HARSHIT MASHRU

PROJECT PRESENTATION

PROJECT IDEA

A PLATFORM-AGNOSTIC USB FORENSIC TOOL FOR HANDS-ON DIGITAL FORENSICS AND INCIDENT RESPONSE. COMMANDS SENT FROM A PHONE TO A WI-FI WEB SERVER ARE RELAYED VIA UART TO A KEYSTROKE INJECTOR, WHICH TYPES THEM ON AN UNLOCKED WINDOWS MACHINE USING A DIGISPARK ATTINY85 AND ESP8266.

PROJECT GOALS

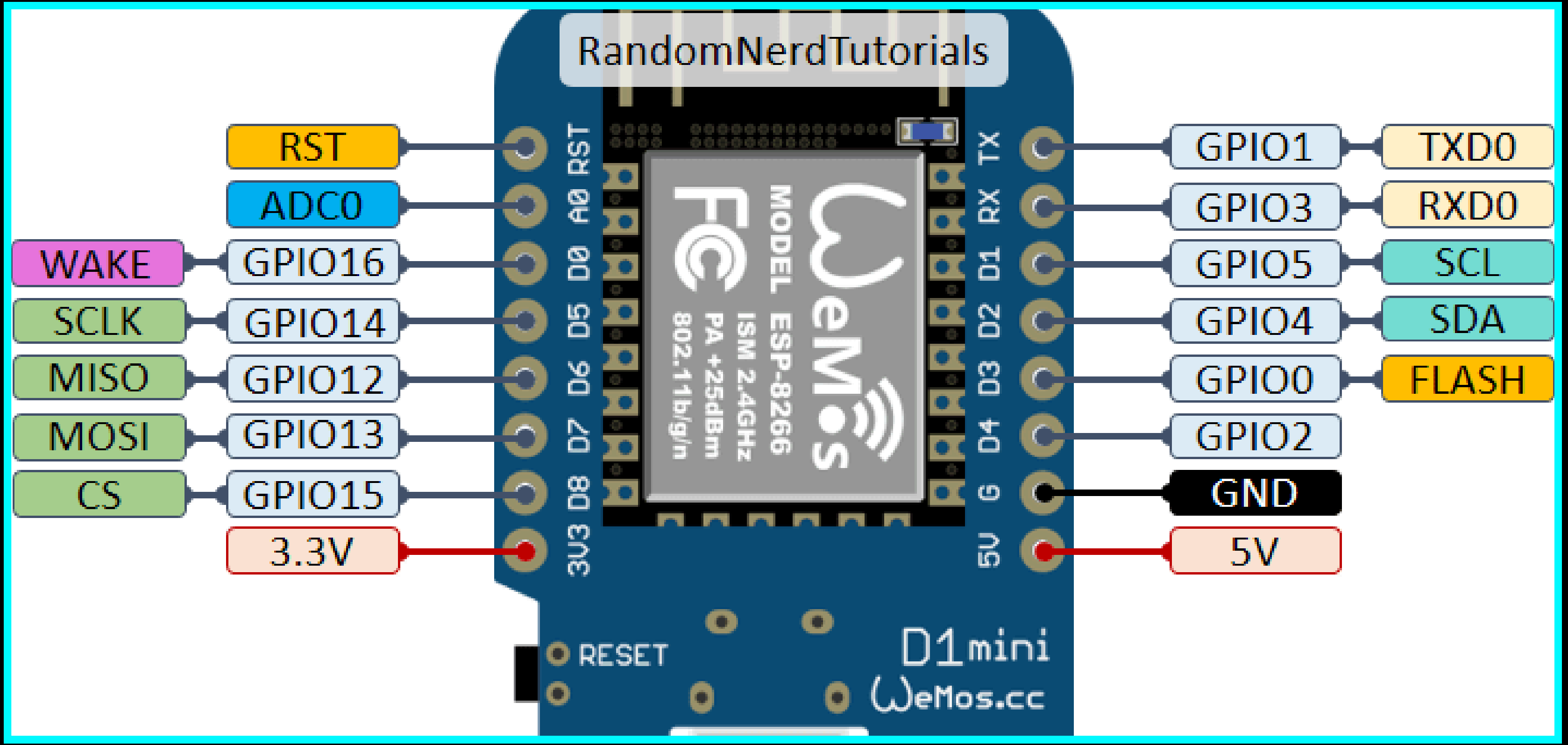
GOAL 1

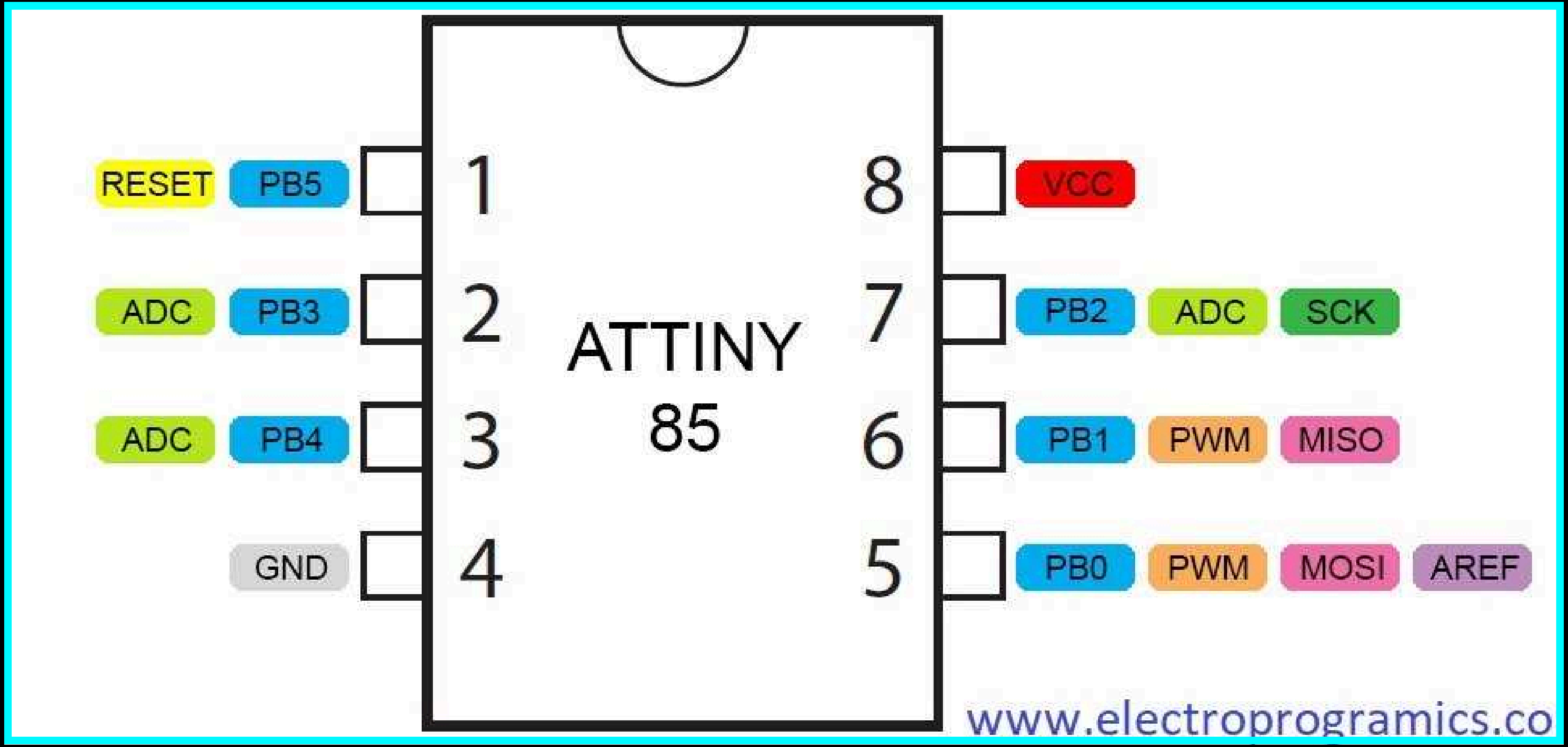
LEVERAGING DIGISPARK ATTINY85'S ABILITY TO PERFORM KEYSTROKES TO EXTRACT CRUCIAL ARTIFACTS

GOAL 2

ENABLING WIFI & CREATING A WEBSERVER ON ESP8266 TO SEND COMMANDS VIA OUR PHONE

ELECTRONICS





ATTINY 85 (LEFT)

The ATtiny85 is a small chip that can be programmed to send keystrokes to a computer. It's often used to automate tasks like typing.

ESP8266 (TOP)

The ESP8266 is a small Wi-Fi chip that can connect devices to the internet. It can also send data or commands, like controlling lights or sending keystrokes to another device

CONNECTING HARDWARE COMPONENTS

- The ATTiny85 will be directly connected to the target machine using the USB port to send keystrokes
- The WIFI chip can be powered by connecting to the machine or directly by connecting the ATTiny’s 5V PIN to ESP8266's 5V PIN
- Connect GND PINs of the both chips
- To transfer the data from the Wifi chip to keystroke chip, as per the code written we will connect D5 PIN to P2 PIN

SOFTWARE COMPONENTS & CHALLENGES

- Used Arduino IDE to flash the chips
- Manufacturer abandoned support for the ATTiny85 chip thus requiring the need to use community maintained libraries
- ATTiny85 doesn’t support UART directly thus requires software emulation for this to communicate with ESP8266
- This caused conflicts between libraries related to sending keystrokes & receiving commands from ESP8266 thus leading to failures.
- Solution found - https://github.com/digistump/DigistumpArduino/issues/128

😎

DEMO

POSSIBLE USECASES

From forensics perspective:

- Browser artifact extraction
- WIFI credentials extraction
- Extracting installed applications and run on startup apps

From a general perspective:

- Installing a backdoor
- Keylogger installation
- Changing background
- Rick roll... and more 😁

FUTURE WORK POSSIBILITIES

- Hosting a server in the public domain to exfiltrate the data from the target machine
- Soldering the 2 chips together
- Devising a way to bypass disk encryption to extract stored passwords

SPECIAL MENTIONS

HELPED WITH DEBUGGING ELECTRICAL ISSUES

🙌

THANKYOU