IoT Sensor Blinding

Milestone #3

Alex Winstead (awinstead2015@my.fit.edu)
Xuchao (Steven) Jiang (xjiang2017@my.fit.edu)
Cole Clements (cclements2016@my.fit.edu)
Jeremy Gluck (jgluck2016@my.fit.edu)
Todd St. Onge (tstonge2016@my.fit.edu)

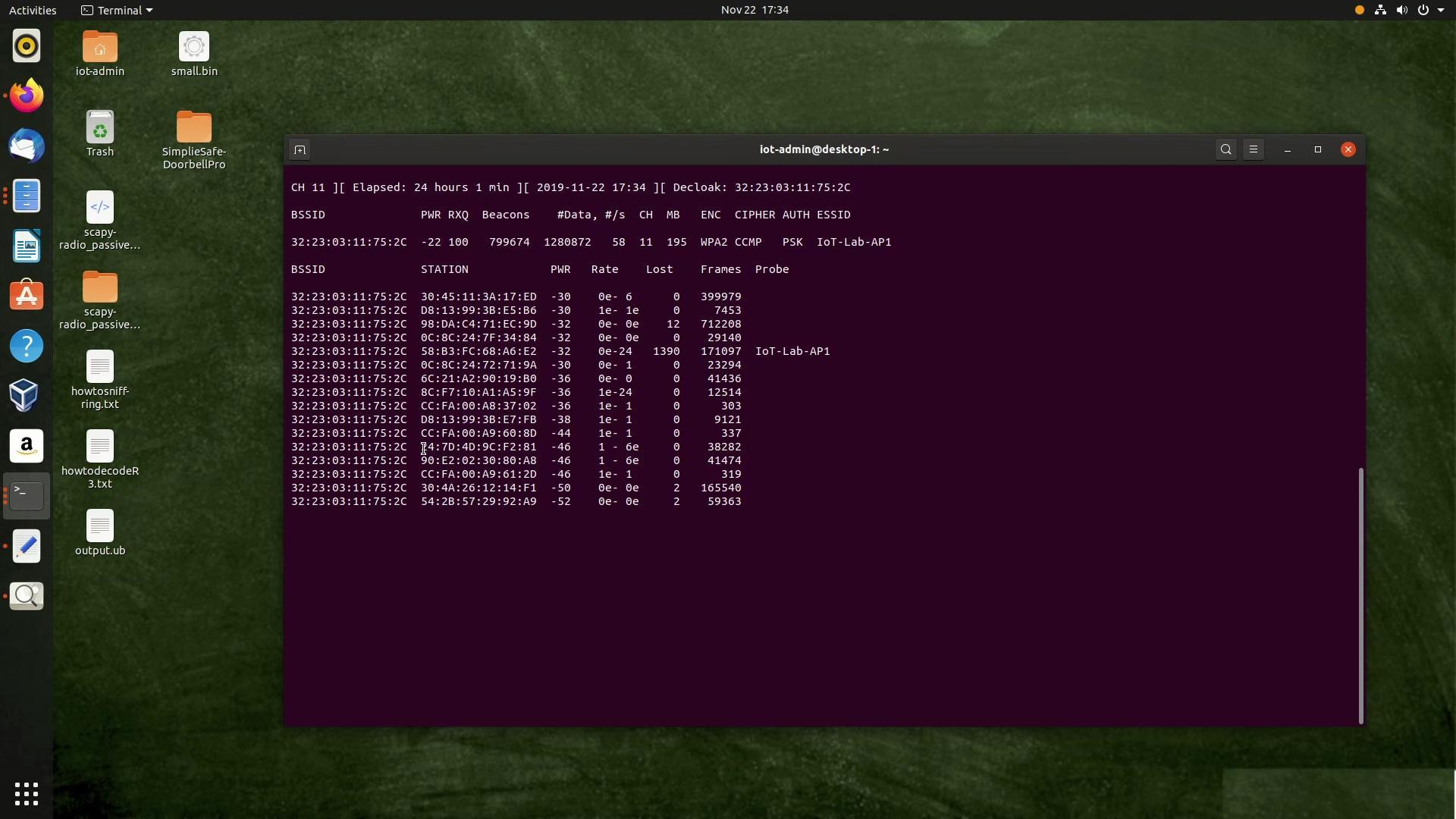
Matthew Craven (mcraven2015@my.fit.edu)

Goals for Milestone 3

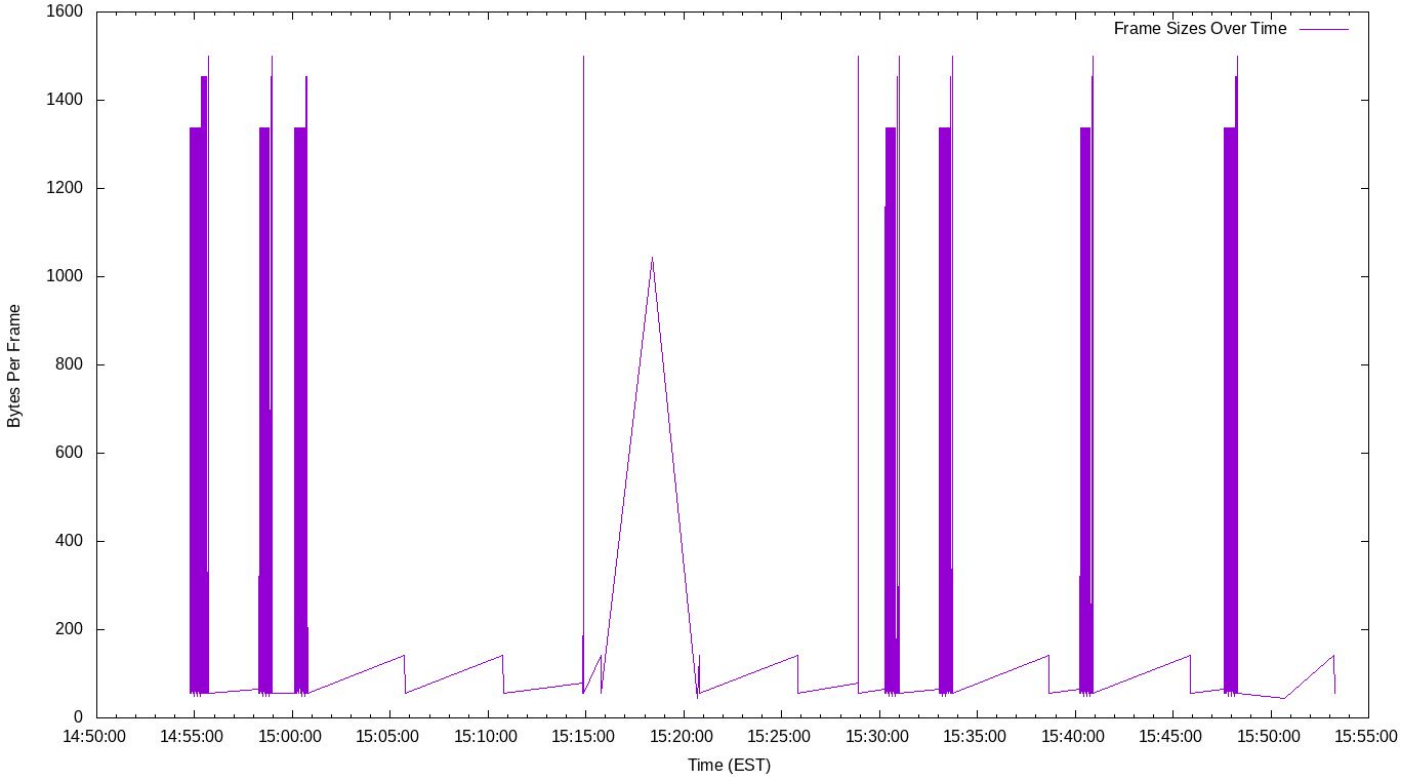
1. Recreate past research
2. Capture network traffic
3. Buildup IoT lab and standardize procedures
4. Label data sets

Recreate Past Research

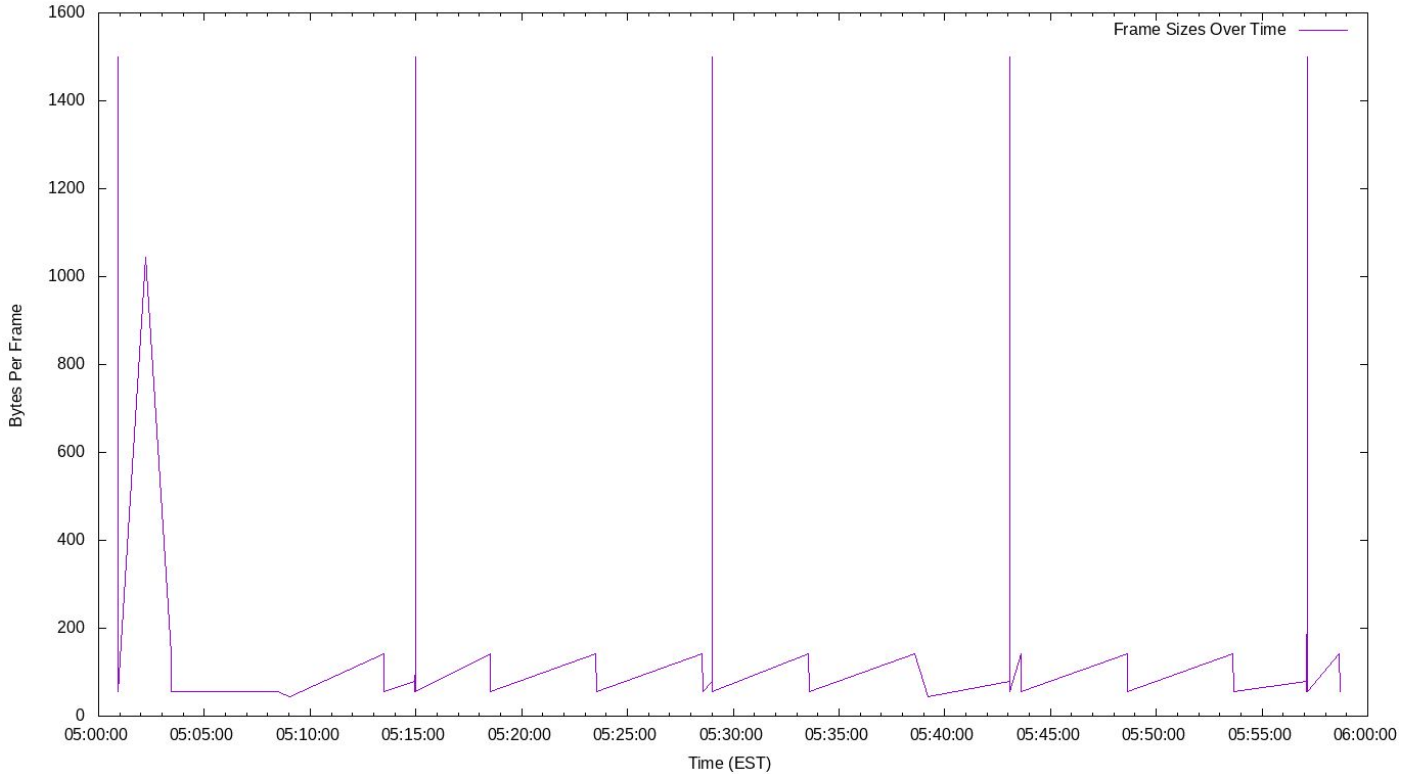
Capturing Network Traffic


Activities
Terminal
Nov 22 17:34
iot-admin
small.bin
Trash
SimplieSafe-DoorbellPro
scapy-radio_passive...
scapy-radio_passive...
howtosniff-ring.txt
howtodecodeR3.txt
output.ub
iot-admin@desktop-1: ~
CH 11][Elapsed: 24 hours 1 min][2019-11-22 17:34][Decloak: 32:23:03:11:75:2C
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
32:23:03:11:75:2C -22 100 799674 1280872 58 11 195 WPA2 CCMP PSK IoT-Lab-AP1
BSSID STATION PWR Rate Lost Frames Probe
32:23:03:11:75:2C 30:45:11:3A:17:ED -30 0e- 6 0 399979
32:23:03:11:75:2C D8:13:99:3B:E5:B6 -30 1e- 1e 0 7453
32:23:03:11:75:2C 98:DA:C4:71:EC:9D -32 0e- 0e 12 712208
32:23:03:11:75:2C 0C:8C:24:7F:34:84 -32 0e- 0e 0 29140
32:23:03:11:75:2C 58:B3:FC:68:A6:E2 -32 0e-24 1390 171097 IoT-Lab-AP1
32:23:03:11:75:2C 0C:8C:24:72:71:9A -30 0e- 1 0 23294
32:23:03:11:75:2C 6C:21:A2:90:19:B0 -36 0e- 0 0 41436
32:23:03:11:75:2C 8C:F7:10:A1:A5:9F -36 1e-24 0 12514
32:23:03:11:75:2C CC:FA:00:A8:37:02 -36 1e- 1 0 303
32:23:03:11:75:2C D8:13:99:3B:E7:FB -38 1e- 1 0 9121
32:23:03:11:75:2C CC:FA:00:A9:60:8D -44 1e- 1 0 337
32:23:03:11:75:2C 24:7D:4D:9C:F2:81 -46 1 - 6e 0 38282
32:23:03:11:75:2C 90:E2:02:30:80:A8 -46 1 - 6e 0 41474
32:23:03:11:75:2C CC:FA:00:A9:61:2D -46 1e- 1 0 319
32:23:03:11:75:2C 30:4A:26:12:14:F1 -50 0e- 0e 2 165540
32:23:03:11:75:2C 54:2B:57:29:92:A9 -52 0e- 0e 2 59363

Ring Doorbell Use Activity



Ring Doorbell Heartbeat Activity

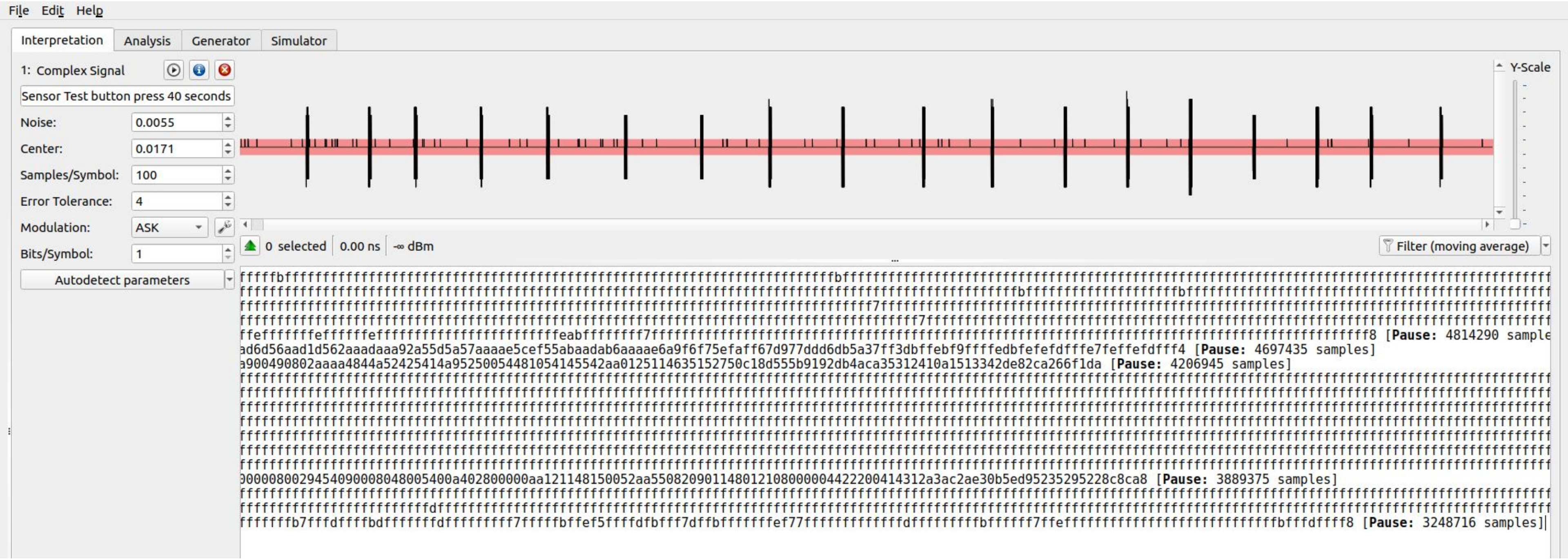


Simplisafe And 433.92

```
        line 0: warning: Skipping data file with no valid points

gnuplot> plot [:][:] 'ss.data' using ($1+(-4*3600)):2 title "Frame Sizes Over Time" with lines
                                                                                          ^
        line 0: x range is invalid
```

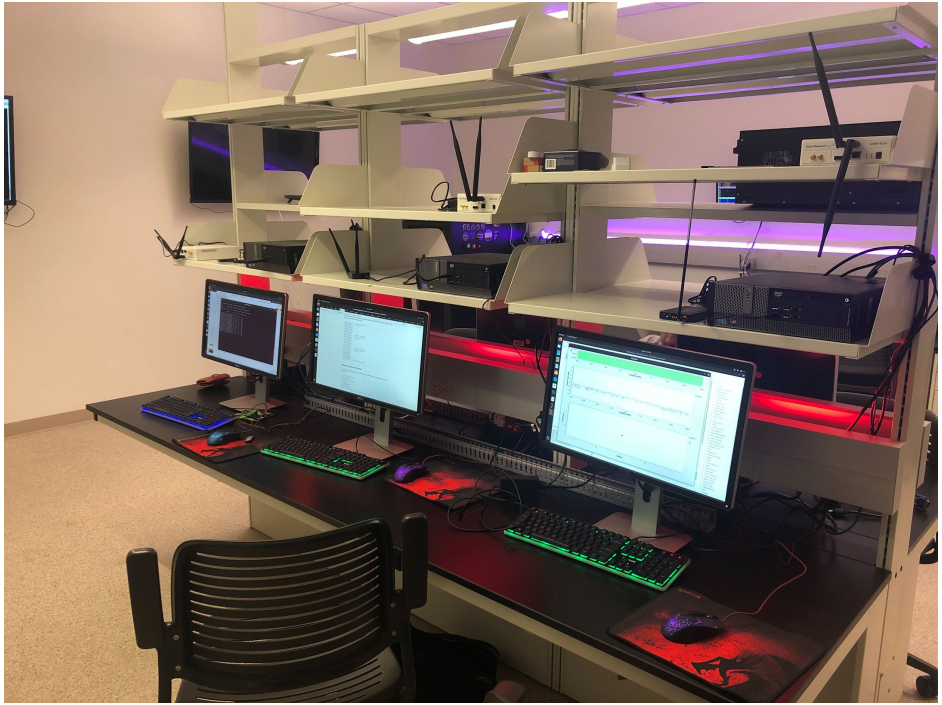
- Currently no heartbeat packet sending
- Only on demand traffic

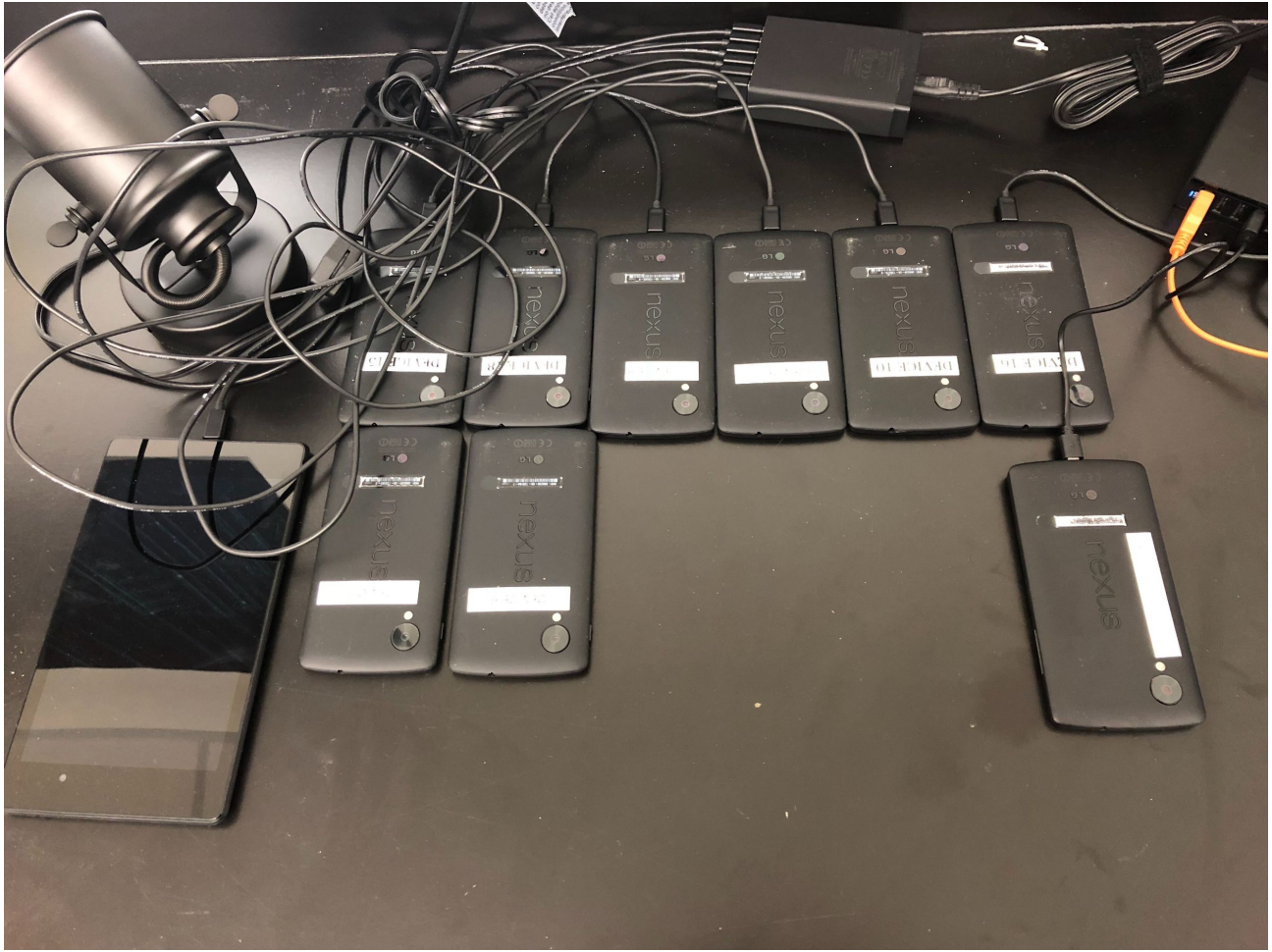

File Edit Help
Interpretation
Analysis
Generator
Simulator
1: Complex Signal
Sensor Test button press 40 seconds
Noise: 0.0055
Center: 0.0171
Samples/Symbol: 100
Error Tolerance: 4
Modulation: ASK
Bits/Symbol: 1
Autodetect parameters
Y-Scale
0 selected
0.00 ns
-∞ dBm
Filter (moving average)
[Pause: 4814290 sample
ad6d56aad1d562aaadaaa92a55d5a57aaaae5cef55abaadab6aaaae6a9f6f75efaff67d977ddd6db5a37ff3dbffebf9ffffedbfefefdfffe7feffefdfff4 [Pause: 4697435 samples]
a900490802aaaa4844a52425414a95250054481054145542aa0125114635152750c18d555b9192db4aca35312410a1513342de82ca266f1da [Pause: 4206945 samples]
0000080029454090008048005400a402800000aa121148150052aa550820901148012108000004422200414312a3ac2ae30b5ed95235295228c8ca8 [Pause: 3889375 samples]
[Pause: 3248716 samples]

IoT Lab is Complete!

New Procedures

- Better storage
- Device Tracking
- Installing New Equipment
- Labeling User Devices




nexus

Standardized Procedures

Product	Account	Notes	PASSWORD
SimpliSafe - Motion Sensor - White	fit.iotlab@gmail.com	Uses 433.92 MHz to base station	
SimpliSafe - Wireless Home Security System - Black	fit.iotlab@gmail.com	Uses 433.92 MHz to base station	
SimpliSafe - SimpliCam- Black	fit.iotlab@gmail.com	2.4 wifi signal	
SimpliSafe - Pro Smart Wi-Fi Video Doorell - Wired - White	fit.iotlab@gmail.com	2.4 wifi signal	
Ring - Spotlight Indoor/Outdoor 1080p Wi-Fi Wireless Security Camera	fit.iotlab@gmail.com		
Ring - Video Doorbell Pro and Chime Pro Bundle - Satin Nickel	fit.iotlab@gmail.com		
Ring - Wi-Fi Smart Video Doorbell - Multi	fit.iotlab@gmail.com		
Ring - Alarm Motion Detector - White	fit.iotlab@gmail.com	-zwave+	
Ring - Alarm Starter Home Security Kit - White	fit.iotlab@gmail.com	-zwave+	
Ring - Motion Detector - White	fit.iotlab@gmail.com	-zwave+	
Google - Nest Secure Alarm System - White	fit.iotlab@gmail.com	wifi, attemped to find packets	
Blink - Wireless Home Security System - White	fit.iotlab@gmail.com	wifi	

Label Data Sets

Tech Stack Used

- Selenium
- Beautifulsoup
- Pandas
- Numpy

FCC- ID’s

- Federal Communication Commission
- Contains useful information on the devices
  - Frequency Range
  - Company Name
  - Device Name

Final DF from Miner

	Device	FCCID	Company	Frequency_Low	Frequency_High
0	SmartThings Tracker	A3LSMV110A	Samsung Electronics IoT Network Device SMV110A...	714.5	700.5
1	SmartThings Motion Sensor	2AF4S-IM6001-MTP01	SAM JIN	2470.00000000	2405.00000000
2	Ring Keypad	2AB2Q-BHAKP001	LEEDARSON LIGHTING	916.00000000	908.40000000
3	SmartThings Water Leak Sensor	2AF4S-IM6001-WLP01	SAM JIN	2470.00000000	2405.00000000
4	SmartThings Button	2AF4S-IM6001-BTP01	SAM JIN	2470.00000000	2405.00000000
5	SmartThings Multipurpose Sensor	2AF4S-IM6001-MPP01	SAM JIN	2470.00000000	2405.00000000
6	Ring Contact Sensor	XQC-BHADW001	Ecolink Intelligent Technology	916.00000000	908.42000000
7	SimpliSafe Glassbreak Sensor	U9K-GB3000	SimpliSafe	433.92000000	433.92000000
8	SmartThings Arrival Sensor	2AF4S-STS-PRS-250	SAM JIN	2470.00000000	2405.00000000
9	idfk	U9K-ES3	SimpliSafe	433.92000000	433.92000000
10	August Connect	2AB6UACR1	August Home August Connect ACR1 FCC ID 2AB6UACR1	2480	2402
11	SimpliSafe Motion Detector	U9K-MS3000	SimpliSafe	433.92000000	433.92000000
12	Ring Motion Detector	XQC-BHAPIR001	Ecolink Intelligent Technology	916.00000000	908.40000000
13	Ring Doorbell	2AEUPBHARG031	Ring	2462.00000000	2412.00000000
14	Geeni Doorbell	Y2EAH4033BW	SHENZHEN APEXIS ELECTRONIC	2462.00000000	2412.00000000
15	SimpliSafe Doorbell	U9K-DB3000	SimpliSafe	2480.00000000	2402.00000000
16	NightOwl Doorbell	2APRB-WDB-20-V2-JUN	Guangzhou Juan Intelligent Tech Joint Stock	2462.00000000	2412.00000000
17	Nest Doorbell	ZQANC51	Nest Labs Nest Hello NC51 FCC ID ZQANC51	2480	2402
18	Blink Camera	2AF77-BCM00100U	Immedia Semiconductor Blink Camera BCM00100U F...	927.20000000	902.30000000
19	Geeni Camera	2AG7CMINI7S	Hangzhou Meari Technology IP Camera MINI7S FCC...	2462.00000000	2412.00000000
20	Geeni Camera 2	TW5T5886G	Shenzhen Gospell Smarthome Electronic HD WiFi ...	2462.00000000	2412.00000000
21	Kasa Camera	TE7KC100	TP-Link Technologies Kasa Smart Spot KC100 FCC...	2462.00000000	2412.00000000
22	Arlo Camera	2APLE18200349	Arlo Technologies	2462.00000000	2412.00000000
23	SimpliSafe Camera	U9K-CM1000	SimpliSafe	2462.00000000	2412.00000000
24	Ring Spotlight	2AEUPBHARC001	Ring Spotlight Cam Wired BHARC001 FCC ID 2AEUP...	2462.00000000	2412.00000000

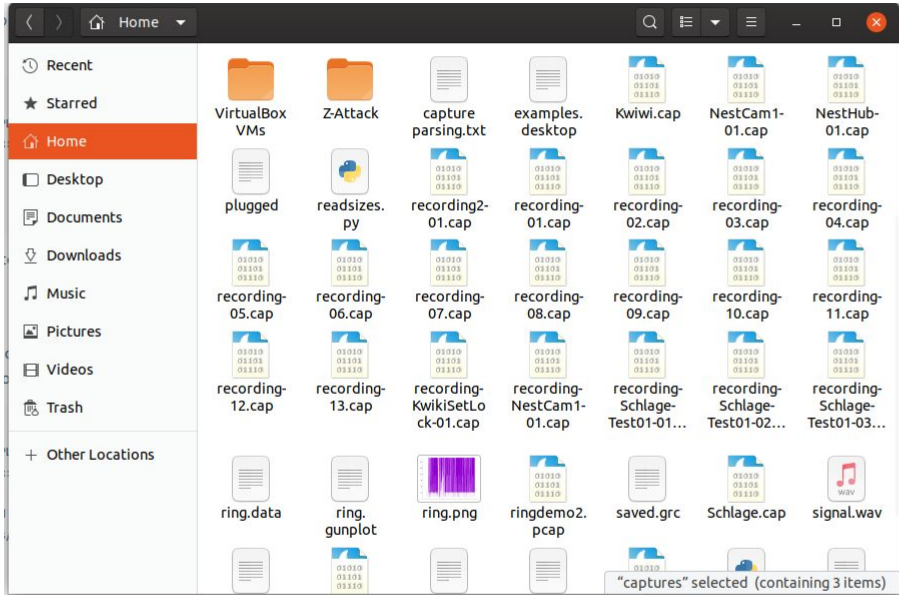
Why this is important

This is the beginning of the Dataframe we will use to develop a classifier to detect exactly what kind of devices are in the network.

- Other features to be added
  - Traffic type
  - Mac address (to train and test as we will know these)
  - Packet size
  - Packet information

Data Gathered

Example of the . cap files we collected that show the network traffic, both for individual devices and for all over long periods of time.



Beyond our Milestones

Challenges

- Minor setbacks with device setup
  - Needing to buy third party software
  - needing valid phone number to sign up.
- Gathering Federal Communications Commission (FCC) information on devices for database
  - Built a python script to mine data from the FCC website.
- Parsing certain datasets
  - Z-Wave Plus has proved to be more difficult to parse.
    - 6/20 devices use Z-Wave Plus

Going Forward

- Collect and parse more data on 802.11 (fringe cases)
- Analyze Z-Wave data
- Further Decode 433.92 signals