (bVar3);
  return 0;
}
```

```
do {
  if ((uint)*(byte *)((int)param_1 + iVar1) != (uint)*(byte *)((int)param_2 + iVar1)) {
    return (uint)*(byte *)((int)param_1 + iVar1) - (uint)*(byte *)((int)param_2 + iVar1);
  }
  bVar3 = iVar2 != iVar1;
  iVar1 = iVar1 + 1;
} while (bVar3);
return 0;
```

FUN6B40

```
int FUN_10006b40(int *param_1,int *param_2,uint param_3)

{
  int iVar1;
  int iVar2;
  bool bVar3;

  if (3 < param_3)
    iVar2 = param_
    if ((((uint)pa
    do {
      if (*param_1
      param_3 = pa
      param_1 = pa
      param_2 = pa
    } while (3 < p
  }
  iVar2 = param_3 - 1;
  if (param_3 == 0) {
    return 0;
  }
LAB_10006b50:
  iVar1 = 0;
  do {
    if ((uint)*(byte *)((int)param_1 + iVar1) != (uint)*(byte *)((int)param_2 + iVar1)) {
      return (uint)*(byte *)((int)param_1 + iVar1) - (uint)*(byte *)((int)param_2 + iVar1);
    }
    bVar3 = iVar2 != iVar1;
    iVar1 = iVar1 + 1;
  } while (bVar3);
  return 0;
}
```

```
do {
  if ((uint)*(byte *)((int)param_1 + iVar1) != (uint)*(byte *)((int)param_2 + iVar1)) {
    return (uint)*(byte *)((int)param_1 + iVar1) - (uint)*(byte *)((int)param_2 + iVar1);
  }
  bVar3 = iVar2 != iVar1;
  iVar1 = iVar1 + 1;
} while (bVar3);
return 0;
```

LET'S HAVE A DEEPER LOOK

```
void FUN_100007a4(void)

{
  char *pcVar1;
  undefined4 uVar2;
  undefined4 uVar3;
  char cVar4;
  int iVar5;
  undefined4 local_60;
  undefined4 uStack_5c;
  undefined4 uStack_58;
  undefined4 local_54;
  undefined4 uStack_50;
  undefined local_4c;
  undefined auStack_48 [24];
  undefined auStack_30 [24];

  uVar3 = DAT_10000854;
  uVar2 = DAT_10000850;
  pcVar1 = DAT_1000084c;
  do {
    while( true ) {
      cVar4 = FUN_1000064c();
      if (cVar4 != '2') break;
      if (*pcVar1 == '\x01') {
        FUN_10004354(uVar3,auStack_30);
        *DAT_1000084c = '\0';
        FUN_10002bcc(auStack_30,0,0x16);
      }
      else {
        FUN_100042f4(uVar2);
      }
    }
    if (cVar4 == '3') {
      local_60 = *DAT_10000858;
      uStack_5c = DAT_10000858[1];
      uStack_58 = DAT_10000858[2];
      local_54 = DAT_10000858[3];
      uStack_50 = DAT_10000858[4];
      local_4c = *(undefined *)(DAT_10000858 + 5);
      iVar5 = FUN_10000724(auStack_30,0x16);
      FUN_1000078c(auStack_48,auStack_30,0x45,0x16);
      if ((iVar5 == 0x15) && (iVar5 = FUN_10006b40(auStack_48,&local_60,0x15), iVar5 == 0)) {
        FUN_100042f4(DAT_10000864);
        *DAT_1000084c = '\x01';
      }
      else {
        FUN_100042f4(DAT_1000085c);
      }
    }
    else if (cVar4 == '1') {
      *DAT_10000860 = *DAT_10000860 == '\0';
    }
  } while( true );
}
```

```
if (cVar4 == '3') {
  local_60 = *DAT_10000858;
  uStack_5c = DAT_10000858[1];
  uStack_58 = DAT_10000858[2];
  local_54 = DAT_10000858[3];
  uStack_50 = DAT_10000858[4];
  local_4c = *(undefined *)(DAT_10000858 + 5);
  iVar5 = FUN_10000724(auStack_30,0x16);
  FUN_1000078c(auStack_48,auStack_30,0x45,0x16);
  if ((iVar5 == 0x15) && (iVar5 = FUN_10006b40(auStack_48,&local_60,0x15), iVar5 == 0)) {
    FUN_100042f4(DAT_10000864);
    *DAT_1000084c = '\x01';
  }
```

FUN078C

```
void FUN_1000078c(int param_1,int param_2,byte param_3,int param_4)

{
  int iVar1;

  if (0 < param_4) {
    iVar1 = 0;
    do {
      *(byte *)(param_1 + iVar1) = *(byte *)(param_2 + iVar1) ^ param_3;
      iVar1 = iVar1 + 1;
    } while (param_4 != iVar1);
  }
  return;
}
```

FUN078C

```
void FUN_1000078c(int param_1,int param_2,byte param_3,int param_4)

{
  int iVar1;

  if (0 < param_4) {
    iVar1 = 0;
    do {
      *(byte *)(param_1 + iVar1) = *(byte *)(param_2 + iVar1) ^ param_3;
      iVar1 = iVar1 + 1;
    } while (param_4 != iVar1);
  }
  return;
}
```

ANY IDEAS ?

FUN078C

```
void FUN_1000078c(int param_1,int param_2,byte param_3,int param_4)

{
  int iVar1;

  if (0 < param_4) {
    iVar1 = 0;
    do {
      *(byte *)(param_1 + iVar1) = *(byte *)(param_2 + iVar1) ^ param_3;
      iVar1 = iVar1 + 1;
    } while (param_4 != iVar1);
  }
  return;
}
```

ANY IDEAS ?

LET'S RENAME ALL OF THIS

```
if (cVar4 == '3') {
  local_60 = *DAT_10000858;
  uStack_5c = DAT_10000858[1];
  uStack_58 = DAT_10000858[2];
  local_54 = DAT_10000858[3];
  uStack_50 = DAT_10000858[4];
  local_4c = *(undefined *)(DAT_10000858 + 5);
  iVar5 = FUN_10000724(srcMemory,0x16);
  xorFunction(dstMemory,srcMemory,0x45,0x16);
  if ((iVar5 == 0x15) && (iVar5 = strCmp(dstMemory,&local_60,0x15), iVar5 == 0)) {
    FUN_100042f4(DAT_10000864);
    *DAT_1000084c = '\x01';
  }
```

RECAP

STEP 1

LOAD FILE IN GHIDRA

STEP 2

FIND INTERESTING FUNCTIONS

STEP 3

LOOK FOR STRINGS

STEP 4

RENAME THE MINIMUM TO ENSURE IT'S MEANINGFUL

LET'S FIND THE FLAG

```
if (cVar4 == '3') {
  local_60 = *DAT_10000858;
  uStack_5c = DAT_10000858[1];
  uStack_58 = DAT_10000858[2];
  local_54 = DAT_10000858[3];
  uStack_50 = DAT_10000858[4];
  local_4c = *(undefined *)(DAT_10000858 + 5);
  iVar5 = FUN_10000724(srcMemory,0x16);
  xorFunction(dstMemory,srcMemory,0x45,0x16);
  if ((iVar5 == 0x15) && (iVar5 = strCmp(dstMemory,&local_60,0x15), iVar5 == 0)) {
    FUN_100042f4(DAT_10000864);
    *DAT_1000084c = '\x01';
  }
```

LET'S FIND THE FLAG

```
if (cVar4 == '3') {
  local_60 = *DAT_10000858;
  uStack_5c = DAT_10000858[1];
  uStack_58 = DAT_10000858[2];
  local_54 = DAT_10000858[3];
  uStack_50 = DAT_10000858[4];
  local_4c = *(undefined *)(DAT_10000858 + 5);
  iVar5 = FUN_10000724(srcMemory,0x16);
  xorFunction(dstMemory,srcMemory,0x45,0x16);
  if ((iVar5 == 0x15) && (iVar5 = strCmp(dstMemory,&local_60,0x15), iVar5 == 0)) {
    FUN_100042f4(DAT_10000864);
    *DAT_1000084c = '\x01';
  }
```

&LOCAL60 -> *DAT_858 -> ADDRESS -> FLAG XOR WITH 0X45

LET'S FIND THE FLAG

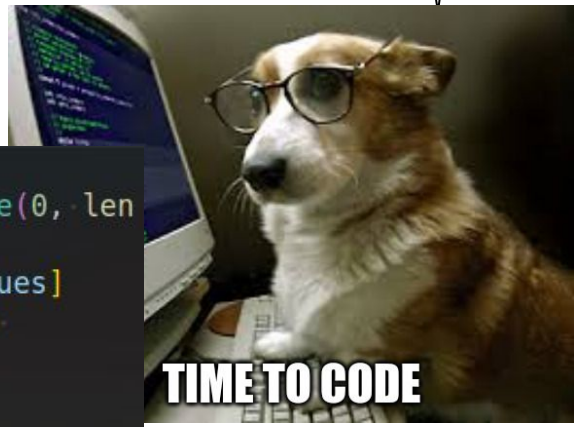
LET'S FIND THE FLAG

```
                    DAT_10000858                                    XREF[1]:     FUN_100007a4:100007e0(R)
10000858 30 71 00 10     undefined4 10007130h                                    ? -> 10007130
```

```
                    DAT_10007130                                    XREF[1]:     FUN_100007a4:100007e4(R)
10007130 33 37 2a 30     undefined4 302A3733h

                    DAT_10007134                                    XREF[1]:     FUN_100007a4:100007e4(R)
10007134 28 1a 26 37     undefined4 37261A28h

                    DAT_10007138                                    XREF[1]:     FUN_100007a4:100007e4(R)
10007138 2a 26 2a 27     undefined4 272A262Ah

                    DAT_1000713c                                    XREF[1]:     FUN_100007a4:100007e8(R)
1000713c 20 24 31 36     undefined4 36312420h

                    DAT_10007140                                    XREF[1]:     FUN_100007a4:100007e8(R)
10007140 28 24 37 2c     undefined4 2C372428h

                    DAT_10007144                                    XREF[1]:     FUN_100007a4:100007ec(R)
10007144 2a              undefined1 2Ah
```

TIME TO CODE

```python
def xor_hex_string(buffer, xor_key):
    hex_values = [int(buffer[i:i+2], 16) for i in range(0, len
    (buffer), 2)]
    xor_result = [value ^ xor_key for value in hex_values]
    flag = ''.join(chr(value) for value in xor_result)
    return flag

buffer = "33372a30281a26372a262a27202431362824372c2a"
xor_key = 0x45
flag = xor_hex_string(buffer, xor_key)
print(flag)
```

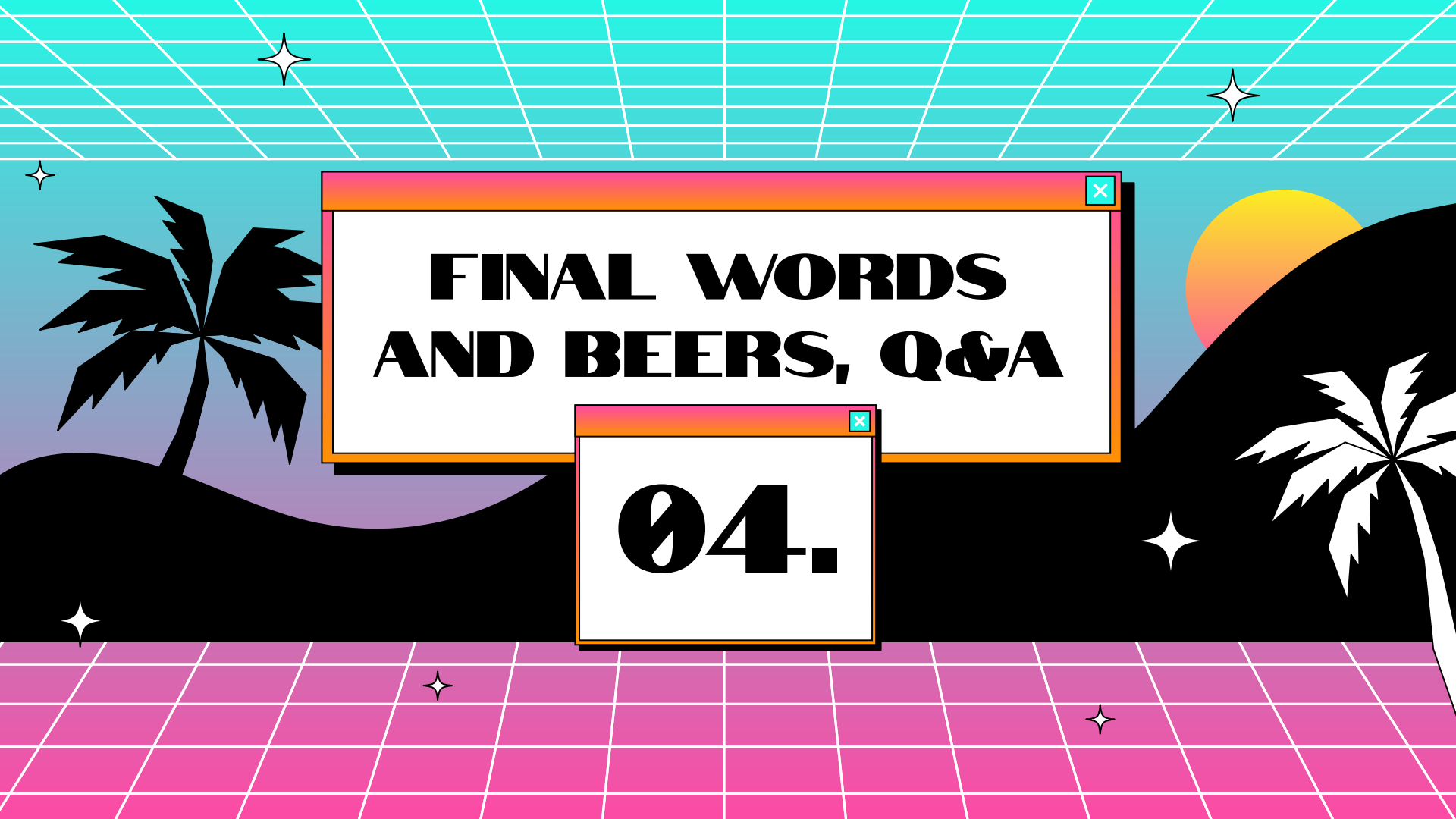


⇒ vroum_crocobeatsmario

CHECKING OUR FLAG

```
Pico PCB Loader v0.15...
---------------------------
Welcome to the Pico PCB Board
Stage 1: Hardware
Stage 2: Car
Select challenge:
Starting challenge: Car

      ______        +------------+
   __//_||_\__      |  Pico      |
  |     ||    |__| | Car Status |
  '--(_)--(_)-'     +------------+

Lights: OFF Motor: OFF
----------------------
 1. Turn lights ON
 2. Start engine

Enter your choice: 3
```

```
=== H1dden Pic0 Menu ===
Password (* to END): vroum_crocobeatsmario
VROOOOOOOOOOOOM! You started the engine!

      ______        +------------+
   __//_||_\__      |  Pico      |
  |     ||    |__| | Car Status |
  '--(_)--(_)-'     +------------+

Lights: OFF Motor: ON
----------------------
 1. Turn lights ON
 2. Read Flag

Enter your choice: 2
Congrats! Flag is ph0wn{vroum_crocobeatsmario}
```


FINAL WORDS
AND BEERS, Q&A
04.

FINAL WORDS

- ➔ FUN CTF AND CHALLENGES
- ➔ NEW BELGIAN FRIENDS (THEY LIKE BEER)
- ➔ (TANNING)

REMERCIEMENTS

- L'ORGA DU FLAG'MALO POUR LE TALK
- LE PHOWN CTF ET LE SHL POUR LES BON MOMENTS PASSÉS
- TOUS LES PARTENAIRES DU FLAG'MALO QUI PERMETTENT D'ORGANISER UN SUPER EVENT CHAQUE ANNÉE
- LE CORPS ENSEIGNANT DE L'IUT POUR CES DEUX SUPER ANNEES
- ET MERCI A VOUS POUR VOTRE ÉCOUTE

THANKS!

DO YOU HAVE ANY QUESTIONS?