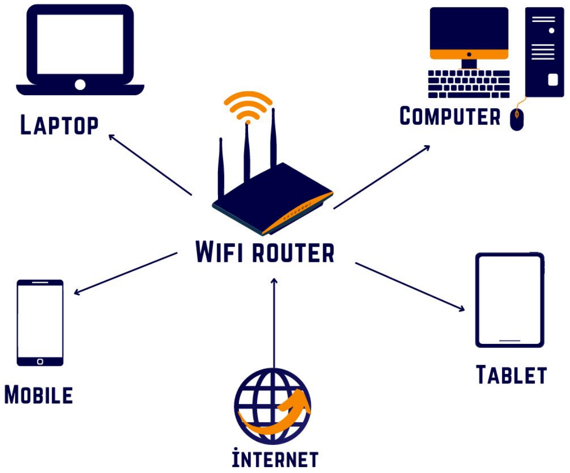
NERVE:

Network Event Realtime Visualization Engine for Security Monitoring

Kasra Lekan, Neha Bagalkot, Sneha Iyer, Nicki Choquette

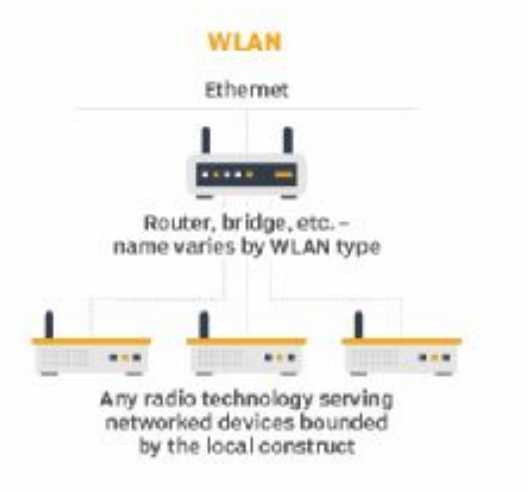
Introduction to WLAN

- A wireless local-area network (WLAN) is a group of colocated computers or other devices that form a network based on radio transmissions rather than wired connections.
- A Wi-Fi network is a type of WLAN



How does WLAN work?

- Information transmitted over radio waves.
- Data is sent in packets.
- The packets contain layers with info to enable routing to intended locations

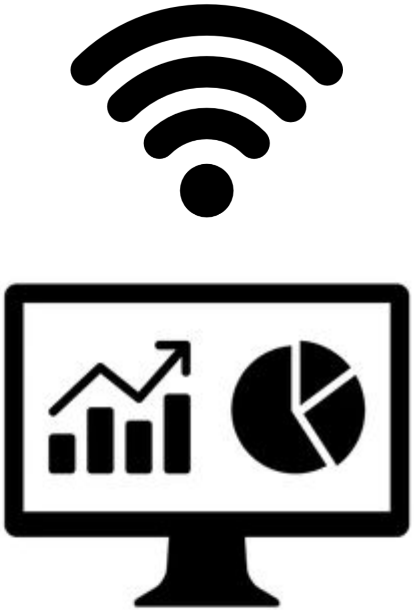

WLAN
Ethernet
Router, bridge, etc. – name varies by WLAN type
Any radio technology serving networked devices bounded by the local construct

Is a WLAN secure?

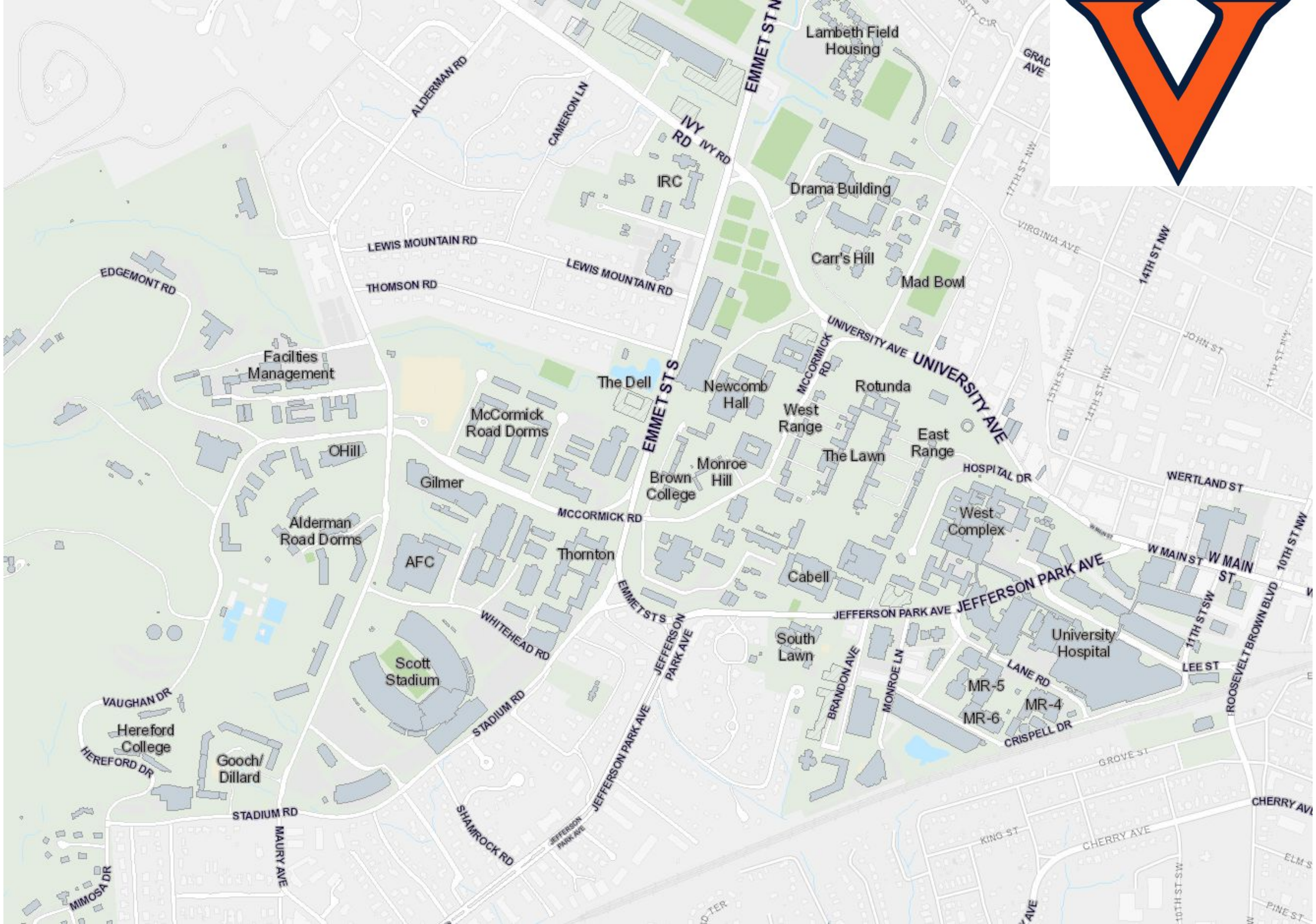
- A WLAN is more vulnerable to being breached than a physical network.
- To access a WLAN, a bad actor must simply be within range of the network.

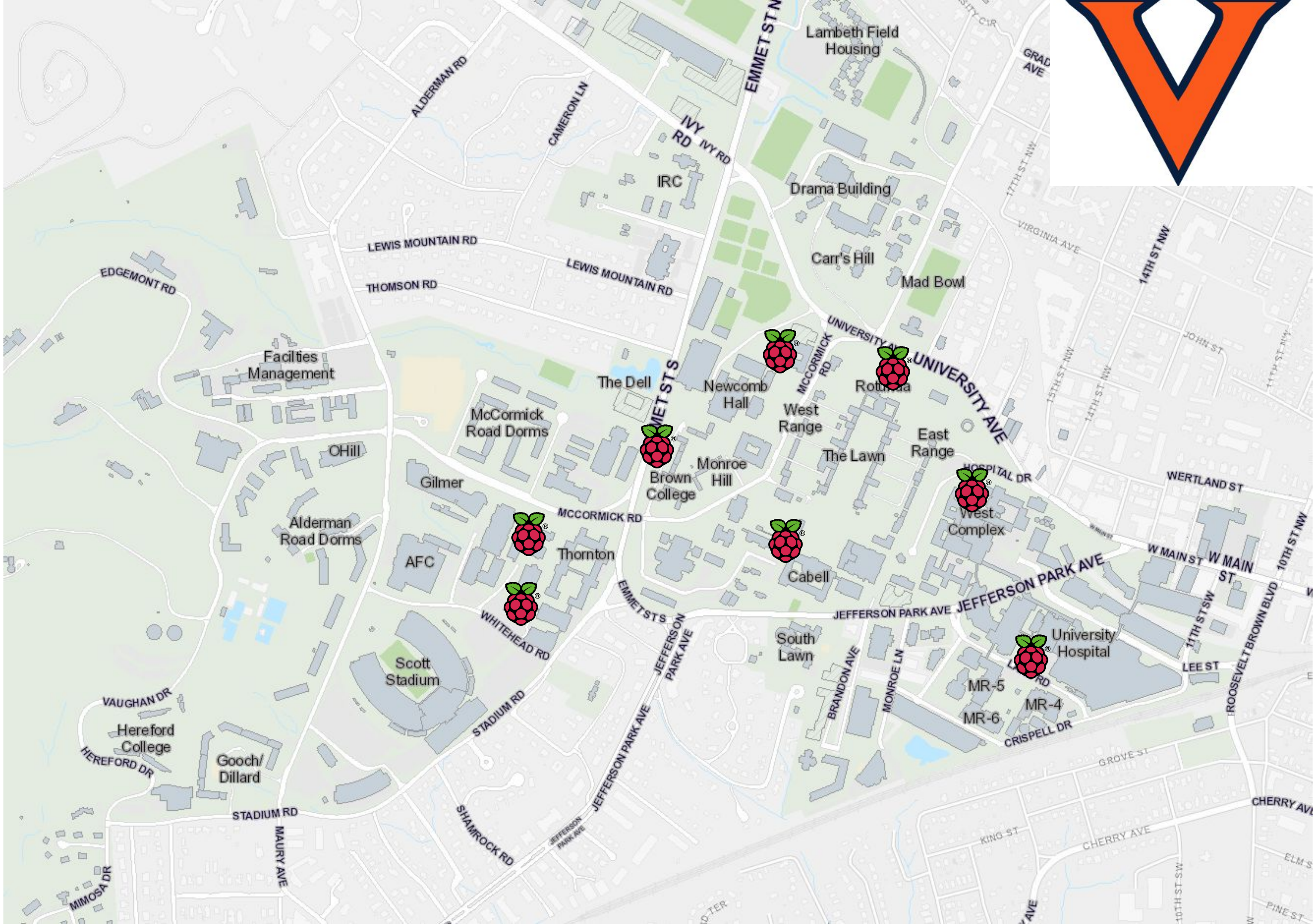
Our project

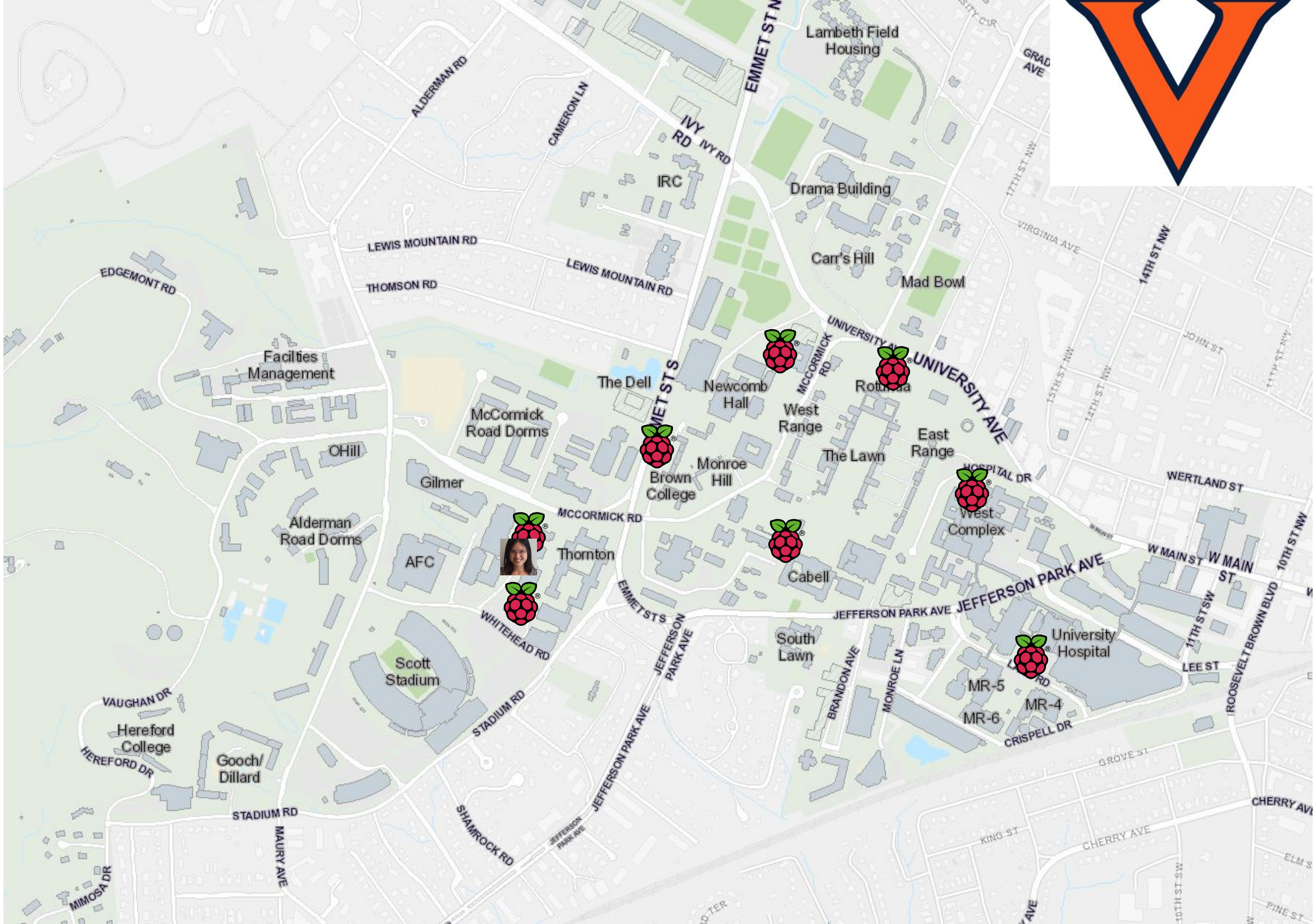
- We worked on designing a real-time dashboard tool to capture packet data on wireless networks and analyze it.
- Our tool is a type of wireless sniffer solution, which we built to capture wireless network traffic and analyze it to generate insights into what's going on in a network at any given time.

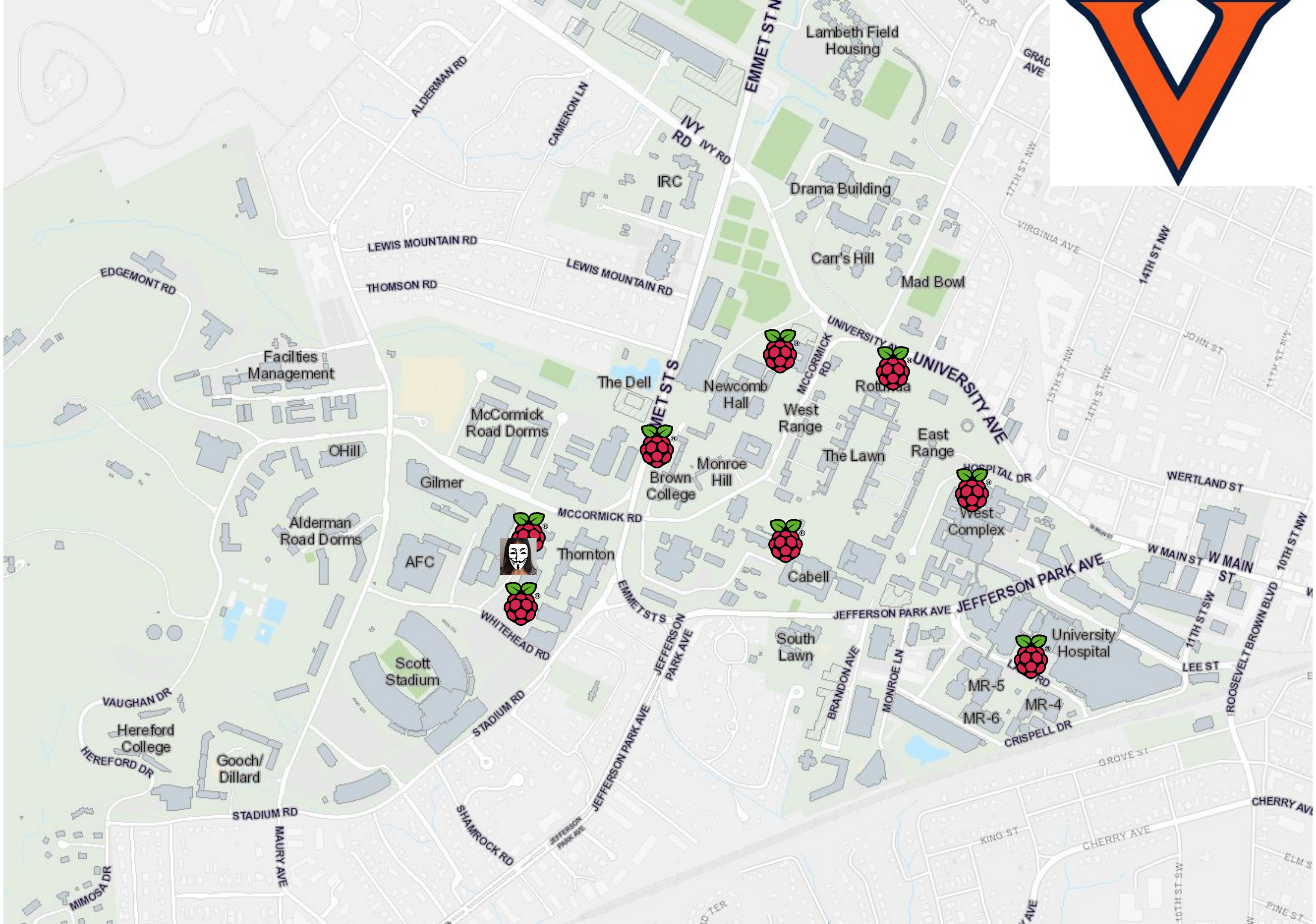


Threat Model

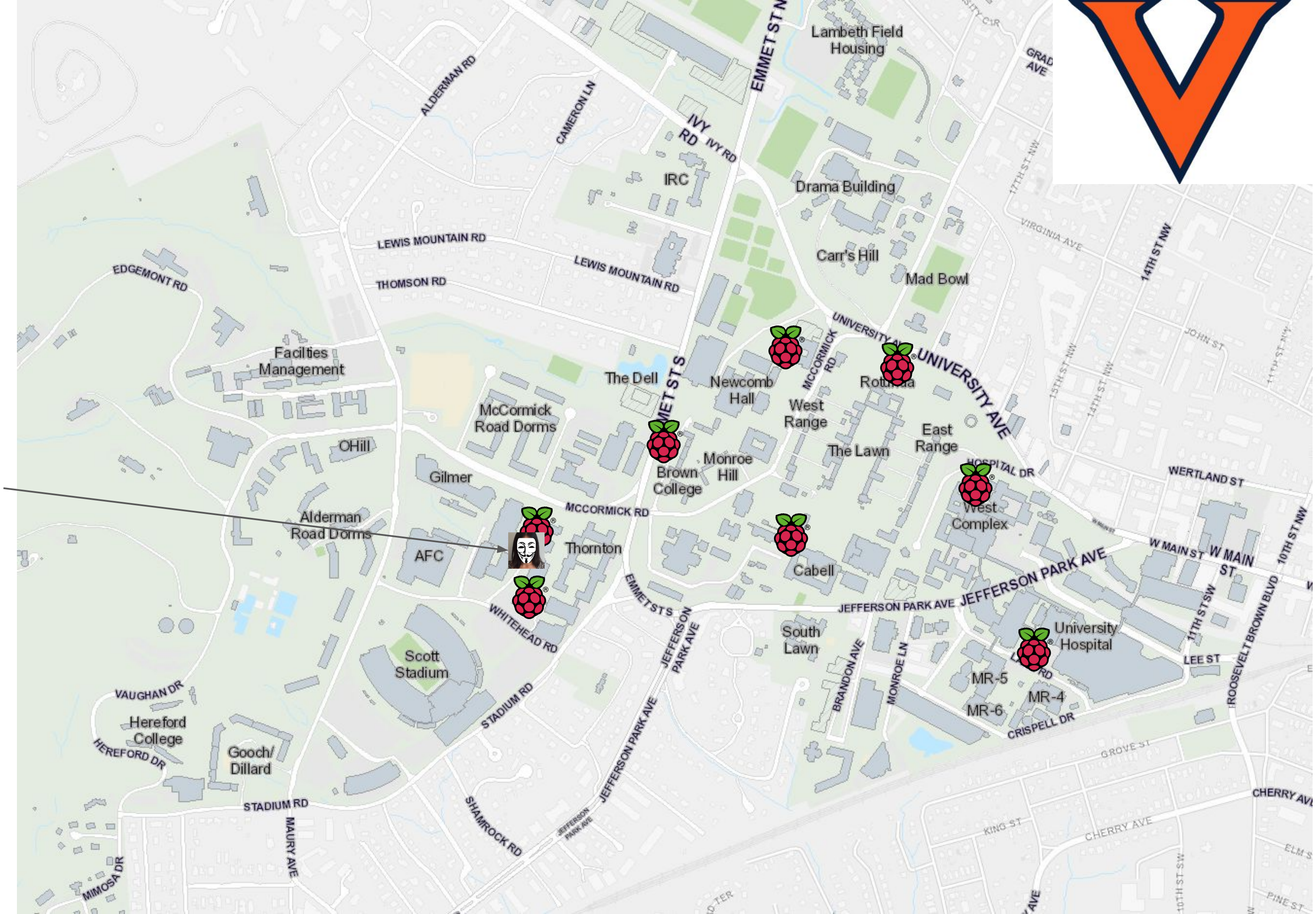

Lambeth Field Housing
EMMET ST N
GRADY AVE
ALDERMAN RD
CAMERON LN
IVY RD
IVY RD
IRC
Drama Building
17TH ST NW
VIRGINIA AVE
14TH ST NW
LEWIS MOUNTAIN RD
LEWIS MOUNTAIN RD
Carr's Hill
Mad Bowl
EDGEMONT RD
THOMSON RD
UNIVERSITY AVE
UNIVERSITY AVE
JOHN ST
15TH ST NW
14TH ST NW
11TH ST NW
MCCORMICK RD
Facilties Management
The Dell
EMMET ST S
Newcomb Hall
Rotunda
West Range
McCormick Road Dorms
OHill
East Range
The Lawn
Monroe Hill
Brown College
Gilmer
HOSPITAL DR
WERTLAND ST
MCCORMICK RD
West Complex
Alderman Road Dorms
AFC
Thornton
W MAIN ST
W MAIN ST
W MAIN ST
10TH ST NW
Cabell
JEFFERSON PARK AVE
EMMET ST S
JEFFERSON PARK AVE
JEFFERSON PARK AVE
WHITEHEAD RD
South Lawn
University Hospital
11TH ST SW
ROOSEVELT BROWN BLVD
LEE ST
Scott Stadium
BRANDON AVE
MONROE LN
LANE RD
MR-5
MR-4
MR-6
CRISPELL DR
VAUGHAN DR
STADIUM RD
JEFFERSON PARK AVE
Hereford College
HEREFORD DR
Gooch/ Dillard
GROVE ST
STADIUM RD
MAURY AVE
SHAMROCK RD
JEFFERSON PARK AVE
CHERRY AVE
KING ST
CHERRY AVE
ELM ST
MIMOSA DR
10TH ST SW
PINE ST


Lambeth Field Housing
EMMET ST N
GRADY AVE
ALDERMAN RD
CAMERON LN
IVY RD
IVY RD
IRC
Drama Building
17TH ST NW
VIRGINIA AVE
14TH ST NW
LEWIS MOUNTAIN RD
LEWIS MOUNTAIN RD
THOMSON RD
EDGEMONT RD
Carr's Hill
Mad Bowl
UNIVERSITY AVE
UNIVERSITY AVE
JOHN ST
Facilties Management
The Dell
EMMET ST S
Newcomb Hall
MCCORMICK RD
Rotunda
15TH ST NW
14TH ST NW
West Range
McCormick Road Dorms
East Range
The Lawn
OHill
Monroe Hill
Brown College
HOSPITAL DR
WERTLAND ST
Gilmer
MCCORMICK RD
West Complex
Alderman Road Dorms
Thornton
AFC
Cabell
W MAIN ST
W MAIN ST
10TH ST NW
JEFFERSON PARK AVE
JEFFERSON PARK AVE
EMMET ST S
WHITEHEAD RD
JEFFERSON PARK AVE
South Lawn
University Hospital
11TH ST SW
ROOSEVELT BROWN BLVD
LEE ST
Scott Stadium
BRANDON AVE
MONROE LN
MR-5
MR-4
MR-6
CRISPELL DR
VAUGHAN DR
STADIUM RD
Hereford College
HEREFORD DR
Gooch/ Dillard
GROVE ST
CHERRY AVE
STADIUM RD
MAURY AVE
SHAMROCK RD
JEFFERSON PARK AVE
JEFFERSON PARK AVE
KING ST
CHERRY AVE
MIMOSA DR
ELM ST
PINE ST
10TH ST SW


Lambeth Field Housing
EMMET ST N
GRAD AVE
ALDERMAN RD
CAMERON LN
IVY RD
IVY RD
IRC
Drama Building
17TH ST NW
VIRGINIA AVE
14TH ST NW
LEWIS MOUNTAIN RD
LEWIS MOUNTAIN RD
THOMSON RD
EDGEMONT RD
Carr's Hill
Mad Bowl
UNIVERSITY AVE
UNIVERSITY AVE
JOHN ST
15TH ST NW
14TH ST NW
Facilties Management
The Dell
EMMET ST S
Newcomb Hall
MCCORMICK RD
Rotunda
West Range
East Range
McCormick Road Dorms
OHill
Monroe Hill
The Lawn
Brown College
Gilmer
HOSPITAL DR
WERTLAND ST
MCCORMICK RD
West Complex
Alderman Road Dorms
Thornton
AFC
Cabell
W MAIN ST
W MAIN ST
10TH ST NW
JEFFERSON PARK AVE
JEFFERSON PARK AVE
EMMET ST S
11TH ST SW
ROOSEVELT BROWN BLVD
WHITEHEAD RD
JEFFERSON PARK AVE
South Lawn
University Hospital
LEE ST
Scott Stadium
BRANDON AVE
MONROE LN
MR-5
MR-4
MR-6
CRISPELL DR
VAUGHAN DR
STADIUM RD
Hereford College
HEREFORD DR
Gooch/ Dillard
GROVE ST
STADIUM RD
JEFFERSON PARK AVE
CHERRY AVE
SHAMROCK RD
MAURY AVE
KING ST
CHERRY AVE
JEFFERSON PARK AVE
MIMOSA DR

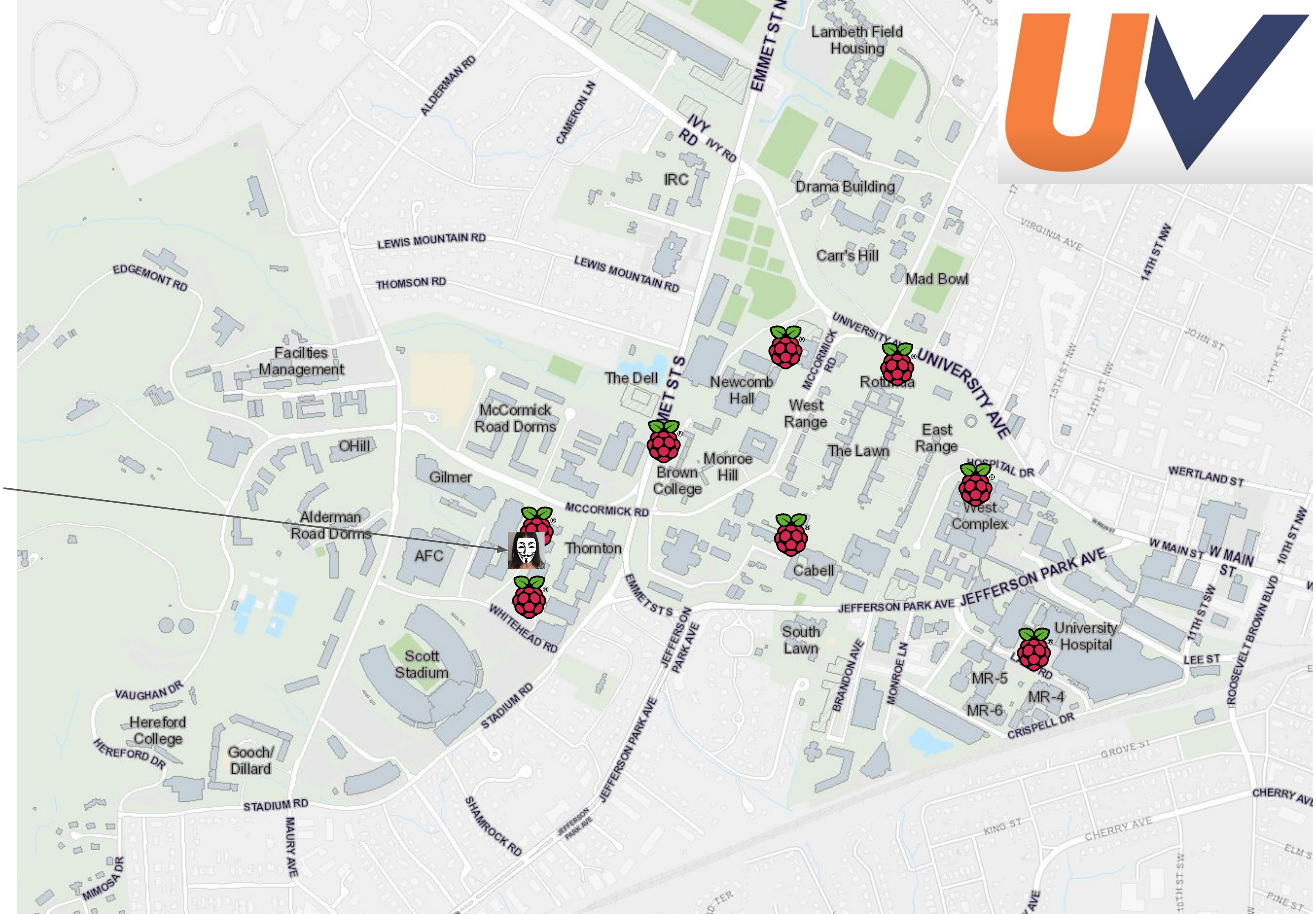


Lambeth Field
Housing
EMMET ST N
IVY RD
IVY RD
ALDERMAN RD
CAMERON LN
IRC
Drama Building
Carr's Hill
Mad Bowl
VIRGINIA AVE
GRAD AVE
17TH ST NW
14TH ST NW
LEWIS MOUNTAIN RD
LEWIS MOUNTAIN RD
THOMSON RD
EDGEMONT RD
Facilties
Management
UNIVERSITY AVE
UNIVERSITY AVE
MCCORMICK RD
The Dell
EMMET ST S
Newcomb
Hall
West
Range
Rotunda
JOHN ST
15TH ST NW
14TH ST NW
McCormick
Road Dorms
OHill
Gilmer
Brown
College
Monroe
Hill
The Lawn
East
Range
HOSPITAL DR
WERTLAND ST
West
Complex
MCCORMICK RD
Alderman
Road Dorms
AFC
Thornton
Cabell
W MAIN ST
W MAIN
ST
JEFFERSON PARK AVE
JEFFERSON PARK AVE
10TH ST NW
EMMET ST S
WHITEHEAD RD
JEFFERSON PARK AVE
South
Lawn
BRANDON AVE
MONROE LN
University
Hospital
LEE ST
11TH ST SW
ROOSEVELT BROWN BLVD
Scott
Stadium
MR-5
MR-4
MR-6
CRISPELL DR
STADIUM RD
VAUGHAN DR
Hereford
College
HEREFORD DR
Gooch/
Dillard
GROVE ST
CHERRY AVE
STADIUM RD
MAURY AVE
SHAMROCK RD
JEFFERSON PARK AVE
JEFFERSON PARK AVE
KING ST
CHERRY AVE
ELM ST
MIMOSA DR
PINE ST



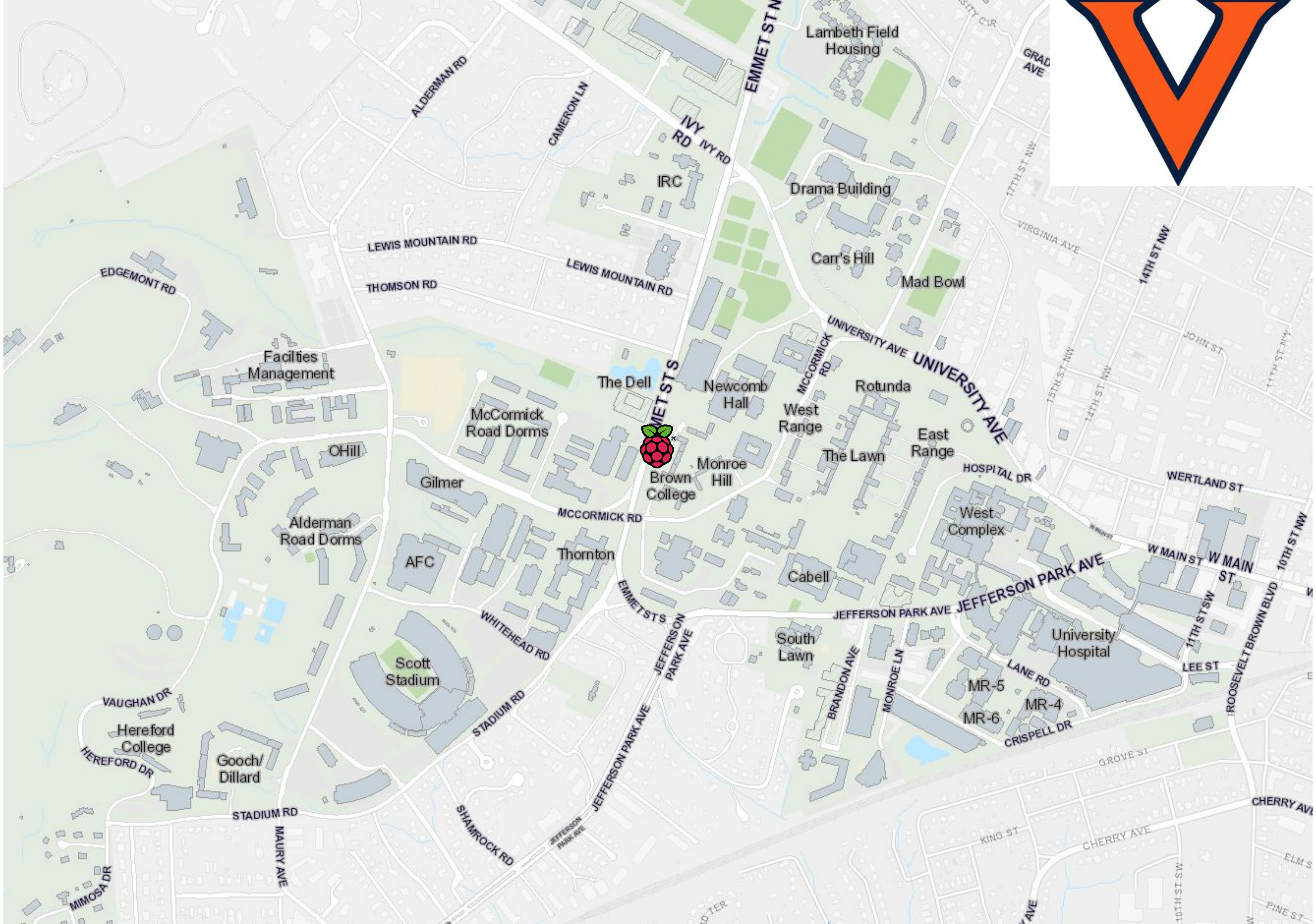
Identify hacker

Identify hacker



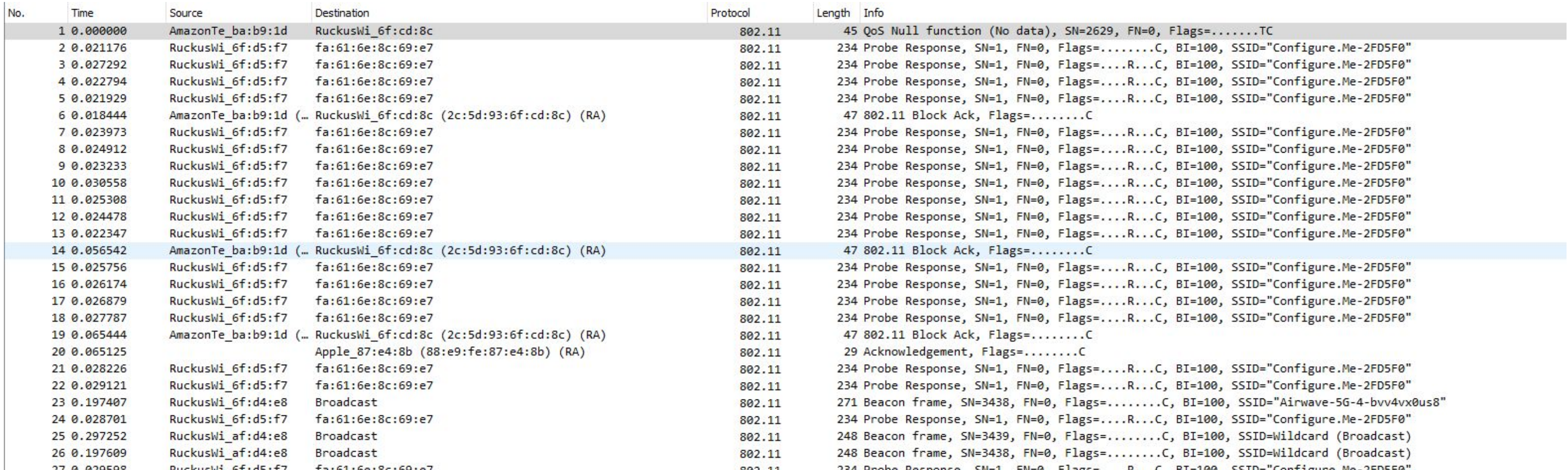
Validating Our Approach

A Small Scale Experiment


Lambeth Field Housing
EMMET ST N
GRADY AVE
ALDERMAN RD
CAMERON LN
IVY RD
IVY RD
IRC
Drama Building
17TH ST NW
VIRGINIA AVE
LEWIS MOUNTAIN RD
LEWIS MOUNTAIN RD
THOMSON RD
EDGEMONT RD
Carr's Hill
Mad Bowl
14TH ST NW
UNIVERSITY AVE
UNIVERSITY AVE
JOHN ST
MCCORMICK RD
Facilties Management
The Dell
EMMET ST S
Newcomb Hall
Rotunda
15TH ST NW
14TH ST NW
11TH ST NW
McCormick Road Dorms
West Range
OHill
East Range
The Lawn
Monroe Hill
Brown College
Gilmer
HOSPITAL DR
WERTLAND ST
MCCORMICK RD
Alderman Road Dorms
West Complex
Thornton
AFC
Cabell
W MAIN ST
W MAIN ST
W MAIN ST
10TH ST NW
JEFFERSON PARK AVE
JEFFERSON PARK AVE
EMMET ST S
JEFFERSON PARK AVE
WHITEHEAD RD
South Lawn
University Hospital
11TH ST SW
ROOSEVELT BROWN BLVD
Scott Stadium
BRANDON AVE
MONROE LN
LANE RD
LEE ST
MR-5
MR-4
MR-6
STADIUM RD
VAUGHAN DR
CRISPELL DR
Hereford College
JEFFERSON PARK AVE
GROVE ST
HEREFORD DR
Gooch/ Dillard
CHERRY AVE
STADIUM RD
KING ST
CHERRY AVE
MAURY AVE
SHAMROCK RD
JEFFERSON PARK AVE
ELM ST
MIMOSA DR
PINE ST
10TH ST SW

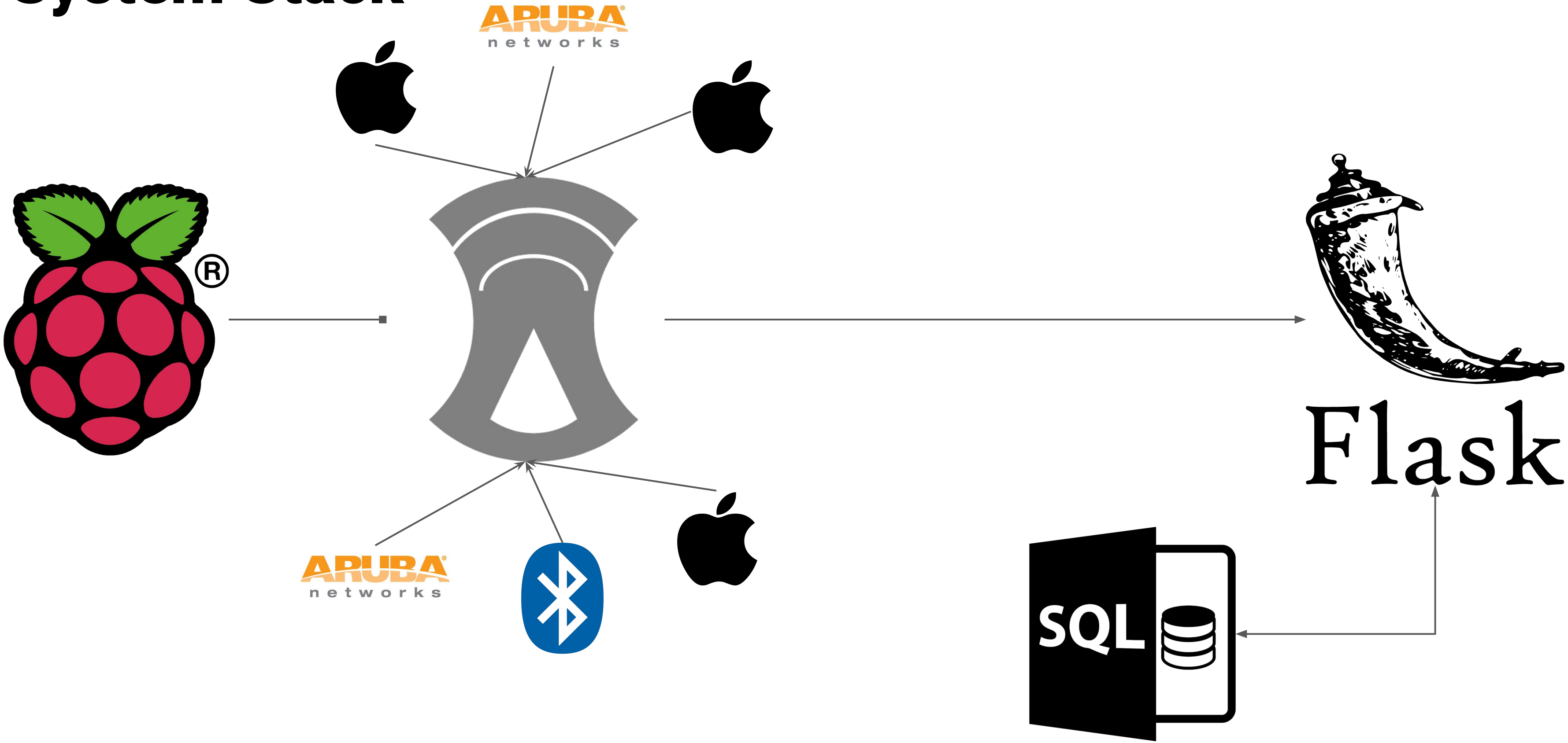
What is Wifi Sniffing?

- WiFi sniffing = intercepting and decoding wireless network traffic
- Capturing data packets (802.11 protocol) → analyze data being transmitted
  - Glean information about devices in topography of the network

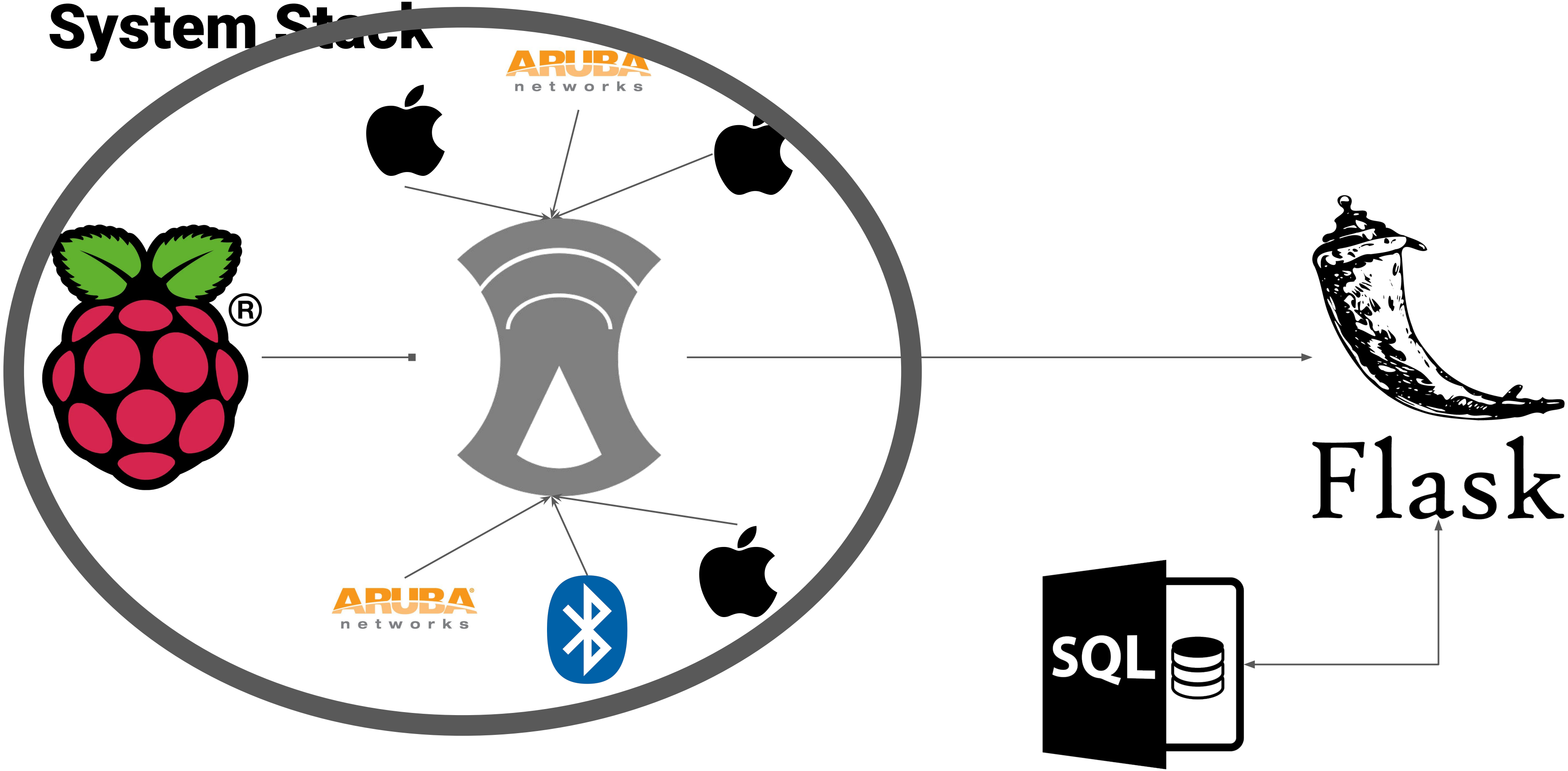


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmazonTe_ba:b9:1d	RuckusWi_6f:cd:8c	802.11	45	QoS Null function (No data), SN=2629, FN=0, Flags=.......TC
2	0.021176	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=........C, BI=100, SSID="Configure.Me-2FD5F0"
3	0.027292	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
4	0.022794	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
5	0.021929	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
6	0.018444	AmazonTe_ba:b9:1d (…	RuckusWi_6f:cd:8c (2c:5d:93:6f:cd:8c) (RA)	802.11	47	802.11 Block Ack, Flags=........C
7	0.023973	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
8	0.024912	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
9	0.023233	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
10	0.030558	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
11	0.025308	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
12	0.024478	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
13	0.022347	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
14	0.056542	AmazonTe_ba:b9:1d (…	RuckusWi_6f:cd:8c (2c:5d:93:6f:cd:8c) (RA)	802.11	47	802.11 Block Ack, Flags=........C
15	0.025756	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
16	0.026174	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
17	0.026879	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
18	0.027787	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
19	0.065444	AmazonTe_ba:b9:1d (…	RuckusWi_6f:cd:8c (2c:5d:93:6f:cd:8c) (RA)	802.11	47	802.11 Block Ack, Flags=........C
20	0.065125		Apple_87:e4:8b (88:e9:fe:87:e4:8b) (RA)	802.11	29	Acknowledgement, Flags=........C
21	0.028226	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
22	0.029121	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
23	0.197407	RuckusWi_6f:d4:e8	Broadcast	802.11	271	Beacon frame, SN=3438, FN=0, Flags=........C, BI=100, SSID="Airwave-5G-4-bvv4vx0us8"
24	0.028701	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"
25	0.297252	RuckusWi_af:d4:e8	Broadcast	802.11	248	Beacon frame, SN=3439, FN=0, Flags=........C, BI=100, SSID=Wildcard (Broadcast)
26	0.197609	RuckusWi_af:d4:e8	Broadcast	802.11	248	Beacon frame, SN=3438, FN=0, Flags=........C, BI=100, SSID=Wildcard (Broadcast)
27	0.029598	RuckusWi_6f:d5:f7	fa:61:6e:8c:69:e7	802.11	234	Probe Response, SN=1, FN=0, Flags=....R...C, BI=100, SSID="Configure.Me-2FD5F0"

System Stack



System Stack



Setting Up Wifi Sniffing

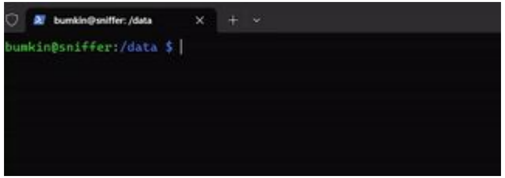
1. Acquiring a WLAN card that supports Monitor Mode

Setting Up Wifi Sniffing

1. Acquiring a WLAN card that supports Monitor Mode

2. Headless Raspberry Pi Setup with Linux

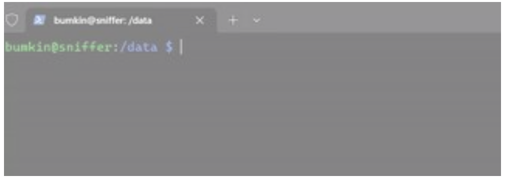
    a. Debugging (Firewall, DNS)



```
bumkin@sniffer:/data $ 
```

Setting Up Wifi Sniffing

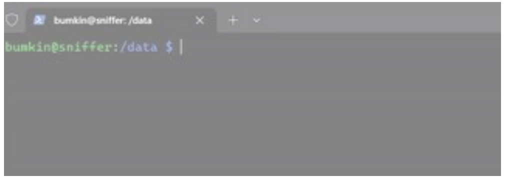
1. Acquiring a WLAN card that supports Monitor Mode
2. Headless Raspberry Pi Setup with Linux
   a. Debugging (Firewall, DNS)
3. Install Kismet



```
bumkin@sniffer:/data $ |
```

Setting Up Wifi Sniffing

1. Acquiring a WLAN card that supports Monitor Mode
2. Headless Raspberry Pi Setup with Linux
   a. Debugging (Firewall, DNS)
3. Install Kismet
4. Port Forwarding

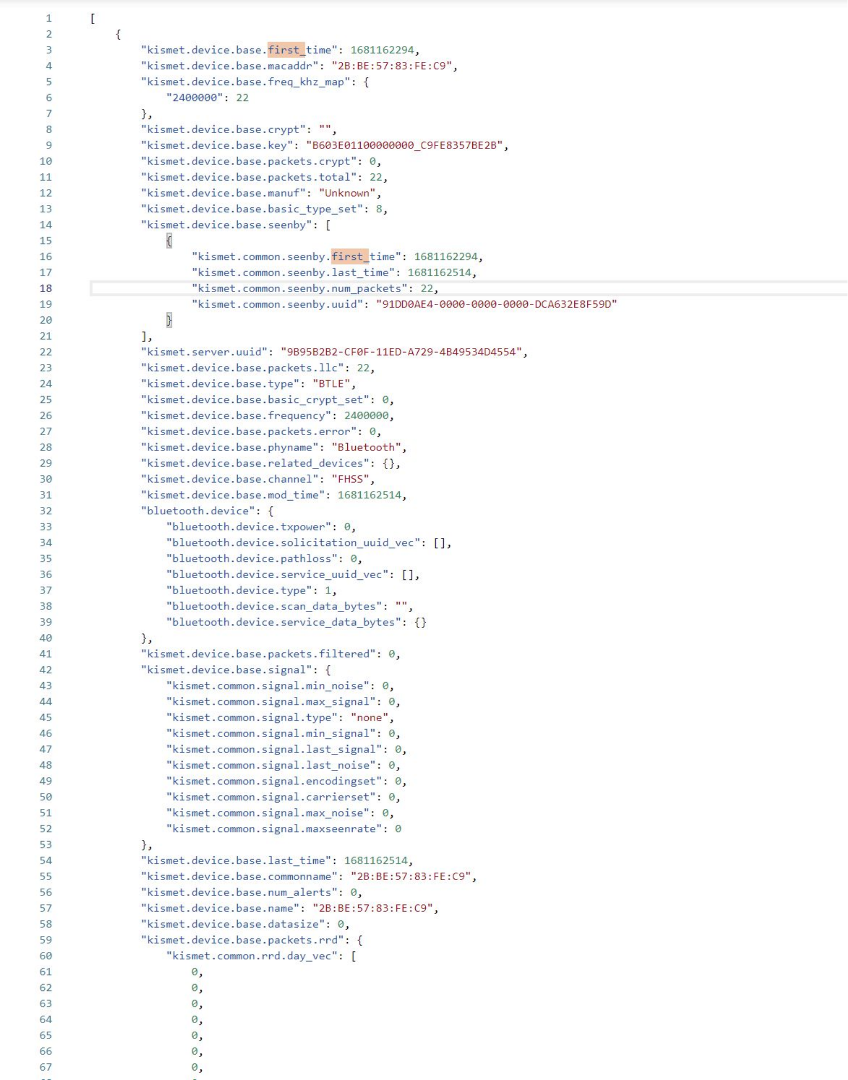


```
bumkin@sniffer:/data $ |
```

Data Analysis

Data Retrieval

- Endpoints:
    - /devices.json
    - /channels.json
    - /ssids.json
    - /tracked_fields.html

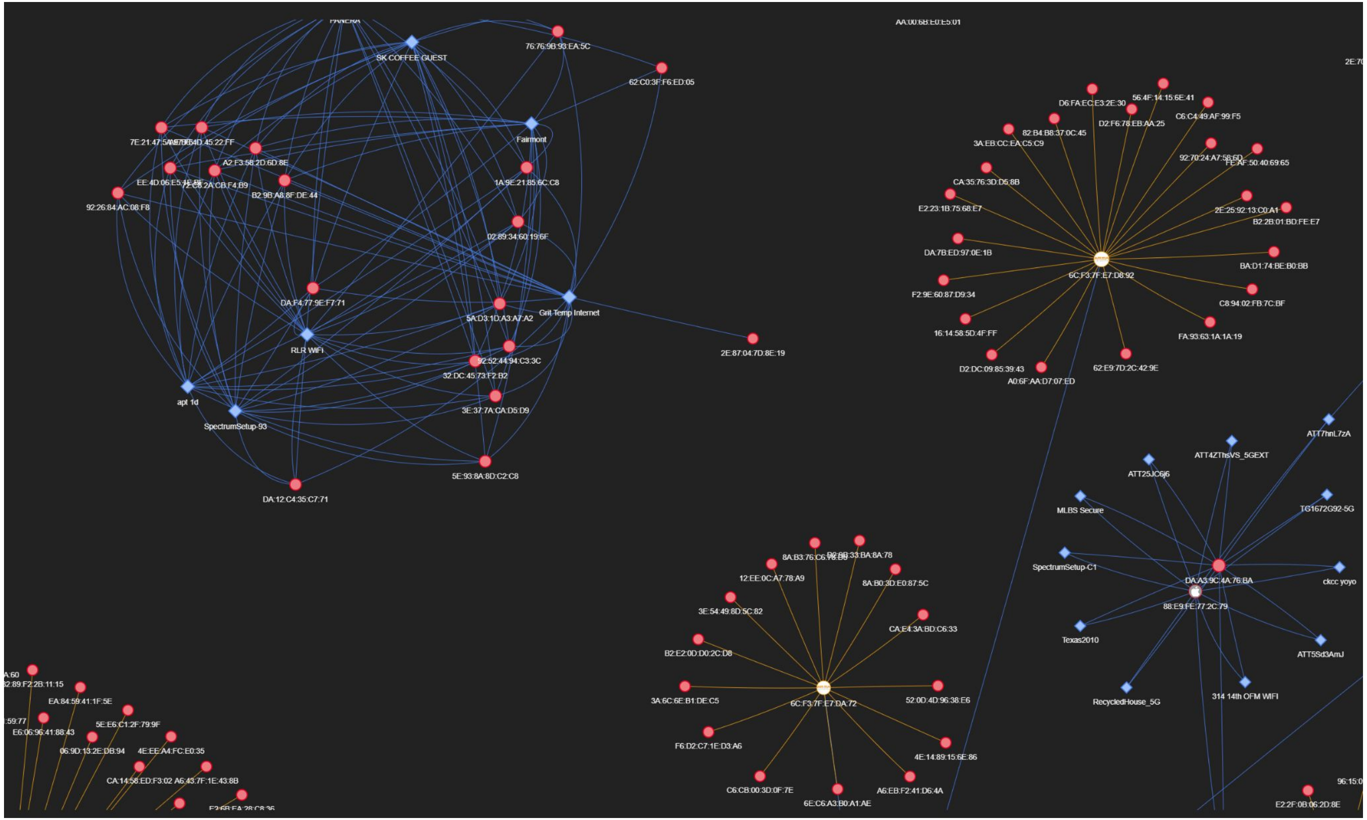


```
[
    {
        "kismet.device.base.first_time": 1681162294,
        "kismet.device.base.macaddr": "2B:BE:57:83:FE:C9",
        "kismet.device.base.freq_khz_map": {
            "2400000": 22
        },
        "kismet.device.base.crypt": "",
        "kismet.device.base.key": "B603E01100000000_C9FE8357BE2B",
        "kismet.device.base.packets.crypt": 0,
        "kismet.device.base.packets.total": 22,
        "kismet.device.base.manuf": "Unknown",
        "kismet.device.base.basic_type_set": 8,
        "kismet.device.base.seenby": [
            {
                "kismet.common.seenby.first_time": 1681162294,
                "kismet.common.seenby.last_time": 1681162514,
                "kismet.common.seenby.num_packets": 22,
                "kismet.common.seenby.uuid": "91DD0AE4-0000-0000-0000-DCA632E8F59D"
            }
        ],
        "kismet.server.uuid": "9B95B2B2-CF0F-11ED-A729-4B49534D4554",
        "kismet.device.base.packets.llc": 22,
        "kismet.device.base.type": "BTLE",
        "kismet.device.base.basic_crypt_set": 0,
        "kismet.device.base.frequency": 2400000,
        "kismet.device.base.packets.error": 0,
        "kismet.device.base.phyname": "Bluetooth",
        "kismet.device.base.related_devices": {},
        "kismet.device.base.channel": "FHSS",
        "kismet.device.base.mod_time": 1681162514,
        "bluetooth.device": {
            "bluetooth.device.txpower": 0,
            "bluetooth.device.solicitation_uuid_vec": [],
            "bluetooth.device.pathloss": 0,
            "bluetooth.device.service_uuid_vec": [],
            "bluetooth.device.type": 1,
            "bluetooth.device.scan_data_bytes": "",
            "bluetooth.device.service_data_bytes": {}
        },
        "kismet.device.base.packets.filtered": 0,
        "kismet.device.base.signal": {
            "kismet.common.signal.min_noise": 0,
            "kismet.common.signal.max_signal": 0,
            "kismet.common.signal.type": "none",
            "kismet.common.signal.min_signal": 0,
            "kismet.common.signal.last_signal": 0,
            "kismet.common.signal.last_noise": 0,
            "kismet.common.signal.encodingset": 0,
            "kismet.common.signal.carrierset": 0,
            "kismet.common.signal.max_noise": 0,
            "kismet.common.signal.maxseenrate": 0
        },
        "kismet.device.base.last_time": 1681162514,
        "kismet.device.base.commonname": "2B:BE:57:83:FE:C9",
        "kismet.device.base.num_alerts": 0,
        "kismet.device.base.name": "2B:BE:57:83:FE:C9",
        "kismet.device.base.datasize": 0,
        "kismet.device.base.packets.rrd": {
            "kismet.common.rrd.day_vec": [
                0,
                0,
                0,
                0,
                0,
                0,
                0,
```

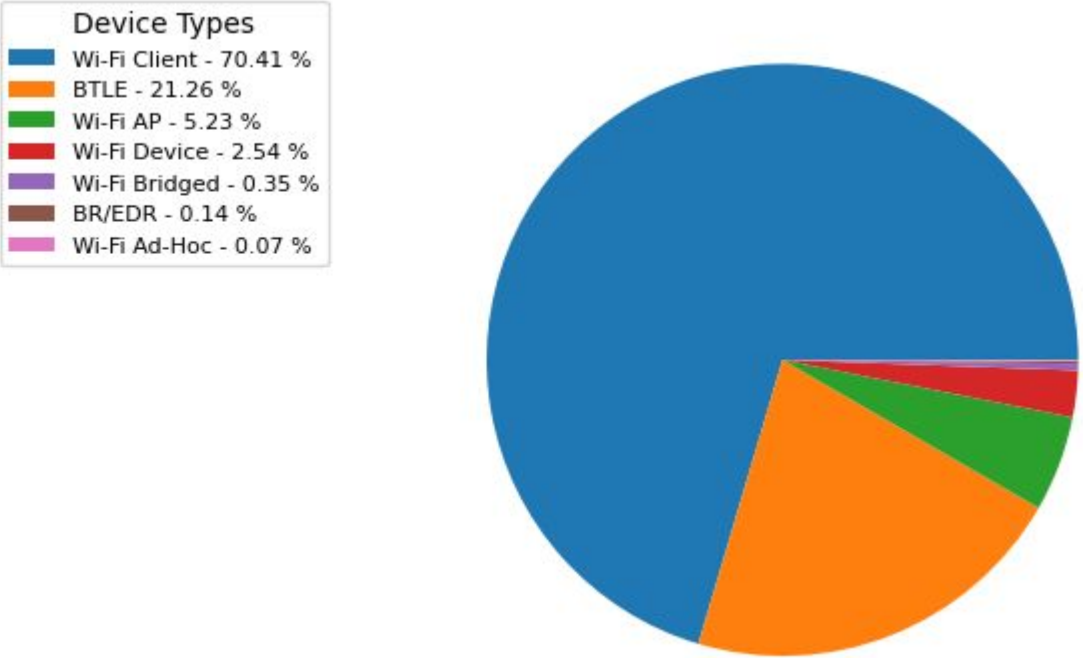
Data Processing

- Jupyter Notebooks
- Pandas dataframes
- Matplotlib
- Pyviz

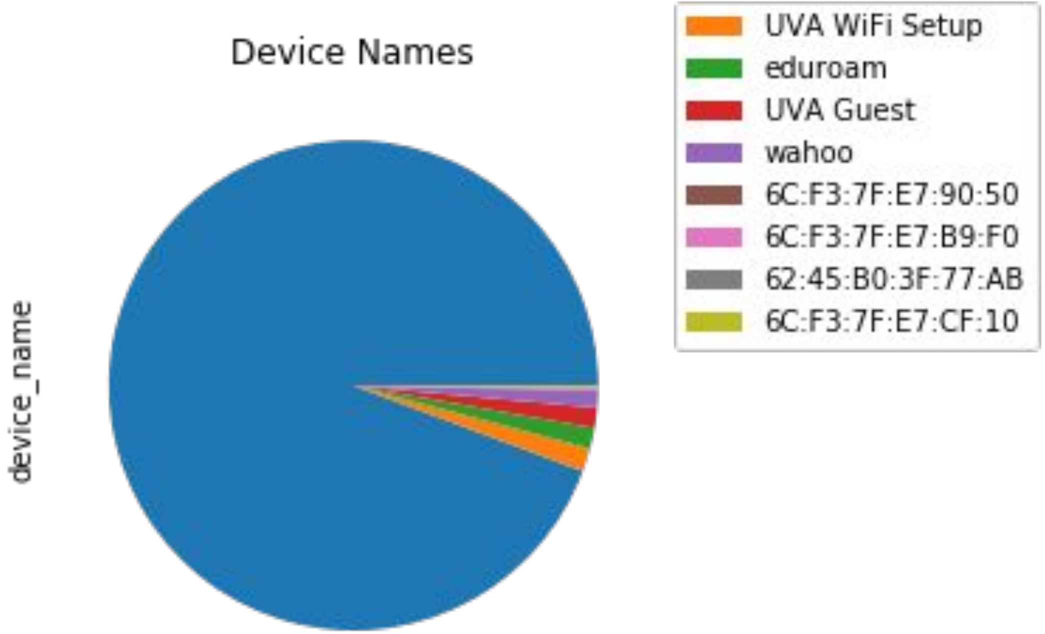
Data Analysis - SSIDs



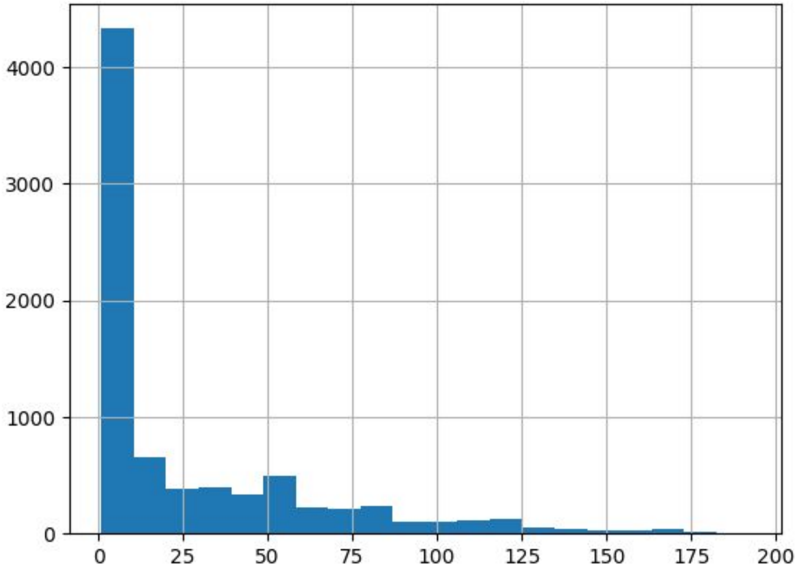
Data Analysis - Summary Statistics

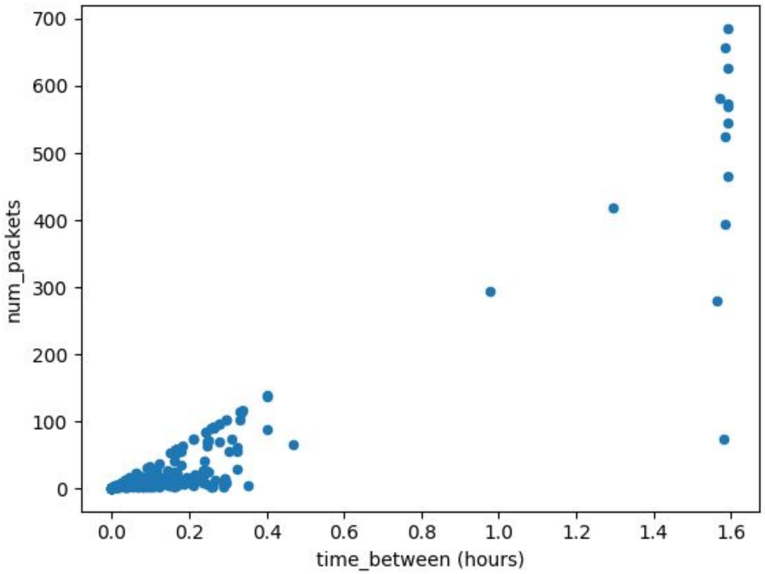


Data Analysis - WLAN



Data Analysis - Bluetooth





Limitations and Challenges

Monitor Mode

- Unsupported by most Windows laptops and some Macs
- Solution: Raspberry Pi and capture card

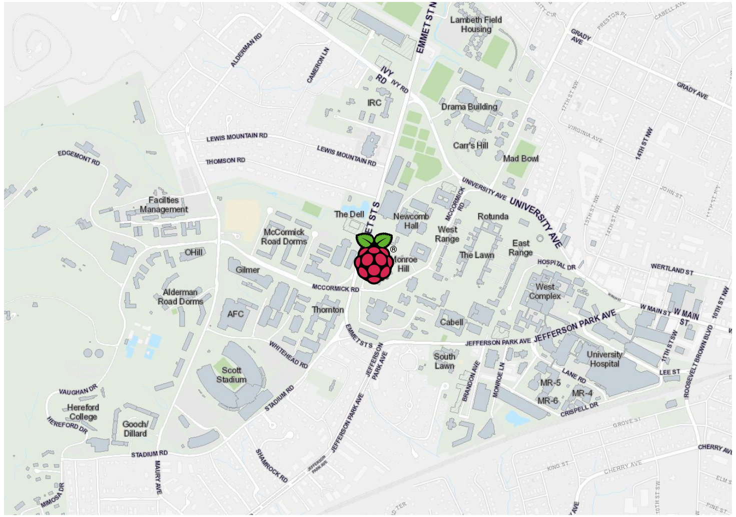
Img source: https://en.wikipedia.org/wiki/Computer_monitor

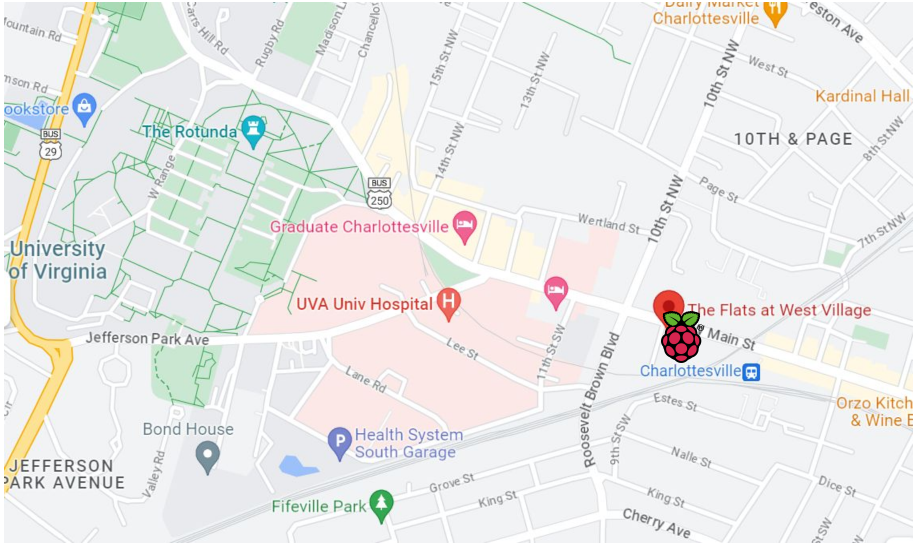
Kismet

- Works for Linux and macOS

Data Collection Locations

- Ability to leave data collection devices unattended was necessary





Unavailable Information

- Eduroam Security
- Unknown Device Manufacturers

https://www.flaticon.com/free-icon/cyber-security_1797500

Dashboard Tool

Backend

- Flask framework
- Application instance
    - “run” method - launches Flask’s integrated development web server.
    - Waits for incoming requests from client - requests are sent to application instance
    - To process incoming data - use request object
        - can use GET and POST methods to receive or send data.
    - Flask invokes a view function and returns a response value to the client.
- Used pandas and matplotlib libraries to create visuals of our analysis for display on the dashboard

Frontend

- Frontend of web apps handles how the application is displayed to the user
- For this project was built using HTML, CSS, and Javascript.
  - HTML is used to display the content
  - CSS describes styles of content
  - Javascript is for “client-side” services.

Demo

Thank you!

Questions?