# Boeing Bluetooth Protocol Analytical Research: Semester 2 Sprint 2

*By: Caroline Terre, Matthew Irvin, Gianna Scarangelli, Jonah Rowell, Connal Grace*


EMBRY-RIDDLE
Aeronautical University

# Project Proposal

- Obtain IoT/Bluetooth devices
- Evaluate security of common IoT devices and protocols such as Bluetooth and Zigbee
- Produce Final White Paper presentation of findings

# Why?

**Current ways bluetooth is actively used on commercial aircraft**

- Refueling process
- Tire pressure
- Entertainment Systems
- Passengers

**Advancements that may be added in the future**

- Temperature tracking
- Airplane Monitoring System

# Brief Overview

- Main goal: discover what possible ways Bluetooth Low Energy and Zigbee may be interrupted or exploited within the realm of aviation
- This semester we have:
  - Researched and tested existing vulnerabilities and softwares for Bluetooth Low Energy
  - Setup Bluetooth audio profiles
  - Researched and tested Flipper Zero Bluetooth exploits
  - Setup BTLE packet detection for data logging purposes

# Purchases Overview

Budget: $25,000

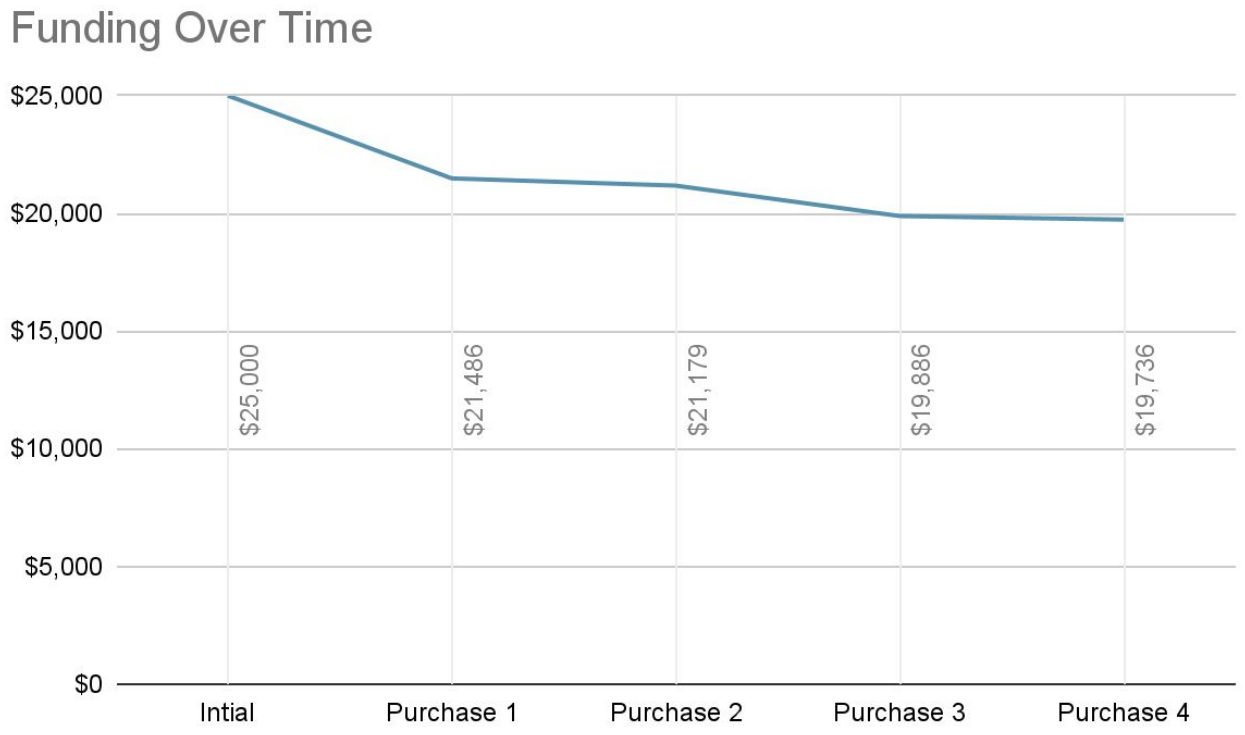
## Current Possession

- 5 Raspberry Pi CanaKit
- 1 Zigbee Development Board
- 2 Hack RF Ones (software defined radio)
- 1 ESP32 Development Board
- 10 Ethernet cables
- 3 Flipper Zero
- 3 Raspberry Pi Keyboards
- 3 Raspberry Pi Displays
- 3 SSD 1TB

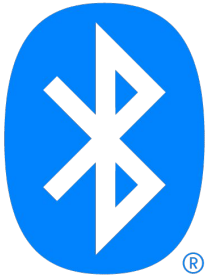
## Ordered & Awaiting

- 2 Antenna for HackRF
- 3 Micro SD
- 1 Mini Hdmi to Mini HDMI Cable
- 10 Mini HDMI to USB A Cables
- 3 HackRF One
- 2 Ubertooth
- 5 BBC MicroBit

# Purchases Timeline



# Wireless Protocols



## Bluetooth

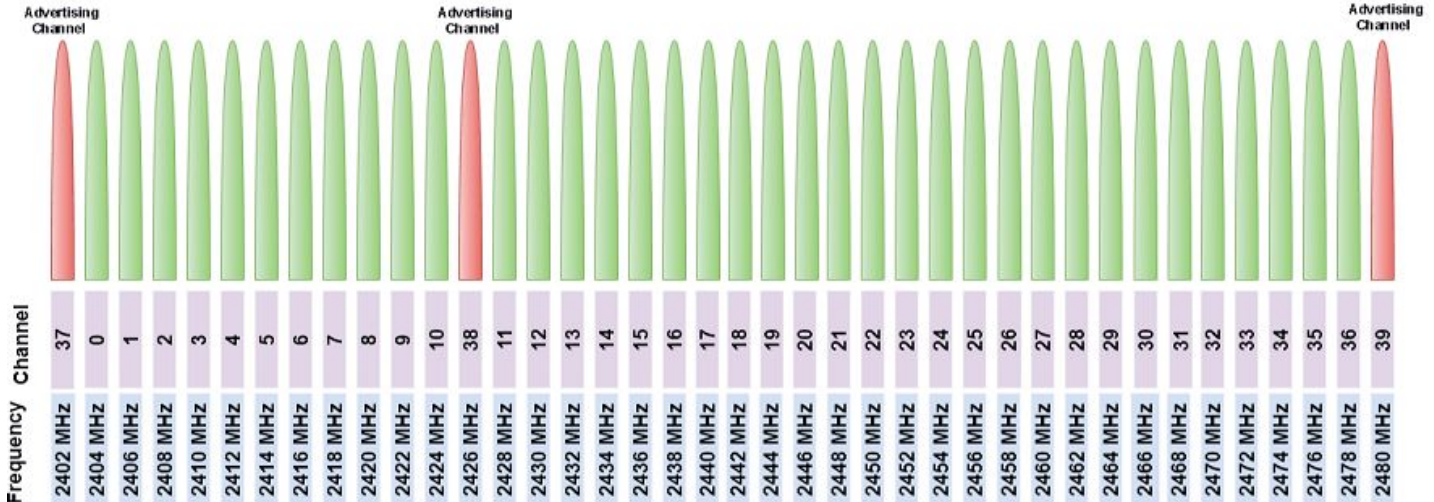
- Short range wireless data transfer standard
- Operates at around 2.4 GHz
- Used in tablets, smartphones and laptops
- Used for high data transfer rate applications


## Zigbee

- Operates around 2.4 GHz and 900 MHz
- IEEE 802.15.4-based
- Often used for low power, low data and low cost
- Commonly used in mesh networks

# Bluetooth Low Energy

- Designed for low power and short range applications
- Operates in the 2.4GHz band with range of 100 meters
- Uses 40 channels compared to 80 with classic Bluetooth
- Channels 37, 38, 39 are used for advertising



# Bluetooth Devices

ESP32

HackRF One


Flipper Zero

# Bluetooth Vulnerabilities

- Insecure Pairing Methods & Authentication Vulnerabilities => Brute Force Attack
- Eavesdropping Vulnerabilities => Man-in-the-Middle Attack
- Security Vulnerabilities => Bluesnarfing
- Bluejacking
- Blueborne Vulnerability
- Blue Low Energy Vulnerabilities
- Bluetooth Standards => Bluetooth Impersonation Attack
- Bluetooth Protocol => Denial-of-Service Attack
- Lack of Firmware Updates

# Requirements

- All devices establish proper and secure connection as defined
- All signals and data rates will operate/transmit between given minimum and maximum standards
- Controlled testing environment assuming no interruptions
- Other requirements for security, software interfaces

# Use Case for Aviation

- Passengers using Bluetooth headphones while on board an Airplane
- To simulate this use case we have two ESP32 communicating with each other using the Advanced Audio Distribution Protocol
- One ESP32 acts like an audio device and transmits sound while the other receives it

# Final Design

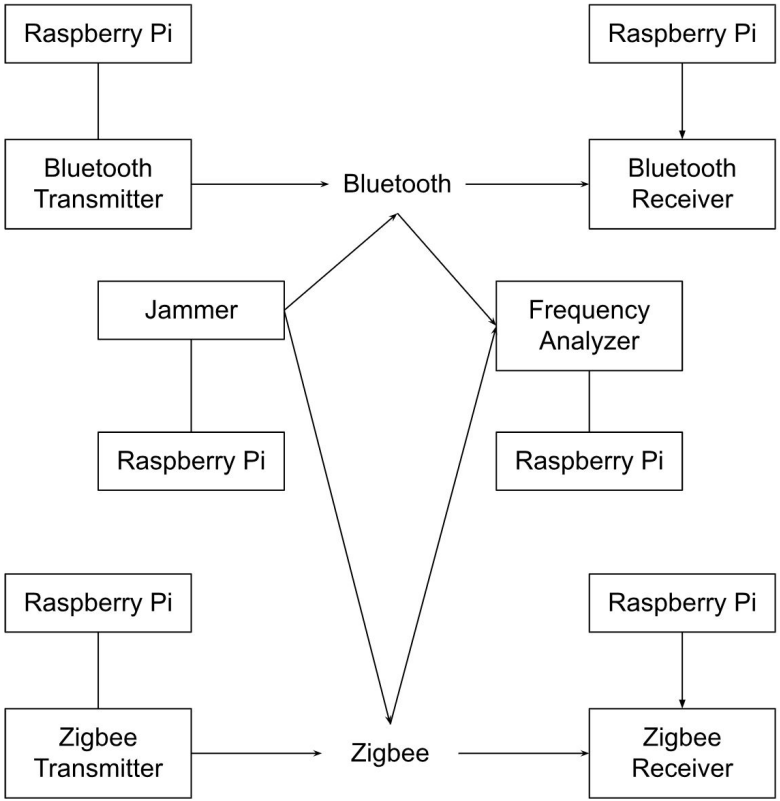
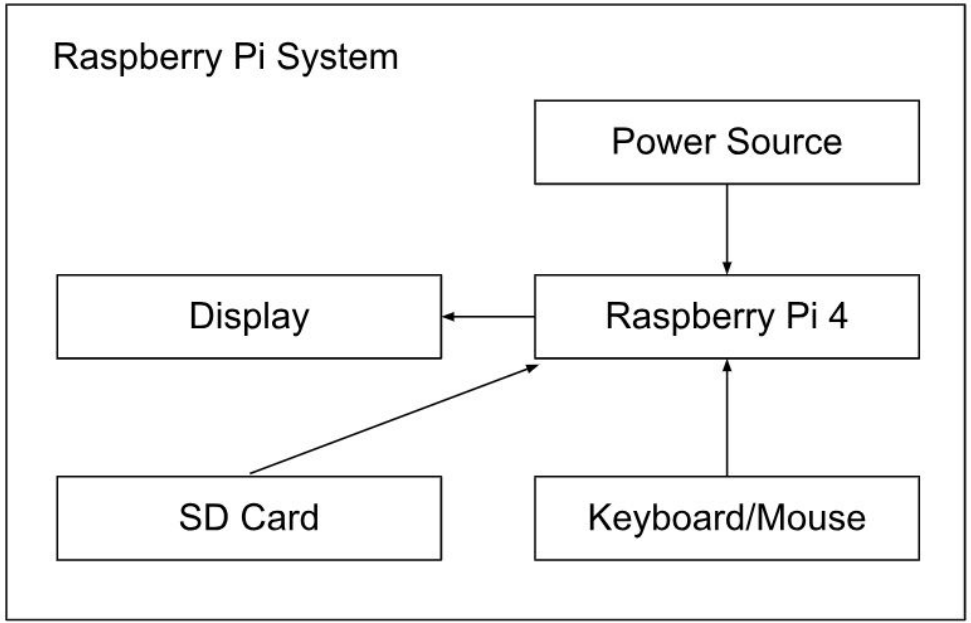
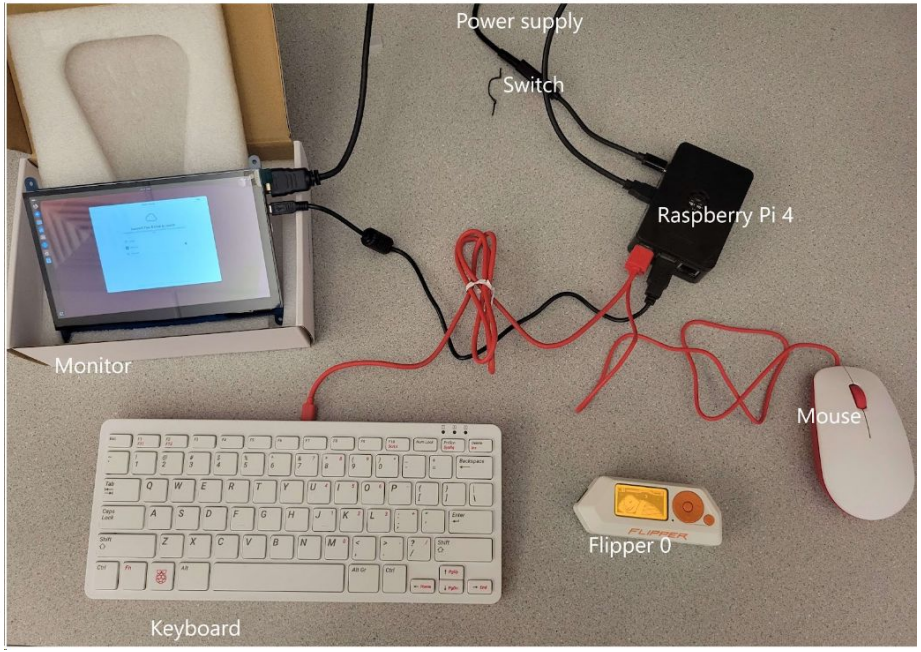


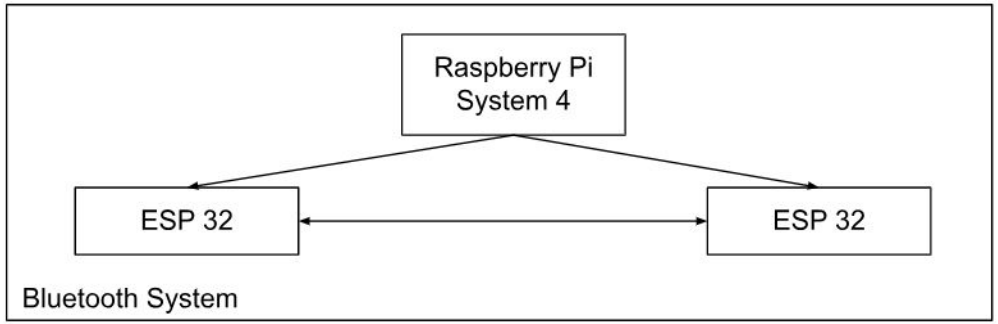

Figure 1: High-Level System Architecture Diagram

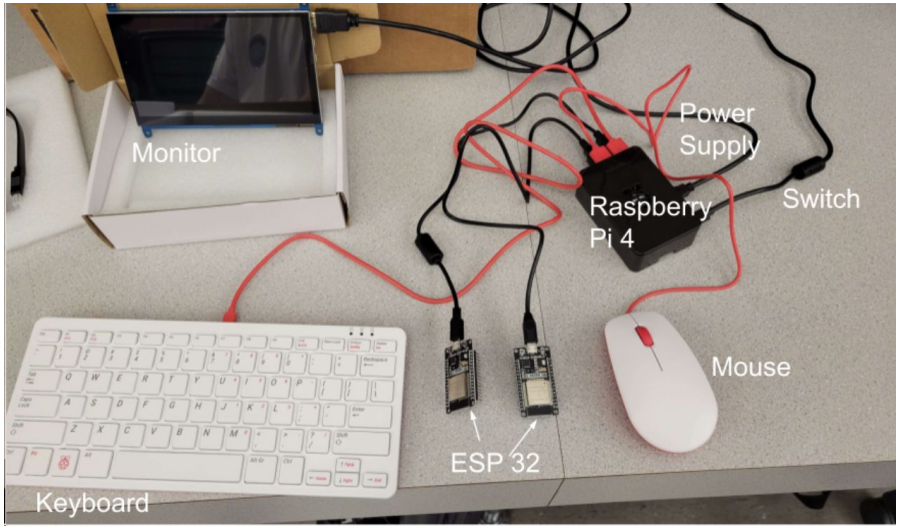
# Raspberry Pi System



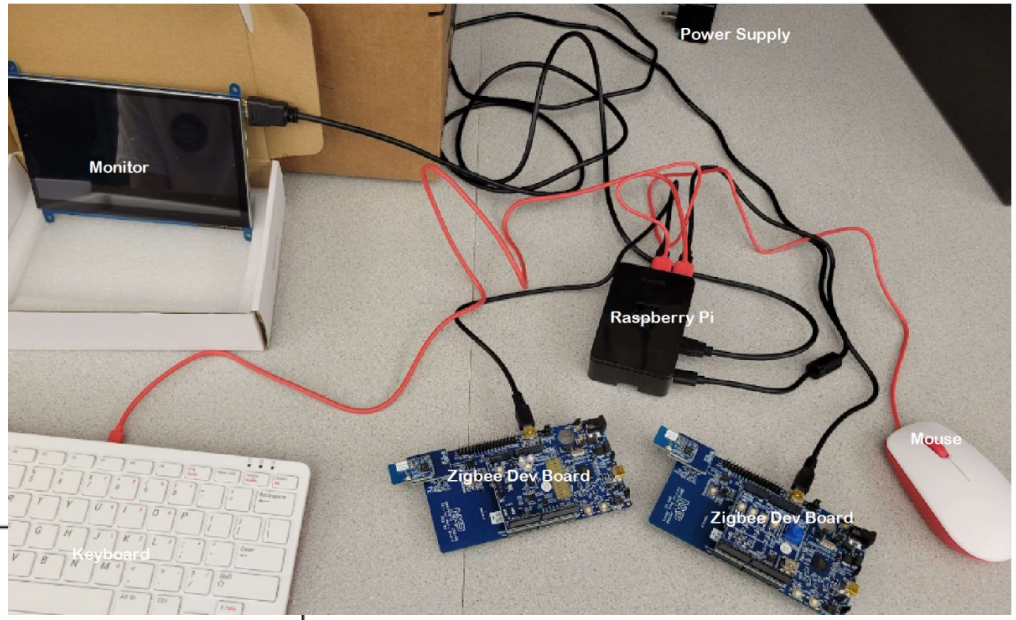
# Bluetooth System

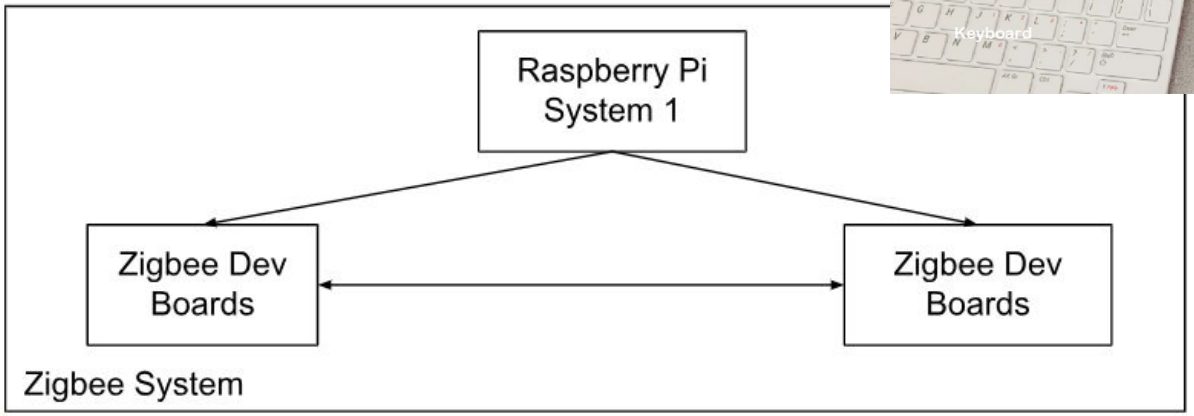


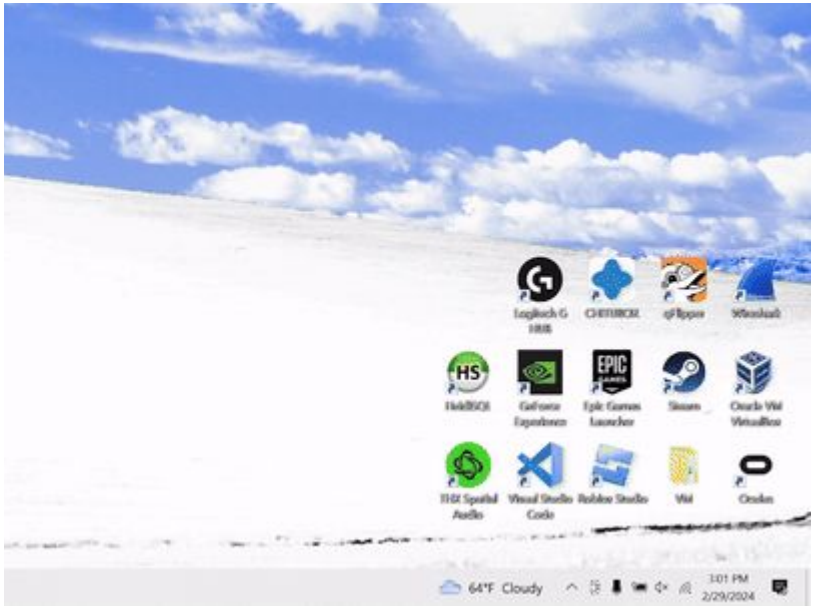
# ESP32 Testing

# Zigbee System



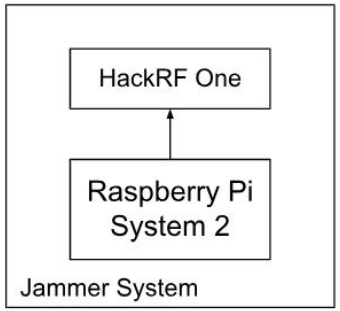



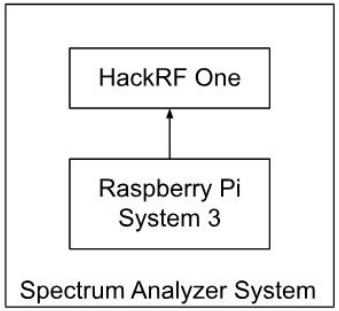
# Flipper Zero

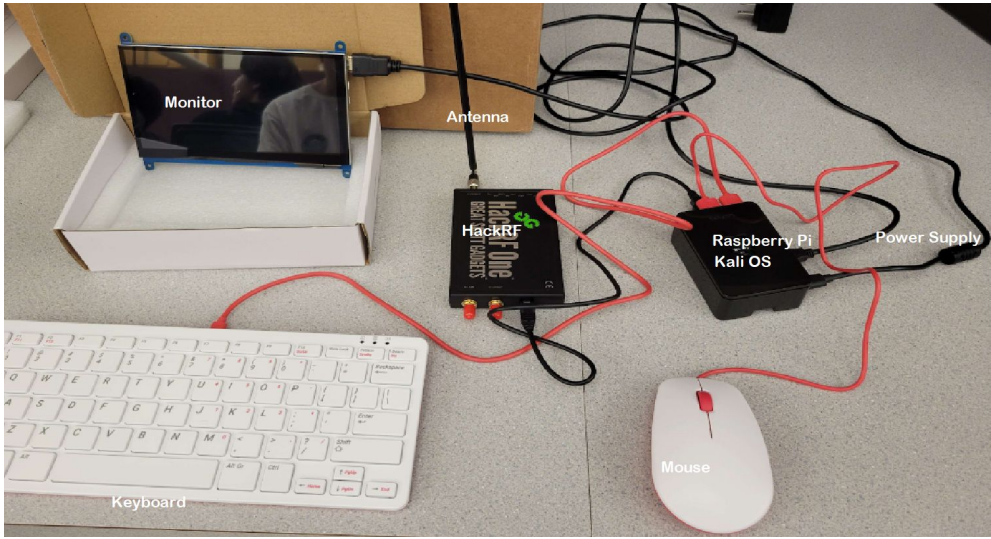



This is a Flipper Zero Bluetooth advertisement spam attack. It is done in 100 microsecond intervals. This can be done on Apple and Android devices as well.

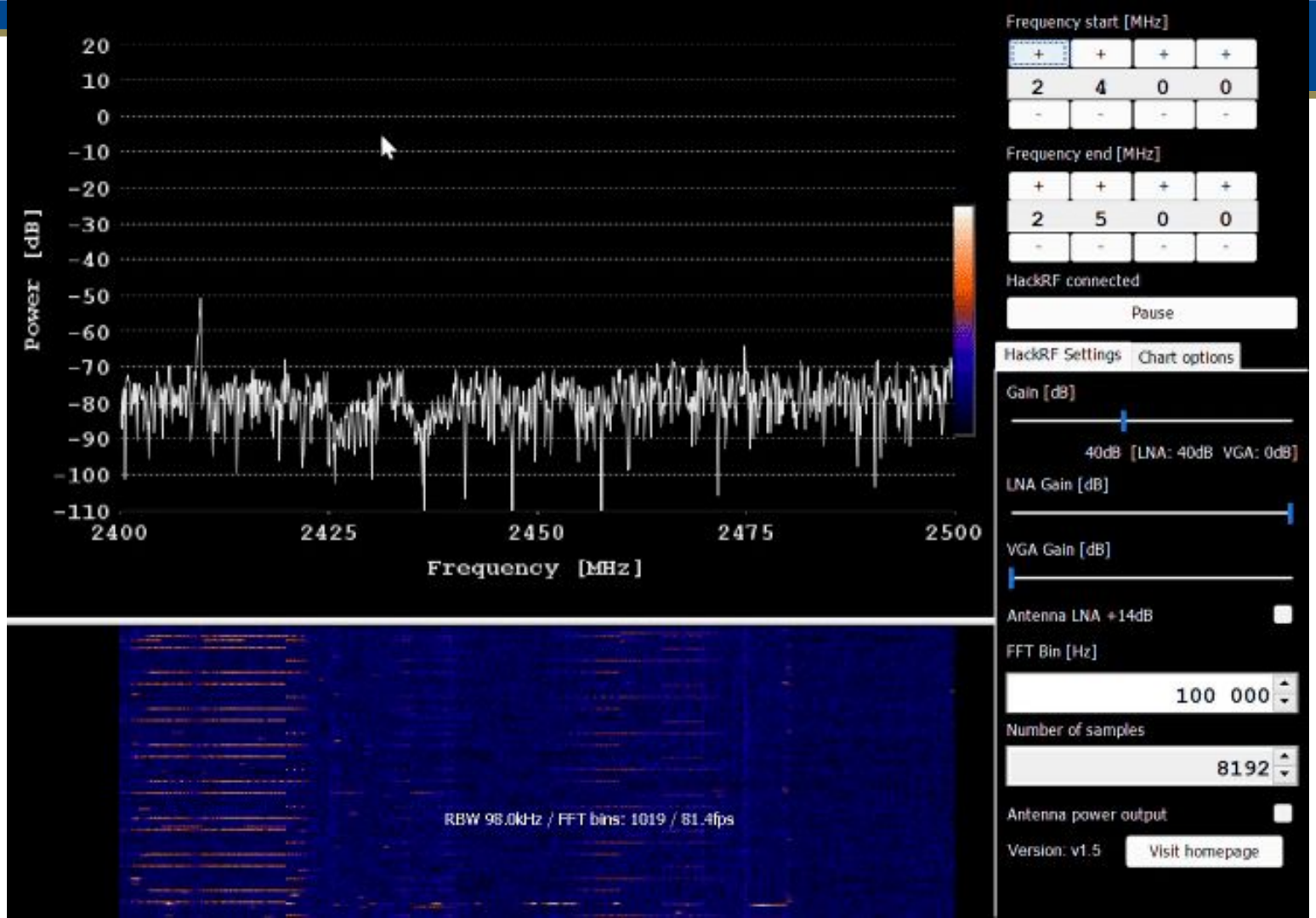
# Software Defined Radio System



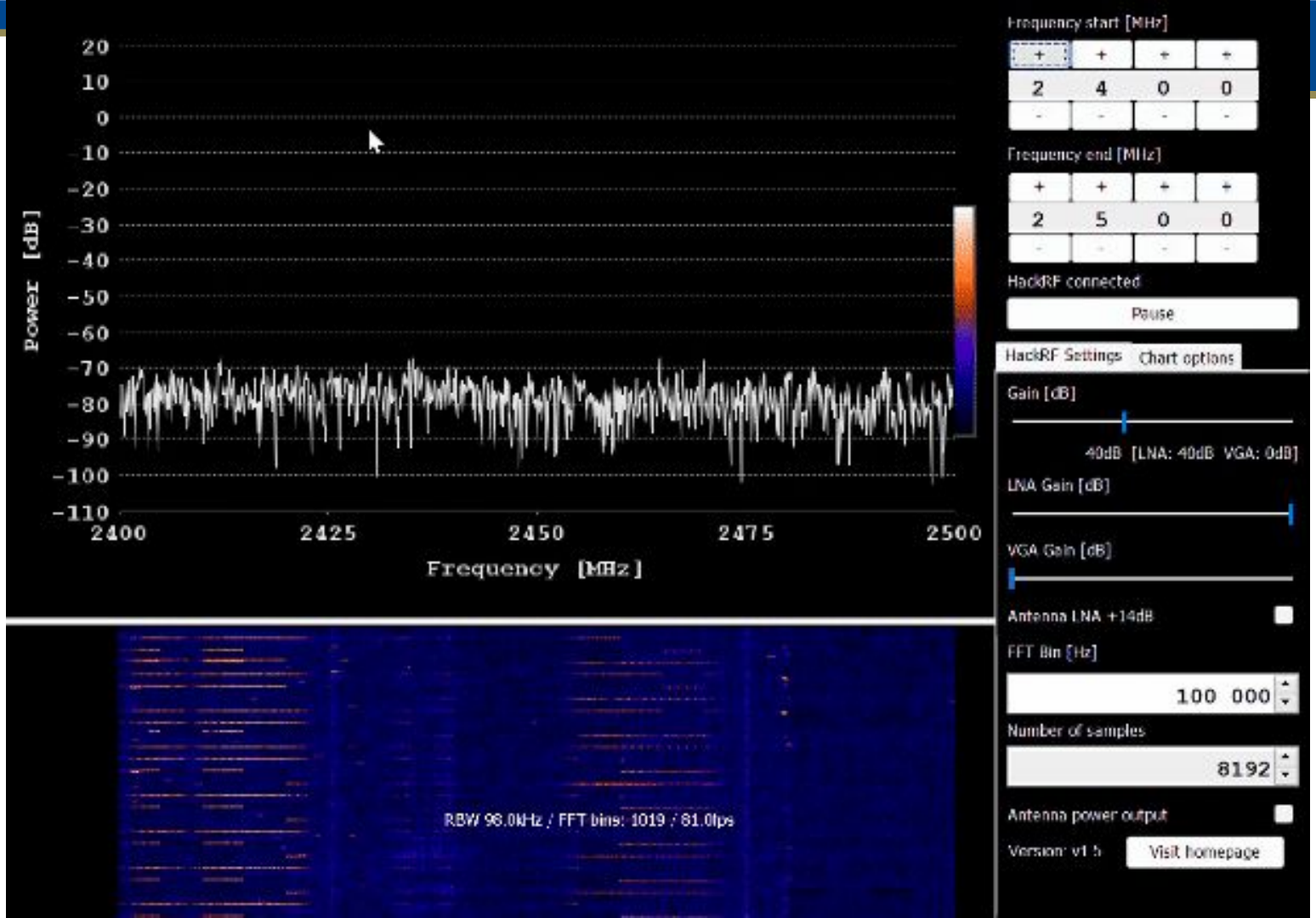



# Hack RF Testing



# Hack RF Testing



# BTLE Packet Analyzer System

- Open source software developed by Jiao Xianjun using HackRF
- Can send and detect BTLE packets
- Provides parameters such as time, advertising address and packet payload
- Allows us to log BTLE packet traffic on specific channel

```
0000127us Pkt001 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0a8eba851db0 Data:16ff0600010f300270ae9a7afd3f73e8894b11d76167e48cc486e456eb51a8 CRC1
0032191us Pkt002 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:5eff060001093022fc97c8fec10efa01e5a7562fe3629b679f30a6ce32a118 CRC1
0263710us Pkt003 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0a8bbe851cb0 Data:1eff0600010f200270ae9e7afd3d73e88b4b11d76167e58cc486e456eb51b8 CRC1
0129590us Pkt004 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL37 AdvA:0a8bba851cb4 Data:1eff0600010f200270ae9e7afd3d73e8894b11d7e167e58cc4866456eb51a8 CRC1
0001452us Pkt005 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060801092022fc97c8fec10efa01e5a7562fe3639b279f30a2ce3261d0 CRC1
0163411us Pkt006 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:20a7bc260639 Data:1eff060001092026b3c4ddce90cadc0f5ca33e638f3998f5b2f4556c4eb919 CRC1
0129692us Pkt007 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:20a7bc260639 Data:1eff060001092026b3c4ddce90cadc0f5ca33c8b86f8fe6aed15bca6e79e54 CRC1
0132115us Pkt008 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060001092022fc97c8fec10efa01e5a7562fe3629b279f30a2ce3261d0 CRC0
0196345us Pkt009 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0a8bba851cb4 Data:1eff0600810f200270ae9e7afd3d73e8994b11476167e5c8c6946452eb51a8 CRC1
0098678us Pkt010 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:28b2ba851cb0 Data:14f90600010f200270ae9e7afd3d73e8895b11d76167e58cc486e456eb51a8 CRC1
0033510us Pkt011 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060001092022fc97c8fec10efa01e5a7562fe3629b279f30a2ce3261d0 CRC0
0196462us Pkt012 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060001092022fc97c8fec10efa01e5a7562fe3629b279f30b2ce3261d0 CRC1
0261563us Pkt013 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:20a6bc360639 Data:1eff0680110900026b3c4ddce90cbdc0f5ea33eab82f8fe6aed95bca6e79e54 CRC1
0033528us Pkt014 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL23 AdvA:473685b8d6c4 Data:02011b0dff4c08160811aaec6dbb8c58bd CRC1
```

# Difficulties

- Timeline of ordering & receiving equipment
- Moving rooms in order to work & short class time
- Software/operating system compatibility
- Outdated software/vulnerabilities
- Operating system corruption
- No antennas for HackRF (still waiting for order)

# Future Goals

- Finalize proper test bed functioning (particularly A2DP/AVRCP Bluetooth)
- Begin with performing jammer attack
- Attempt to exploit and explore other vulnerabilities within these devices
- Write-up of our findings

# Thank You Boeing!