Last Updated: [02/20/2024]
Guide Version: 1.0

Pre-Class Preparation

Necessary Equipment

- **Computer:** Windows or MacBook.
- **Tablet:** to view lab guide. (Not required but will make it much easier to read the lab guide)
- **A USB-A to USB-C adapter:** for those with only USB-C ports on your computer. If you have a USB-A port on your computer, get a new computer!

Software Installation Options

- **Web Browser:** You must have Google Chrome installed to interact with the Flipper Zero when we load software via the Web Updater. Sorry, no love for Safari.
- **qFlipper application:** Start by downloading the qFlipper application from the Flipper Zero Update Page. This will be our primary tool for interacting with your Flipper Zero.
- **Flipper web updater:** For loading firmware and applications directly from your computer, visit the Flipper web updater. We will be using this in later labs. Please bookmark it for future reference.
- **Flipper iOS or Android app:** Visit the Apple or Android App stores to download the Flipper Mobile App to your mobile devices.
- **NFC Tools for your computer:** Essential for specific labs, download PC NFC Tools.

- **NFC Tools for mobile devices:** This app is also available for download from the Apple or Android App stores.

Additional Resources Familiarity

- Flipper Zero Official Website
- Flipper Zero Documentation

GitHub Repositories

- **Luke's GitHub**
- Flipper Zero Official Firmware
- Extreme Firmware
- Rogue Master Firmware
- Unleashed Firmware
- fzeeflasher for Wi-Fi Dev Board
- uFBT - Micro Flipper Build Tool

Community Links

- Flipper Zero Discord Community
- Reddit r/flipperzero

Course Outline: Day 1

Session 1: Pre-Class Preparation and Device Overview

- 10 minutes: Introduction and Welcome.
- 15 minutes: Device Overview (What's under the hood).
- 15 minutes: Pre-Class Preparation (Equipment prep and Software Installation).

Session 2 : Lab: Weather Station and Sub-GHz

- 10 minutes: Lab: Weather Station Read.
- 30 minutes: Lab: Sub-GHz (Frequency Analysis, Configuration for Recording, Recording the Signal, Saving and Analyzing the Data, Testing Recorded Signal).
- 10 minutes: Break.

Session 3 : Lab: Signal Generator and Wi-Fi Dev Board Flash

- 10 minutes: Lab: GPIO LED Signal Generator (Demo).
- 30 minutes: Lab: Wi-Fi Dev Board Flash (Attaching, Entering Bootloader Mode, Initiating Quick Flash, Completion, Final Steps).
- 30 minutes: .pcap generation labs.
- 10 minutes: Participant Feedback and Evaluation.
- **Homework**: Load the advanced firmware tonight and prepare it for day 2.

Course Outline: Day 2

Session 3: Bluetooth and Infrared Remotes.

- 15 minutes: Demonstrate BLE & Bluetooth capabilities.
- 15 minutes: Demonstrate infrared capabilities.

Session 4: Lab: 125 kHz Low Frequency (LF) RFID Analysis and Emulation

- 10 minutes: Introduction to Different (LF) 125 kHz Card Types.
- 30 minutes: Lab: 125 kHz (LF) RFID analysis, emulation, identification, and cloning.

Session 5: Lab: 13.56 MHz (HF) NFC Analysis and Emulation

- 10 minutes: Introduction to Different HF 13.56 MHz Card Types.
- 10 minutes: Break.
- 30 minutes: Lab: 13.56 MHz (HF) RFID analysis, emulation, identification, and cloning.
- 30 minutes: Reading and writing NTAG215 with the Flipper Zero.

Wrap-up, Conclusion, and Ethical Discussion

- 15 minutes: Tesla Field Trip.
- 15 minutes: Participant Feedback and Evaluation.

Day 1 Info & Labs

Flipper Zero Capabilities Overview (What it can't do?)

High-Frequency RF Analysis

- It's not designed for high-frequency RF signal analysis, like Wi-Fi or Bluetooth hacking, unless you have specific GPIO modules.

Limited Processing Power

- As a handheld device, it doesn't have the processing capabilities of a whole computer, limiting its use in computationally intensive tasks.

No Cellular Capabilities

- Flipper Zero doesn't include cellular connectivity and can't interact with mobile networks.

Limited Range

- Its range for reading signals, especially for NFC and RFID, is limited compared to more specialized equipment.

Limited Legal Use

- Some of its functionalities might be restricted or illegal in certain jurisdictions, especially regarding signal replay and emulation.

Not a Network Hacking Tool

- It cannot hack into networks or perform sophisticated network penetration testing.

Limited Memory

- Storage and memory constraints limit the data it can hold and process.

No Built-in Display for Complex Outputs

- It has a simple screen for essential interaction but is unsuitable for complex data visualization or output.

Not a Replacement for Specialized Tools

- While versatile, it can't replace specialized tools like RF analysis, professional-grade hardware debugging, etc.

Requires Technical Knowledge

- Users need a certain level of technical understanding to utilize its capabilities, especially when developing custom applications fully.

Flipper Zero Capabilities Overview (What it can do?)

Multi-Tool Functionality

- Flipper Zero is a versatile device capable of interacting with various digital protocols and interfaces like RFID, NFC, infrared, Bluetooth, and more.

RFID & NFC

- It can read and emulate different RFID tags and NFC devices, making it useful for various applications, including security research and IoT interactions.

Infrared Communication

- Flipper Zero can control devices like TVs or air conditioners, duplicating and transmitting IR signals with its infrared module.

Radio Frequency Analysis

- It's equipped to analyze and replay radio frequency signals within specific ranges, making it a tool for studying wireless devices and systems.

Digital Protocol Interaction

- Flipper Zero can interact with several digital communication protocols, such as UART, I2C, SPI, 1-Wire, etc., aiding in hardware hacking and debugging.

Custom Applications

- Its open-source nature allows users to develop and run custom applications, expanding its functionality beyond its built-in features.

GPIO Pins for DIY Projects

- The device includes GPIO pins for custom hardware integrations, making it a platform for DIY electronics enthusiasts.

Data Collection and Analysis

- Can be used to gather data from various sensors or systems for analysis and research purposes.

Portable and Battery-Powered

- Its compact, handheld design with an internal battery makes it highly portable for fieldwork.

Community Support

- A robust community of developers and enthusiasts contributes to continuous improvement and extensive documentation.

Lab actions are color-coded to the following colors. If you see the color below, run the command on either the Flipper Zero or your computer.

Commands performed on the Flipper will be Orange.

Commands performed on the Computer will be Violet.

Lab: Physical Setup

Objective: To physically set up the Flipper Zero and power it on.

Procedure

Step 1: Wi-Fi Module
   a. **Do not open yet!** We will flash and use it in a later Lab.

Step 2: Apply Screen Protectors
   a. Follow the instructions included with your screen protectors.

Step 3: Silicone Case
   a. Place the Flipper Zero into the silicone case.

Step 4: SD Card Insert
   a. Insert the SD card into the slot with the pins facing up.

Step 5: Powering On
   a. Power on the Flipper Zero. First Start.

Step 6: Navigation of Menus
   a. Familiarize yourself with navigating through the Flipper Zero menus and settings. Controls

Step 7: Format SD Card
   a. Navigate to Settings > Storage > Format SD Card and click the right directional pad to select Format. **Additional Instructions** MicroSD card setup

Step 8: Customized Settings
   a. Navigate to Settings > System > to customize basic settings such as Hand orientation (Lefty or Righty), Units (For our European & Canadian) friends, and Time and Date formats.

Lab: Updating the Flipper Zero's Firmware

Objective: Install official firmware. Why do we have to update? Navigate to RFID from the main menu and observe an "Update Needed" message.

Procedure

Step 1: Verifying Libraries
   a. Go to the main menu of the Flipper Zero by pressing the Select button
   b. Navigate using the Directional pad to 125 kHz RFID, select, and observe.
   c. What do you see? You should see that an Update Required message is displayed.

Step 2: Computer Connection
   a. Connect your computer to the Flipper Zero with a USB cable and open the qFlipper application on your computer.

Step 3: Access Flipper Zero Labs App Repository
   a. Click on the wrench icon in the upper left-hand corner of the qflipper application.

Step 4: Access Flipper Zero Labs App Repository
   a. Click on the drop-down menu that says RELEASE and select the release code with the small green bar next to it.

Step 5: Access Flipper Zero Labs App Repository
   a. Once the release code has been selected, click on the green button to the right of the qFlipper display that says UPDATE.
   b. A window will appear that says, "Update your flipper firmware." Click UPDATE.

Your Flipper Zero will now update to the current release firmware build. You will see a "Success!" in your qFlipper application when finished. Go to the main menu,

open 125 kHz RFID, and observe. What's the difference? You should now see all the RFID sub-menus.

Lab: Application Installation

Objective: Install Day 1 applications. Why do we have to update? Open RFID from the main menu of Flipper Zero and observe that an "Update Needed" message has been displayed.

Procedure

Step 1: Access Flipper Zero Labs App Repository

a. Close qFlipper on your computer before the next step, or you will get a connection error.
b. Use Google Chrome and navigate to the Flipper Labs App repository at Flipper Lab.

Step 2: Connect Flipper Zero Device

a. Once on the Flipper Labs App repository page, you'll notice a sidebar on the left.
b. In the sidebar, locate and click on My Flipper.
c. Click the Connect button. A popup window that says, "lab.flipper.net wants to connect to a serial port."
d. In the popup window, find your Flipper device listed.
e. Select your Flipper Zero device from the list.
f. Click on the Connect button.

Step 3: Verify Connection and Device Info

a. Click on My Flipper in the sidebar.
b. Your current Flipper Zero device information is displayed if the connection is successful.
c. This information will include Firmware version, build date, SD Card info, Databases, Hardware, Radio Firmware, and Radio stack.

Step 4: Install Apps to Flipper Zero

a. Return to the left column of the Flipper Zero Labs app repository page.
b. Click on Apps.
c. Apps are categorized into Flipper Zero's main categories: Sub-GHz, RFID, NFC, Infrared, GPIO, iButton, USB, Games Media, Tools, and Bluetooth at the top of the apps page.

Step 5: Install Sub-GHz Apps

a. Click on Sub-GH.
b. Install the Weather Station app and Spectrum Analyzer App.

Step 6: Install GPIO Apps

a. Click on GPIO.
b. Install the Signal Generator App and [ESP32] Wi-Fi Marauder App.

Step 7: Install Tools Apps

a. Click on Tools.
b. Install the RFID Detector App and Multi Converter App (For European and Canadian users).

Step 8: Explore Flipper Zero Technologies

a. Take some time to explore all the different Flipper Zero technologies and categories listed in the App repository.
b. See if any additional apps interest you and may be helpful in your projects.

LAB: Weather Station Read

Objective: Using the Flipper Zero device to identify and record remote weather station data.

Procedure

Step 1: Open the Weather Station App

a. Navigate to Apps > Sub-GHz > Weather Station and select and open.
b. Click on Read Weather Station.

Step 2: Weather Station Scanning

a. Your Flipper Zero should be Scanning. Observe the frequency and modulation type.

Step 3: Receiving Weather Station Data

a. You will receive data from the weather station if your frequency and modulation type are correct. If incorrect, click the config button by pressing left on the Directional pad and set the frequency (433.92 MHz) and modulation type (AM650).

Step 4: Weather Station Data Observation

a. Once you've received a reading from the weather station, open the file and note the different parameters of what you've captured (Device type, Channel, Sn, battery status, and weather data.

LAB: Sub-GHz

Objective: Using the Flipper Zero device, identify and record a remote control's frequency and modulation type.

Safety and Ethical Considerations

- Ensure that all activities comply with local laws and regulations regarding radio frequency use.
- Avoid interfering with critical systems or services.

Respect privacy and do not record or analyze device signals without proper authorization.

Procedure

Step 1: Frequency Analysis Supported Frequencies

a. Assemble and power on the LED controller and LED light panel
b. Power on the Flipper Zero and navigate to the Sub-GHz > Frequency Analyzer menu.
c. Operate the remote control near the Flipper Zero.
d. Observe the frequency the remote uses, as displayed on the Flipper Zero.

Step 2: Configuration for Recording

a. Navigate to the Sub-GHz > Read Raw.
b. The frequency should match what you previously observed within the frequency analyzer. If not, access the configuration settings by clicking the left arrow and manually setting the correct frequency and modulation type.
c. Set the frequency to match the one observed in the Frequency Analyzer.
d. Adjust the modulation type if necessary. Note: This may require trial and error, as the correct modulation type is crucial for accurately recording the signal.

Step 3: Recording the Signal (Read) Reading Sub-GHz Signals

a. Ensure the frequency and modulation settings are correct.
b. Select the Read button within the Sub-GHz menu on the Flipper Zero.
c. While reading, you will press multiple buttons on the LED remote, starting with the power button. Observe the file type and encoding.
d. Stop the recording by pressing the back button once sufficient data has been captured.
e. Select the entries captured and press the select button to look at the data recorded.
f. Select Send to send the recorded signal to your LED.
g. Select Save to save the file(s) to your SD card. Use a name you can find later for analysis or emulation.
h. Once saved, navigate to the Sub-GHz > Saved.
i. Select Emulate. A screen will appear that has the signal's information presented. Press Send to have the Flipper Zero send the saved signal.

Step 4: Recording the Signal (Read Raw) Reading Raw Sub-GHz Signals

a. Navigate to the Sub-GHz > Read Raw.
b. The frequency should match what you previously observed within the frequency analyzer. If not, access the Config settings by clicking the left on the Directional pad and manually setting the correct frequency and modulation type. Ensure the frequency and modulation settings are correct.
c. Select the REC (Record) button on the Flipper Zero to record raw signals.
d. While recording, press the power button on your LED remote several times.
e. Observe the energy spikes on Flipper Zero's RSSI graph each time the remote button is pressed.
f. Stop the recording by pressing the Back button once sufficient data has been captured.
g. Select Send on the Flipper Zero. This will transmit the recorded signal(s). Observe the behavior of the LED (e.g., does it respond as it did to the remote?).
h. Select Save to save the file(s) to your SD card. Use a name you can find later for analysis or emulation.

Step 5: Troubleshooting

a. If the Flipper Zero does not record the signal(s) correctly, recheck the frequency and modulation settings.
b. Experiment with different modulation types if the initial attempts are not successful.

Step 6: Documentation

a. Keep a record of the frequencies and modulation types tested, along with the results of each attempt.

b. Document any exciting findings or anomalies for future reference.
c. Following these steps, you should be able to successfully identify and record the frequency and modulation of remote controls using the Flipper Zero, such as garage door openers, LED light controllers, or the thing I told you not to emulate (CAR FOBs!). This experiment can be a valuable learning experience in understanding and working with Sub-GHz frequencies.

LAB: Signal Generator

Objective: The Flipper Zero device sends signals to a single LED connected to the GPIO to demo PWM (Pulse Width Modulation).

Procedure

Step 1: Attaching the LED to the Flipper Zero

a. The LED has two leads. One lead is longer than the other. The longer lead is the positive lead, which should be connected to pin A4 on the left-hand side of Flipper Zero's GPIO.
b. The second shorter lead is the negative lead and should be connected to pin GND on the left-hand side of Flipper Zero's GPIO.

Step 2: Open PWM (Pulse Width Modulation)

a. Navigate to Apps > GPIO > Signal Generator.
b. Select PWM Generator.
c. Change the GPIO Pin setting from 2(A7) to 4(A4) using the right Directional pad button.
d. If everything is set up correctly, your LED will be illuminated.

Step 3: Modify PWM (Pulse Width Modulation)

a. Scroll down to Frequency and change the Frequency from 1000Hz to 1Hz by selecting and pressing the Directional pad down until you get to 1Hz. Observe the output of the LED. The LED should flash once per second.
b. Change the Frequency from 1Hz to 2Hz and observe. The LED will flash once every 500ms.
c. Change the Frequency to 10Hz. The LED will flash every 100ms. This is approximately the rate at which a BSSID sends out beacons in a Wi-Fi network.

Lab: Wi-Fi Dev board Flash

Objective: To flash the Wi-Fi Dev Board with the Marauder firmware.

Procedure

Step 1: Attaching the Wi-Fi Dev Board to your computer

a. Securely connect your Wi-Fi Dev board to your computer via the USB-C port while holding the BOOT button on the Wi-Fi Dev board. This will place the Wi-Fi Dev board into bootloader mode.

Step 2: Accessing the ESP Flasher

a. In a web browser, navigate to fzeeflasher.
b. Click the Connect button in the upper right-hand corner. A popup window says, "fzeeflasher.gethub.io wants to connect to a serial port".
c. Select ESP32-S2 (cu.usbmodem01) and click Connect.

d. If successful, you will see a “Connected successfully” along with device information. If you do not see a successful connection, repeat.

Step 3: Flashing the Wi-Fi Dev board

a. From the Select Model dropdown, select “ESP32-S2”, from the SELECT BOARD drop-down on the left.
b. Select the Latest Version from the VERSION dropdown in the middle.
c. Select “Marauder” from the FIRMWARE dropdown on the right.
d. Verify that all your drop-down settings are correct and click the program button.
e. Once the Wi-Fi Dev board has been successfully flashed, you will receive a message from the webpage terminal that “FLASHING PROCESS COMPLETED”.

Step 4: Connect the Wi-Fi Dev board to the Flipper Zero

a. You can now disconnect your Wi-Fi Dev board from your computer and connect it to your Flipper Zero device.
b. When you connect the Wi-Fi Dev board to your Flipper Zero device, you should see the LED blink once in a blue, green, and red sequence. If you don’t see that sequence, repeat Step 2 and Step 3.

Step 5: Final Steps and LED Indicators

a. Reboot Flipper Zero using the back button and left key. Look for a sequence of blue, green, and red LEDs on the Wi-Fi dev board, signaling a successful firmware flash. The flashing is unsuccessful if you see a continuous red or no LED upon rebooting Repeat the flashing process or seek help from an instructor if necessary.

Lab: Wi-Fi .pcap Generation

Objective: Capturing and analyzing Frames with the Flipper Zero and a computer.

Procedure

Step 1: Accessing the Wi-Fi Marauder App

a. Navigate to the Apps > GPIO > [ESP32] Wi-Fi Marauder folder on your Flipper Zero.

Step 2: Scanning for Access Points (APs)

b. Navigate to Scan AP. Observe the blue LED activation on the board, indicating scanning activity. The Flipper Zero will scan for all visible 2.4GHz BSSIDs (Basic Service Set Identifiers). You should see this on the LCD screen of the Flipper Zero.
c. If you don’t get a blue LED or data, utilize the reset button on the Wi-Fi board to reset the device and try again. If that doesn’t work, hard reset the Flipper Zero by pressing the back and left Directional pad buttons simultaneously.

Step 3: Viewing Scanned Networks

a. Press the back button, navigate to List, and select it.
b. A numbered list displays the detected SSIDs and channel numbers.
c. Browse the list and find a network of interest (Lab AP), particularly noting the sequential number next to the channel number and SSID.

Step 4: Setting the Channel for Capture

a. Press back to return to the main Marauder menu.

b. Navigate to the channel and click the right button on the directional pad to highlight and select Set.
c. Enter the previously noted channel number when prompted with the “channel -s” prompt. (Example: channel – s 11).
d. Press back to return to the main menu of Marauder.

Step 5: Capturing Network Traffic

a. Navigate to the Sniff menu and click the right on the directional pad five times until raw is displayed. Select raw to begin capturing frames.
b. To stop the capture, press the back button.
c. Sometimes, the Flipper loves capturing frames so much that it doesn’t want to stop; if this happens, hard reset the Flipper Zero, press the reset button on the Wi-Fi dev board, and repeat Step 5.

Step 6: Accessing and Downloading the Capture File

a. Connect the Flipper Zero to your computer using a USB cable.
b. Open the qFlipper application on your computer.
c. Navigate to the SD > apps_data > marauder > .pcaps folder.
d. Locate the .pcap file in the folder. Right-click on it and select download.

Step 7: Analyzing the Captured Data

a. Open the downloaded .pcap file in your preferred analysis application.
b. Analyze the captured data for interesting patterns, anomalies, or specific frame types.

Day 2 Info & Labs

Bluetooth & Infrared Remotes

- Demonstrate Bluetooth HID capabilities. HID Controllers
- Demonstrate IR Remote capabilities.
- Demonstrate BLE Attacks.

High-Frequency (NFC) NTAG215 13.56 MHz

- Low-cost solution with limited memory.
- Limited security features.

Low-Frequency (LF) 125 kHz

HID ProxCard II

- Basic encryption and security.
- Short read range, typically a few inches.
- Widely used in older access control systems.

EM4100/EM4200 Cards

- Simple, read-only tags.
- No built-in encryption, low-security level.
- Common in simple identification and access control applications.

T5577 Cards

- Read/write capabilities.
- Can be programmed and reprogrammed multiple times.

- Used in applications where data on the card needs to be updated or changed.

HID DuoProx II

- Dual technology with both RFID and magnetic stripe.
- Useful for systems transitioning from magnetic stripe to RFID.
- Offers the convenience of two technologies in one card.

Indala Proximity Cards

- Proprietary technology offers increased security over standard 125 kHz cards.
- Longer read range than typical LF cards.
- Often used in more secure access control environments.

High-Frequency (HF) 13.56 MHz

MIFARE Classic

- Basic encryption (Crypto1).
- 1K or 4K memory options.
- Widely used in transit, access control, and loyalty programs.

MIFARE DESFire

- Advanced security with AES and DES/3DES encryption.
- Higher storage capacity (up to 8K).
- Suited for multi-application use (e.g., transport, access control, cashless vending).

MIFARE Ultralight

- Low-cost solution with limited memory.
- Ideal for temporary or single-use applications like event ticketing.
- Limited security features.

NFC Enabled Cards

- Operate at the HF band.
- Can be used with NFC-enabled devices like smartphones.
- Versatile use in access control, payments, and data transfer.

ISO 14443 & ISO 15693 Cards

- ISO 14443: Higher security, shorter read range (used in credit cards, passports).
- ISO 15693: Longer read range, used in library books, inventory tracking.

LF and HF cards differ mainly in frequency, read range, and application use. LF cards are typically used in less secure, more straightforward applications. In contrast, HF cards, especially MIFARE DESFire, are used in more secure, complex systems requiring higher storage capacity and advanced encryption methods.

LAB: 125 kHz “LF” RFID Analysis and Emulation

Objective: This lab is designed to provide hands-on experience with RFID technology using the Flipper Zero. Participants will learn to identify, clone, and emulate RFID cards, understand their data structure, and explore the security implications of RFID technology.

Safety and Ethics

- Emphasize the importance of ethical behavior and legal compliance.

- RFID cloning should only be performed in a controlled, educational setting and with permission.

Procedure

Step 1: Reading RFID 125 kHz Signals Reading 125 kHz RFID cards
   a. Power on the Flipper Zero and navigate to the RFID menu.
   b. Place the item you want to read against the back of the Flipper Zero and select read.
   c. If you get a successful read, the item's info will be displayed on the screen of the Flipper Zero.
   d. To emulate or save, click More by using the "right" button on the directional pad.
   e. Save the file with the name "WLPC_RFID."

Step 2: Emulating RFID 125 kHz Signals
   a. Navigate to the RFID > Saved Menu.
   b. Select the file WLPC_RFID that was saved earlier.
   c. Select Emulate and place the back of your Flipper Zero against the RFID reader.

Step 3: Cloning RFID 125 kHz Data to T5577 Card Writing data to T5577 cards
   a. Navigate to the RFID > Saved Menu.
   b. Select the file WLPC_RFID that was saved earlier.
   c. Select Write and place the back of your Flipper Zero against the RFID T5577 card.
   d. If the task is completed, your Flipper Zero will briefly display the "Writing" and "Success" messages.
   d. Take the card and read it with the Flipper Zero. Does the data payload match the file WLPC_RFID?

Lab: 13.56 MHz "HF" NFC Analysis and Emulation

Objective: This lab is designed to provide hands-on experience with NFC technology using the Flipper Zero. Participants will learn to identify, clone, and emulate NFC cards, understand their data structure, and explore the security implications of RFID technology.

Safety and Ethics

- Emphasize the importance of ethical behavior and legal compliance.
- RFID cloning should only be performed in a controlled, educational setting and with permission.

Procedure

Step 1: Reading NFC 13.56 MHz Signals Reading NFC Cards
   a. Power on the Flipper Zero and navigate to the NFC menu.
   b. Place the item you want to read against the back of the Flipper Zero and select read.

c. If you get a successful read, the item's info will be displayed on the screen of the Flipper Zero.
d. To emulate or save, click More using the "right" button on the directional pad.
e. Save the file with the name "WLPC_NFC".

Step 2: Emulating NFC 13.56 MHz Signals

a. Navigate to the NFC > Saved Menu.
b. Select the file WLPC_NFC that was saved earlier.
c. Select Emulate and place the back of your Flipper Zero against the RFID reader.
d. Test your MIFARE 1K device on the NFC reader.

Step 3: Cloning NFC 13.56 MHz Data to MIFARE 1K Device Writing data to magic cards

a. Navigate to the Apps > NFC > NFC Magic Menu.
b. Select Check Magic Tag.
c. Place the back of your Flipper Zero against the MIFARE 1K device.
d. If the task is completed, your Flipper Zero will display "Magic card detected Classic Gen 1A/B"
e. Click the right directional pad to select More.
f. Select Write. A directory of saved items will appear. Select the file you saved earlier named NFC.
g. You will receive a "Risky operation" message on the Flipper Zero. Select Continue.
h. Once the info has been written, you will receive a "Success" message.
i. Test your MIFARE 1K device on the NFC reader.