Is my host spying on me?

Akash Deep Singh

OYO ROOMS

airbnb

SLEEP TIGHT

Airbnb Hosts Are Spying on Guests With Hidden Cameras

And the platform's botched handling of the issue puts guests in harm's way.

Kristin Houser | April 6th 2019

Best Policy

Airbnb's policy on recording guests is clear: hosts are allowed to have cameras on their property — but only if the devices aren't in bathrooms or

TECHNOLOGY

Airbnb Has a Hidden-Camera Problem

The home-rental start-up says it's cracking down on hosts who record guests. Is it doing enough?

SIDNEY FUSSELL MAR 26, 2019

MORE STO

Your Hea
Gold Min
SIDNEY FUS

The Micr
May Be H
Home
SIDNEY FUS

The Anal
Your Scre
Your Own

CNN World » Africa | Americas | Asia | Australia | China | Europe | Middle East | India | UK Live TV U.S. Editi

Hundreds of motel guests were secretly filmed and live-streamed online

By Sophie Jeong and James Griffiths, CNN
Updated 4:51 AM ET, Thu March 21, 2019

AirBnB policies on surveillance for hosts

- AirBnB requires hosts to disclose all security cameras and other recording devices in their listings
  - **even if it's not turned on or hooked up**
- prohibits any security cameras and other recording devices that are in or that observe the interior of certain private spaces (such as bedrooms and bathrooms), regardless of whether they've been disclosed.
- requires hosts to disclose if an active recording is taking place.
- If a host discloses the device after booking, Airbnb will allow the guest to cancel the reservation and receive a refund.

https://www.airbnb.com/help/article/887/what-are-airbnb-s-rules-about-security-cameras-and-other-recording-devices-in-listings

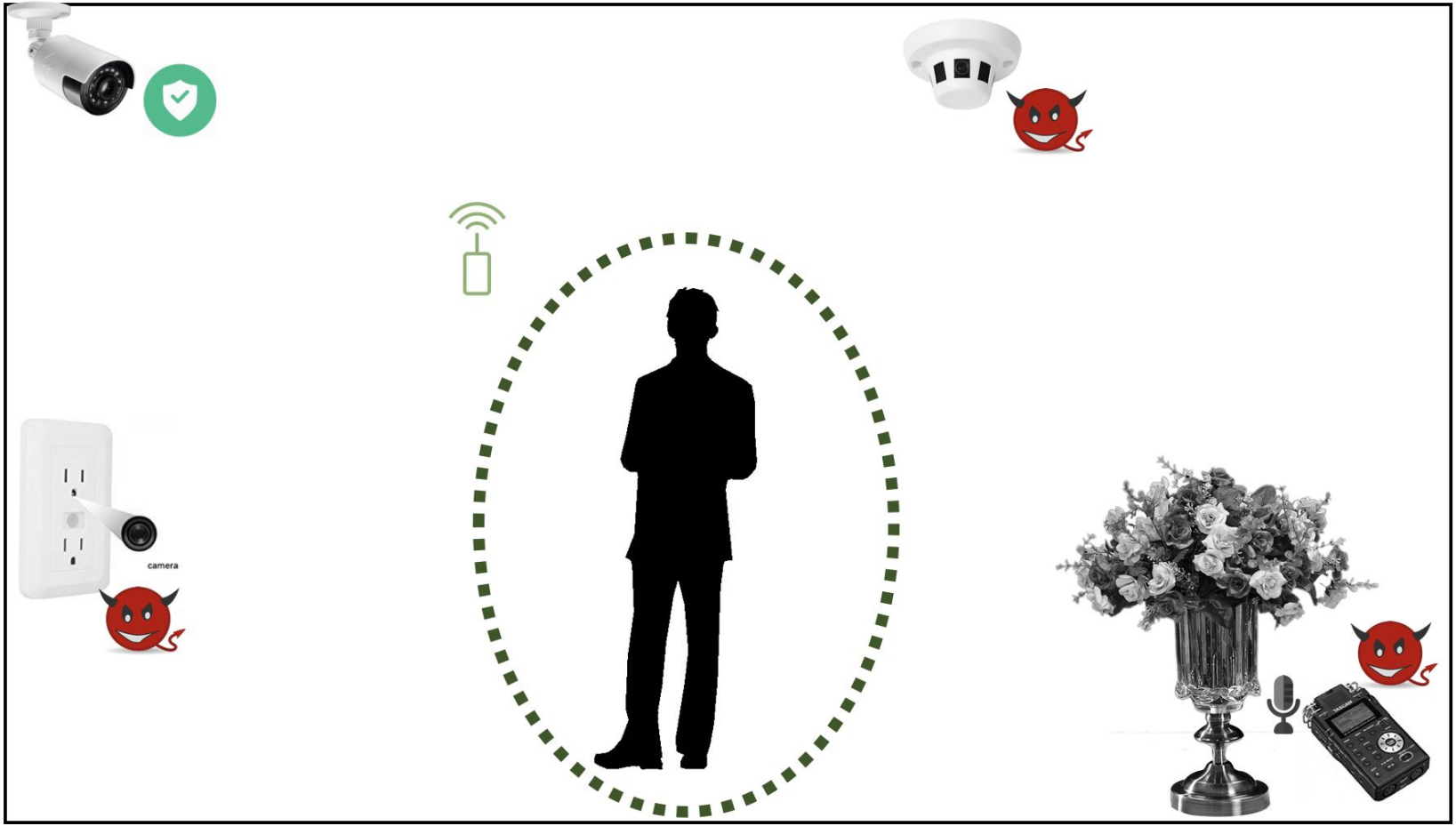
AirBnB policies on surveillance for guests

- requires that guests do not spy on other people, or otherwise violate others' privacy.
- prohibits the use of a security camera or any other recording device by a guest to monitor a host or any third party present in the listing without the consent of that person.

"Any mechanism that can be used to capture or transmit audio, video, or still images is considered a surveillance device"

Adversary Model

- The operator of the building or a 3rd party
- The adversary needs real-time access to information coming out of the room.
- The adversary is using wireless devices to spy on the user.


camera

Problem statement

Given a room, can you find:

- How many wireless devices are present?
- What type of devices are these?
- Where are they located?
- What physical state triggers the traffic?
- How often do they communicate?

Bug Detector

- Most commonly used today
- A receiver which simply scans the spectrum and beeps based on Rx power threshold.
- Lots of false positives!!

IoT Inspector (ARP Spoofing)

- An open-source desktop tool with a one-click install process
- Automatically discovers IoT devices and analyzes their network traffic
- Helps you identify security and privacy issues with graphs and tables
- Requires minimal technical skills and no special hardware
- Use it to quickly inspect devices (e.g., from your computer) or continuously monitor your network (e.g., from a Raspberry Pi)
- Destination IP addresses and ports contacted, Device manufacturers, Aggregate traffic statistics, SSDP messages, DHCP hostnames

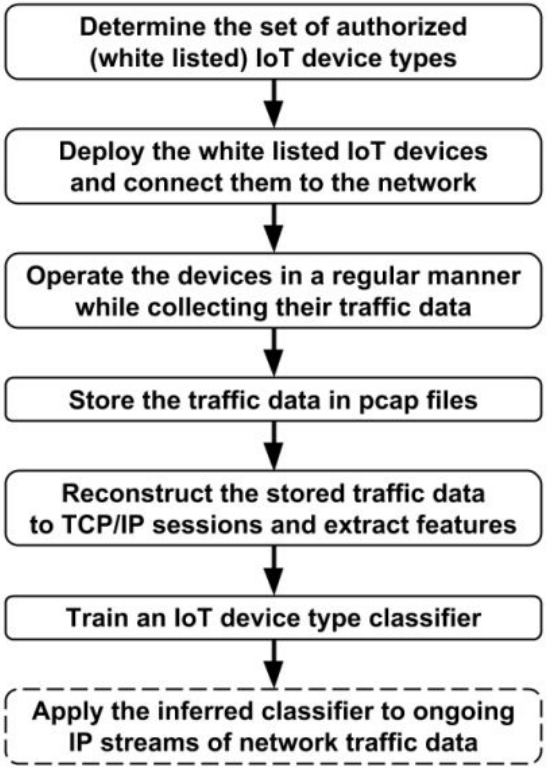
IoT Inspector works through ARP-spoofing

From IoT-Inspector website

IoT Inspector works through ARP-spoofing

From IoT-Inspector website

Detection of Unauthorized IoT Devices Using Machine Learning Techniques



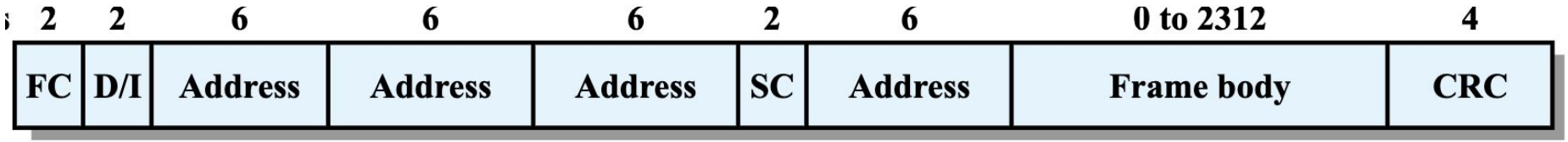
Meidan, Yair, et al. "Detection of unauthorized iot devices using machine learning techniques." *arXiv preprint arXiv:1709.04647* (2017).

WiFi

Possible types of networks in the area?

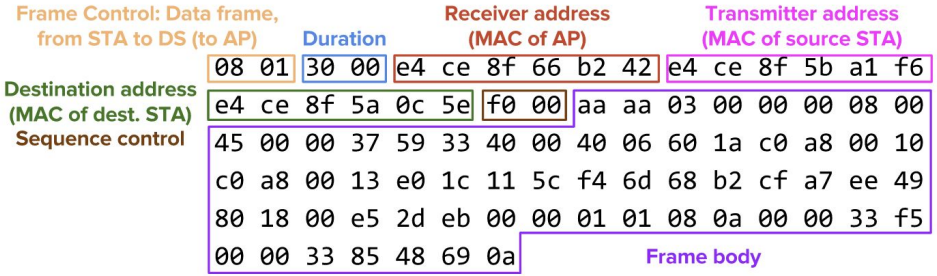
- Open Network
- Open Network + layer of web login
- Closed Network but password available
- Closed Network and password not available
- Hidden Network (Can’t see SSID)

Wifi Packet



FC = Frame control
D/I = Duration/connection ID
SC = Sequence control

Figure 1: IEEE 802.11 MAC frame format. Image from William Stallings "Data and Computer Communications".



RAW Hex Dump

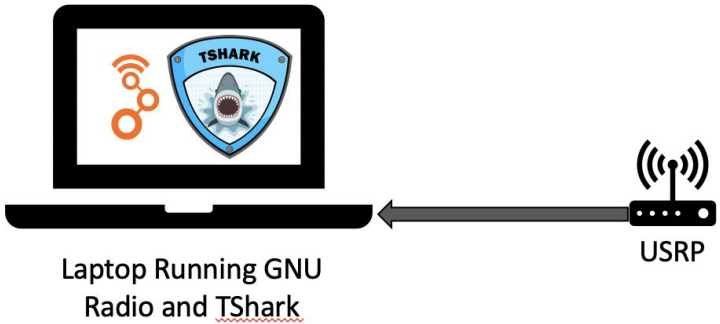
https://witestlab.poly.edu/blog/802-11-wireless-lan-2/

Detection

- Wireshark packet sniffing -
  - a large number of TCP/UDP packets show the presence of a video recorder.
  - Mac address lookup
  - Reverse DNS lookup

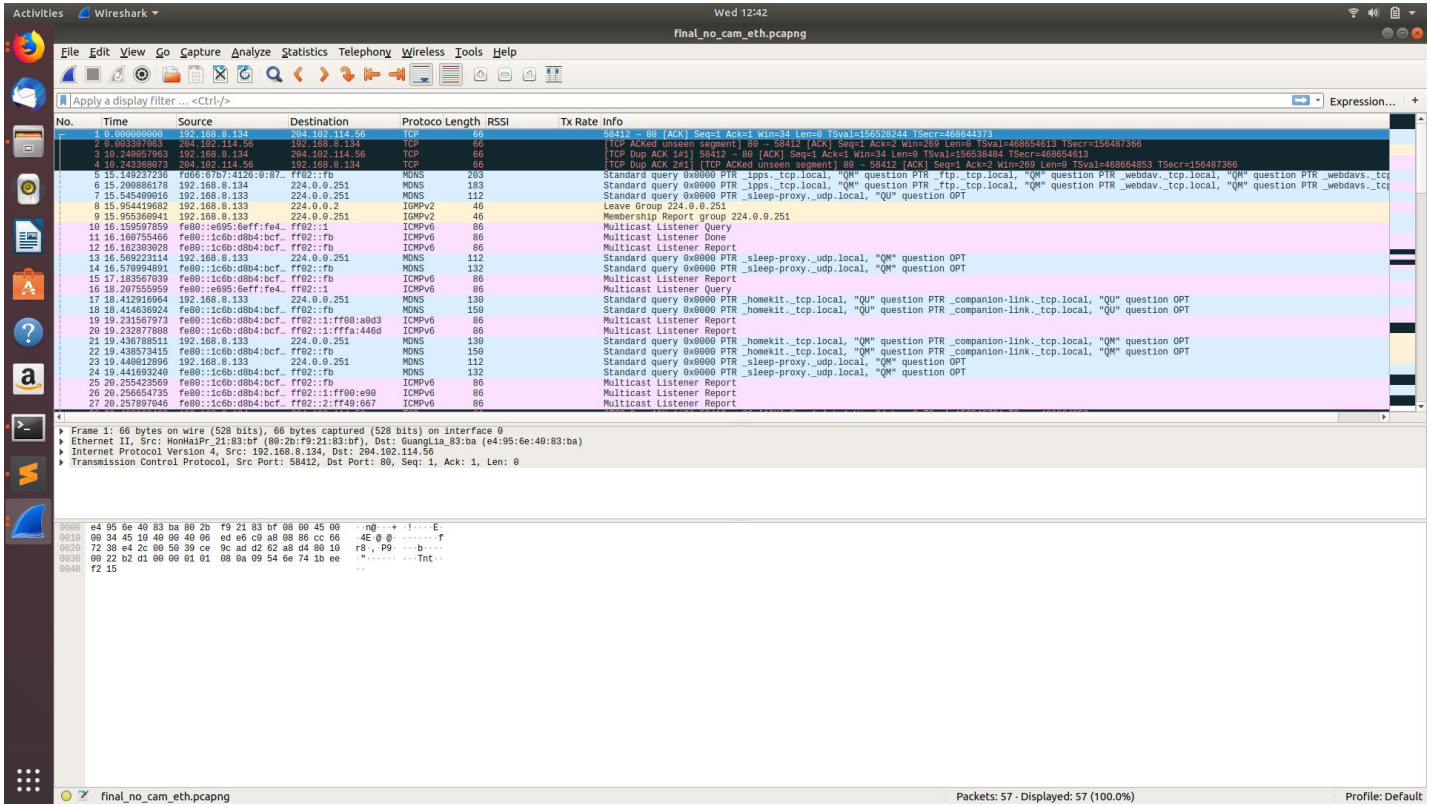
- USRP
  - Wifi receiver that can sniff packets in 2.4 and 5 GHz frequencies
  - Converted the received data into wireshark readable format
  - Mac address lookup

Hardware

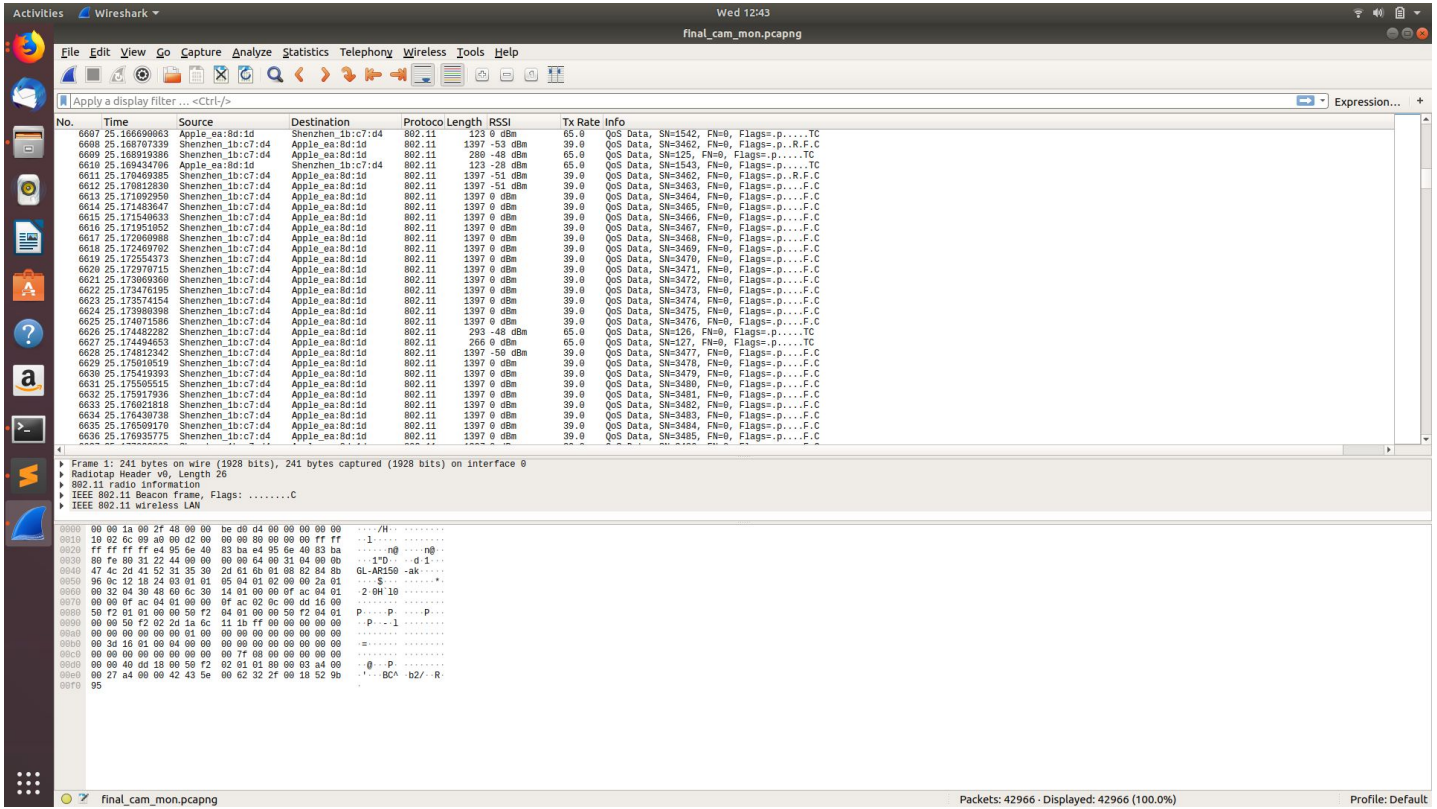

TSHARK
Laptop Running GNU Radio and TShark
USRP


GPIO
RESET
REF
USRP B205 mini-i
70 MHz - 6 GHz
USB3
Ettus Research
A National Instruments Company
RX2
TRX

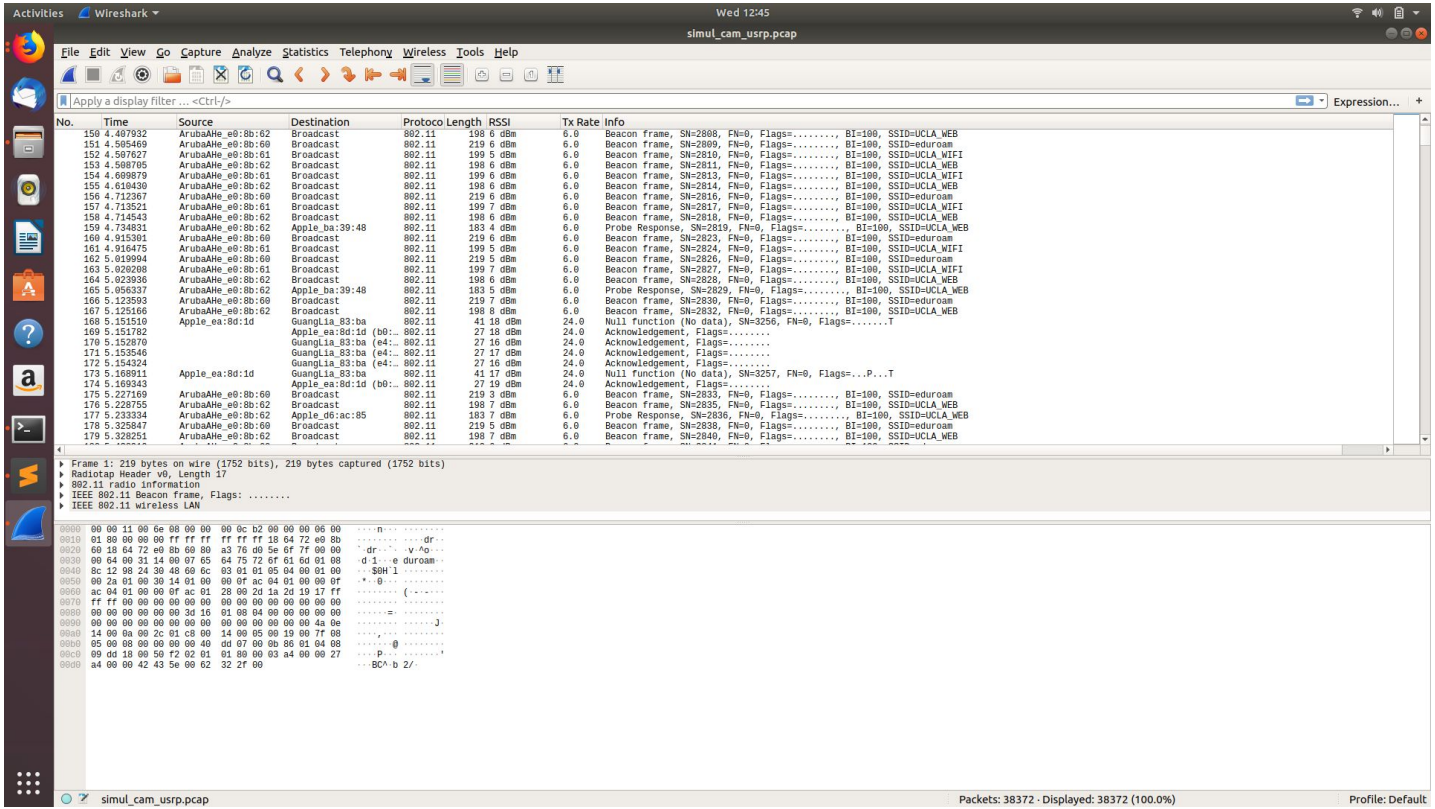
Packet Sniffing in managed mode

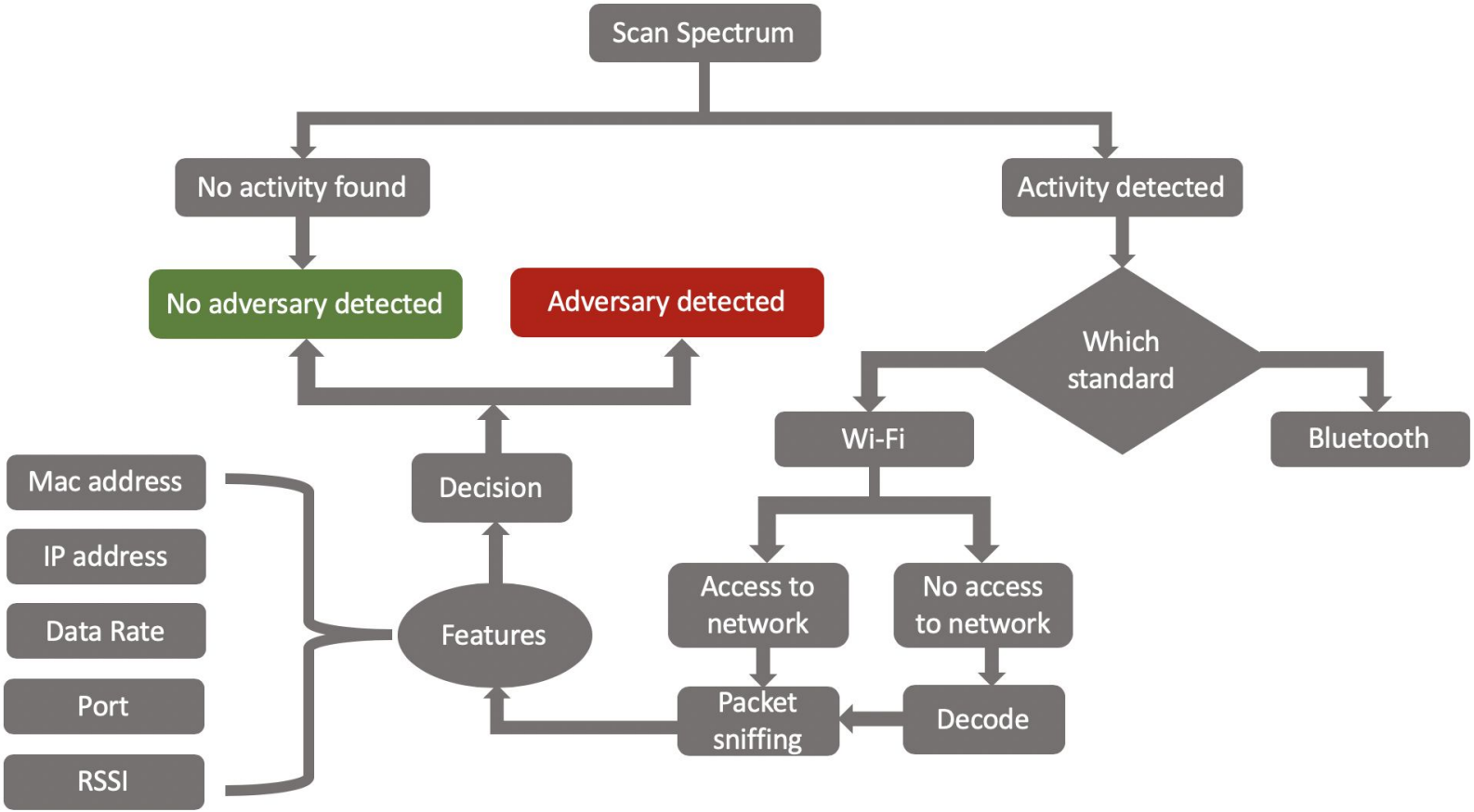


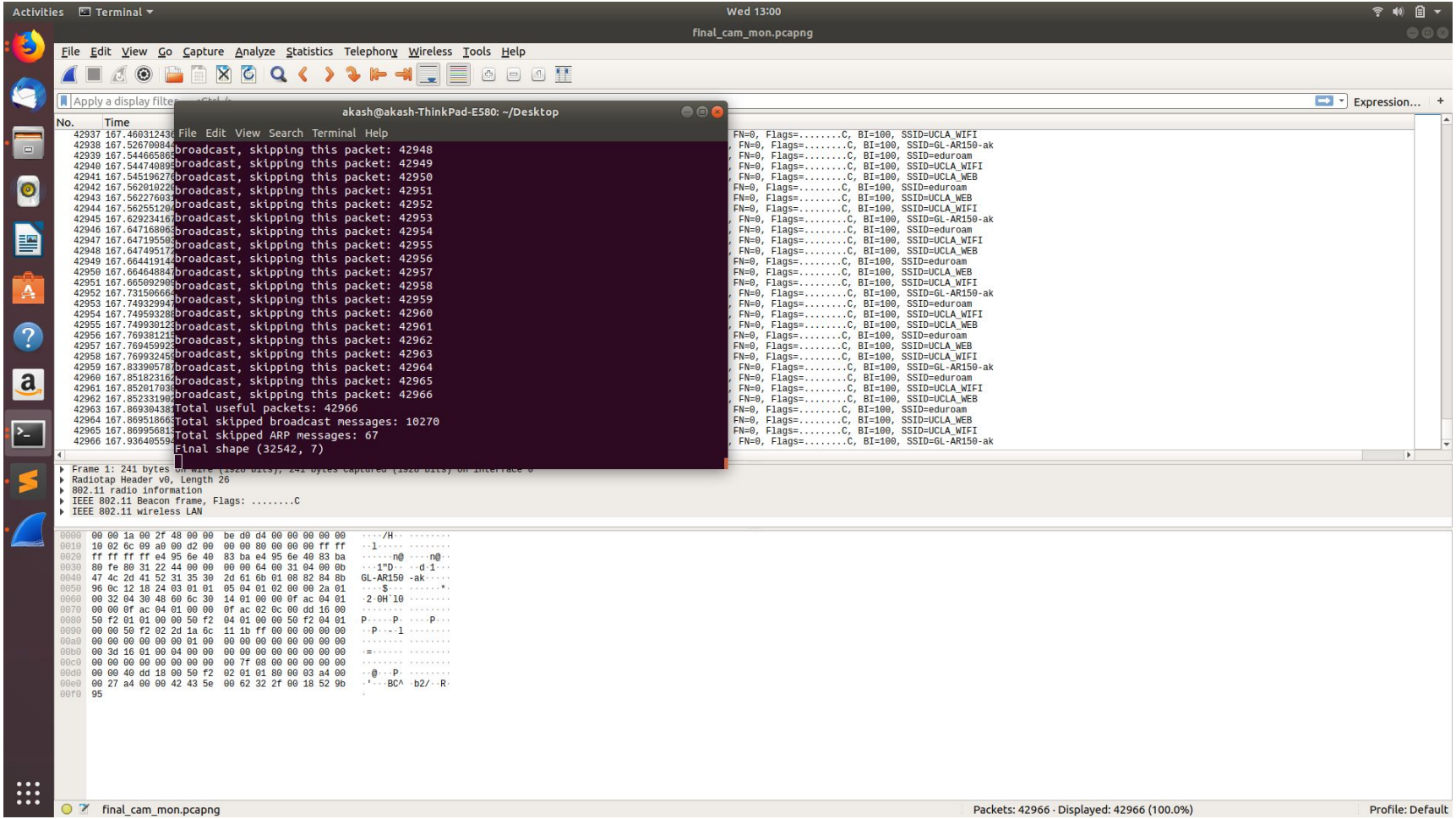
Packet sniffing in monitor mode



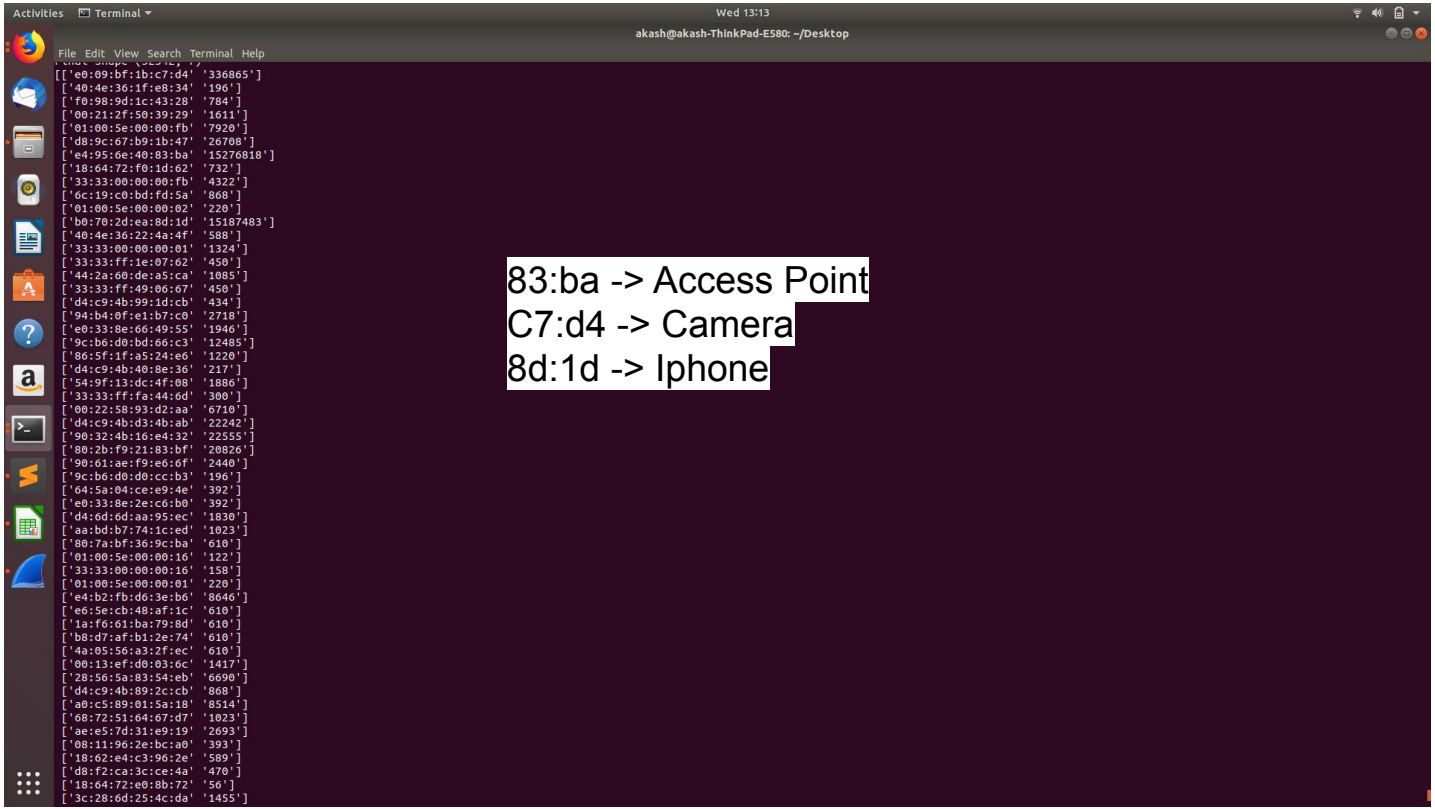
Packet sniffing using USRP




Scan Spectrum
No activity found
Activity detected
No adversary detected
Adversary detected
Which standard
Wi-Fi
Bluetooth
Mac address
IP address
Data Rate
Port
RSSI
Decision
Features
Access to network
No access to network
Packet sniffing
Decode


Activities
Terminal
Wed 13:00
final_cam_mon.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter
Expression...
No. Time
akash@akash-ThinkPad-E580: ~/Desktop
File Edit View Search Terminal Help
broadcast, skipping this packet: 42948
broadcast, skipping this packet: 42949
broadcast, skipping this packet: 42950
broadcast, skipping this packet: 42951
broadcast, skipping this packet: 42952
broadcast, skipping this packet: 42953
broadcast, skipping this packet: 42954
broadcast, skipping this packet: 42955
broadcast, skipping this packet: 42956
broadcast, skipping this packet: 42957
broadcast, skipping this packet: 42958
broadcast, skipping this packet: 42959
broadcast, skipping this packet: 42960
broadcast, skipping this packet: 42961
broadcast, skipping this packet: 42962
broadcast, skipping this packet: 42963
broadcast, skipping this packet: 42964
broadcast, skipping this packet: 42965
broadcast, skipping this packet: 42966
Total useful packets: 42966
Total skipped broadcast messages: 10270
Total skipped ARP messages: 67
Final shape (32542, 7)
Frame 1: 241 bytes
Radiotap Header v0, Length 26
802.11 radio information
IEEE 802.11 Beacon frame, Flags: C
IEEE 802.11 wireless LAN
final_cam_mon.pcapng
Packets: 42966 · Displayed: 42966 (100.0%)
Profile: Default

Top Tx

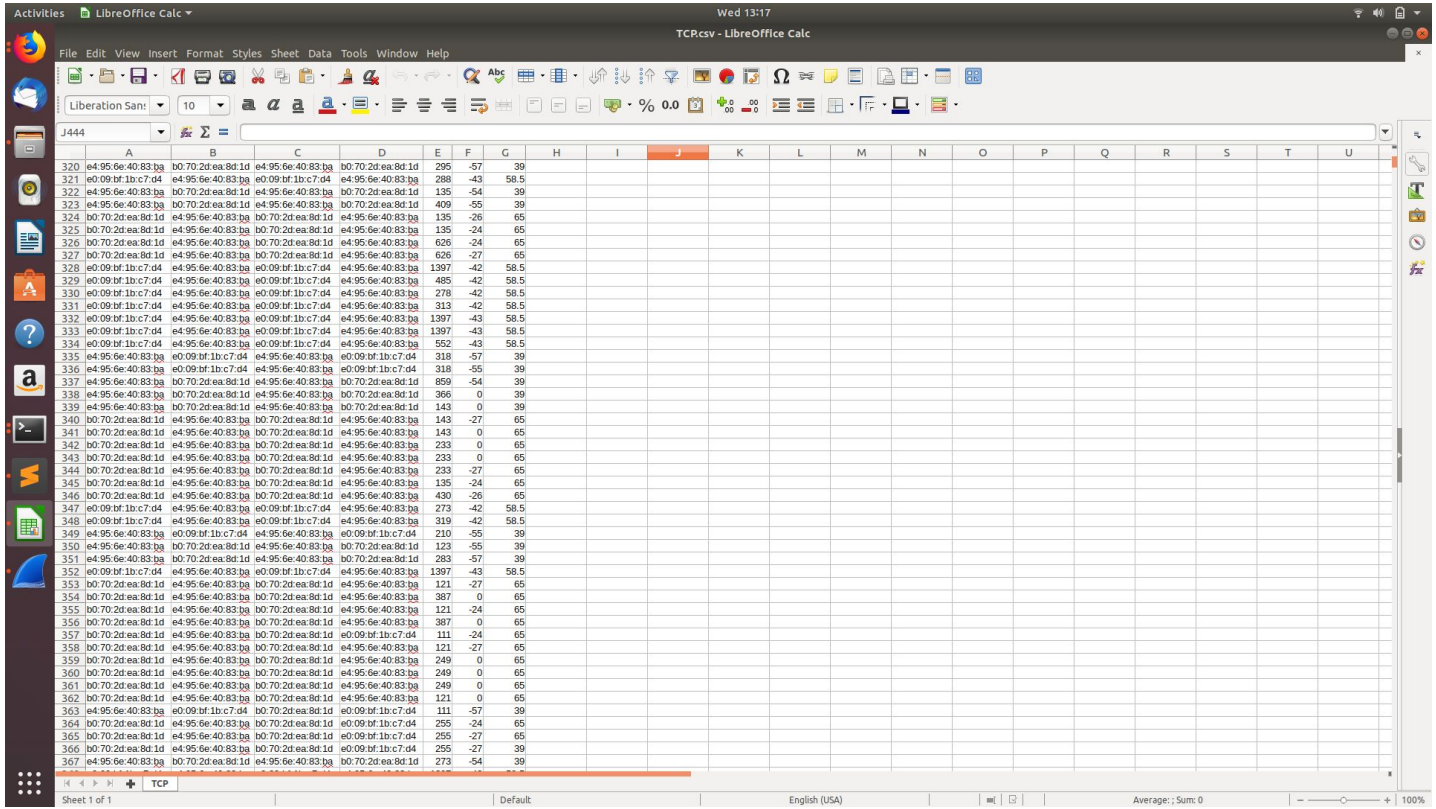


83:ba -> Access Point
C7:d4 -> Camera
8d:1d -> Iphone

Top Rx

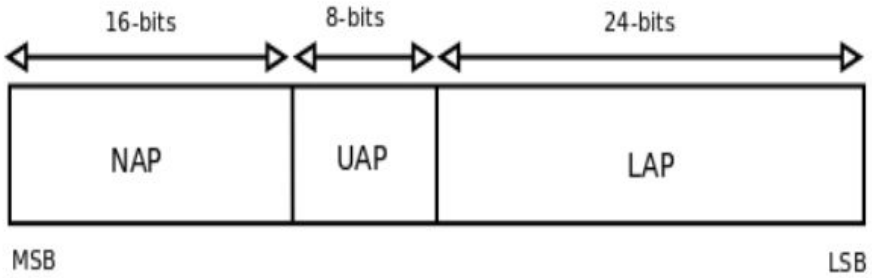
83:ba -> Access Point
C7:d4 -> Camera
8d:1d -> Iphone

Statistics


Activities
LibreOffice Calc
Wed 13:17
TCP.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation San
10
J444
TCP
Sheet 1 of 1
Default
English (USA)
Average: ; Sum: 0
100%

Bluetooth

Bluetooth Address - 48 bits



The three parts of a Bluetooth MAC address.

- LAP: Lower Address Part -> Transmitted with every packet
- Upper Address Part -> Only transmitted during handshake
- Non significant Address Part -> ignored during initial connection

79 channels of 1 MHz each

1600 hops a second in pseudo random manner

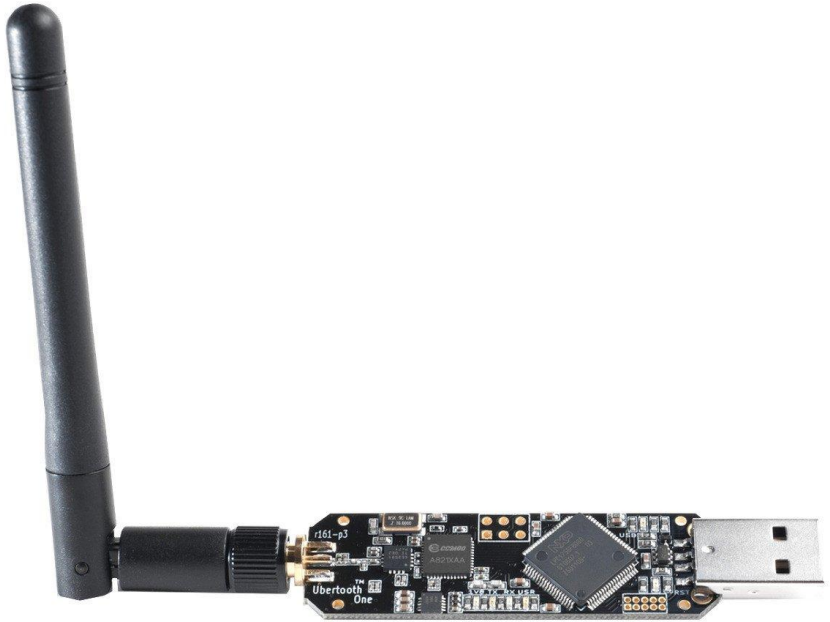
How to get UAP: Header Error Check (HEC): UAP + Header Bytes

Detection

- Wireshark packet sniffing -
  - a large number of TCP/UDP packets show the presence of a video recorder.
  - Mac address lookup
  - Reverse DNS lookup

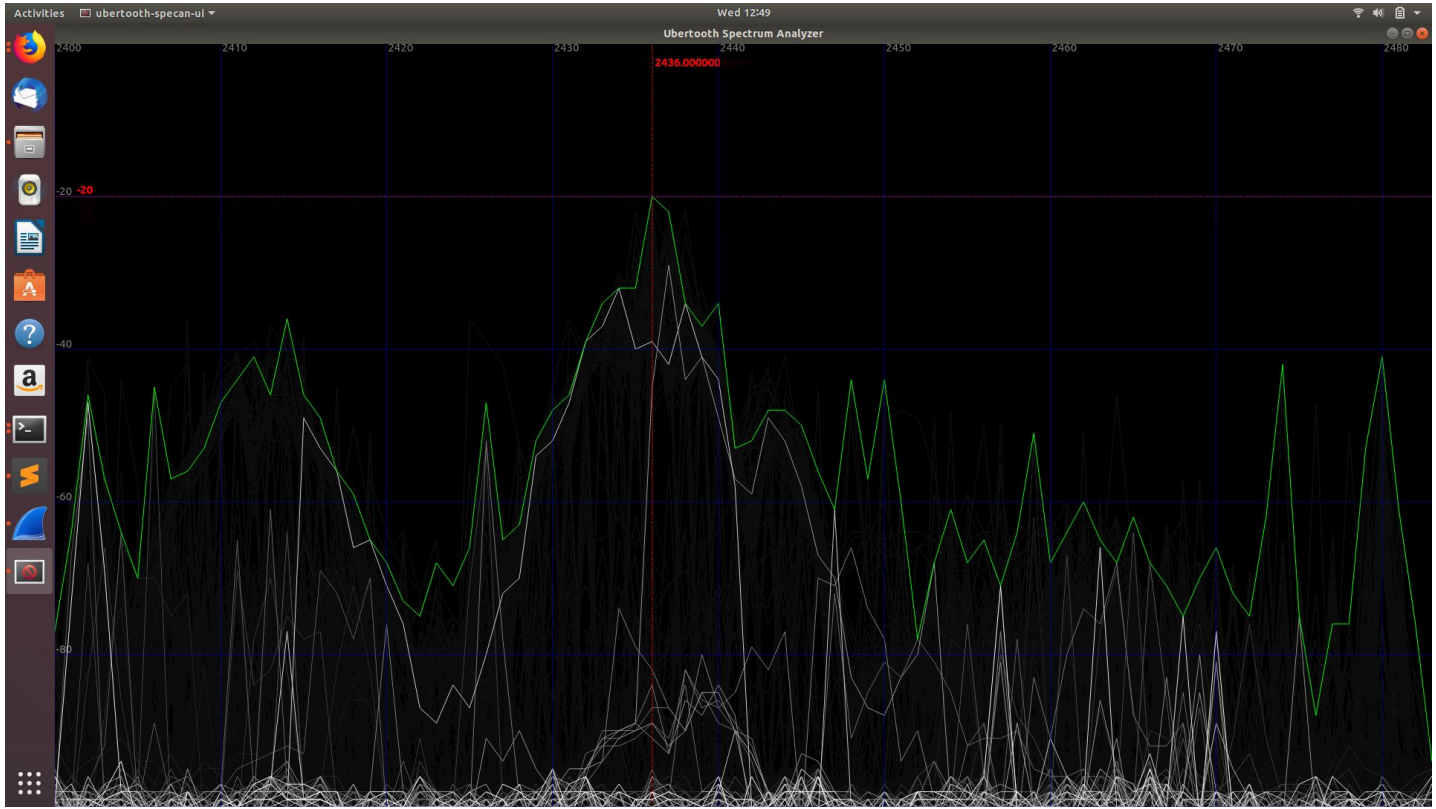
- USRP
  - Wifi receiver that can sniff packets in 2.4 and 5 GHz frequencies
  - Converted the received data into wireshark readable format
  - Mac address lookup

Hardware

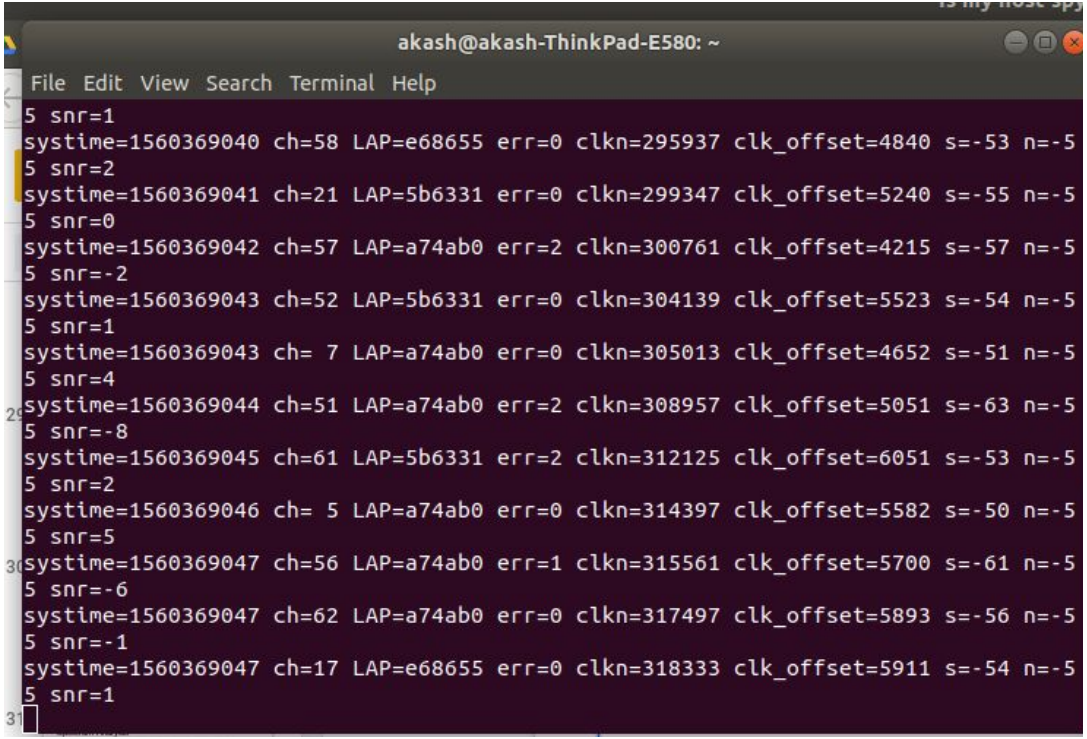


Ubertooth One

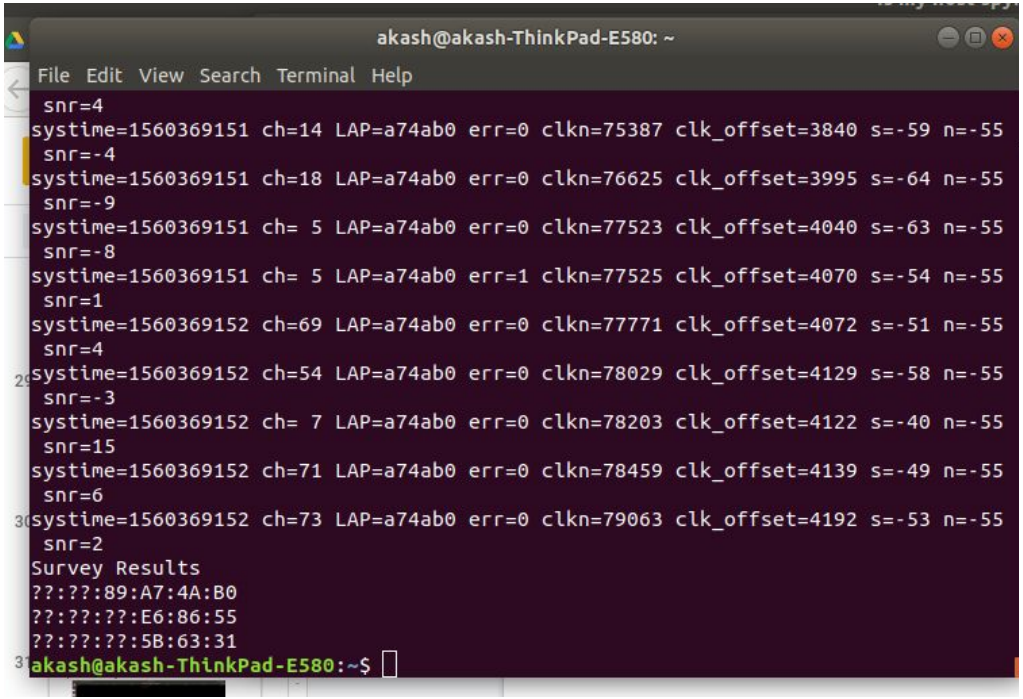
Spectrum Analysis



Passive sniffing



Device discovery

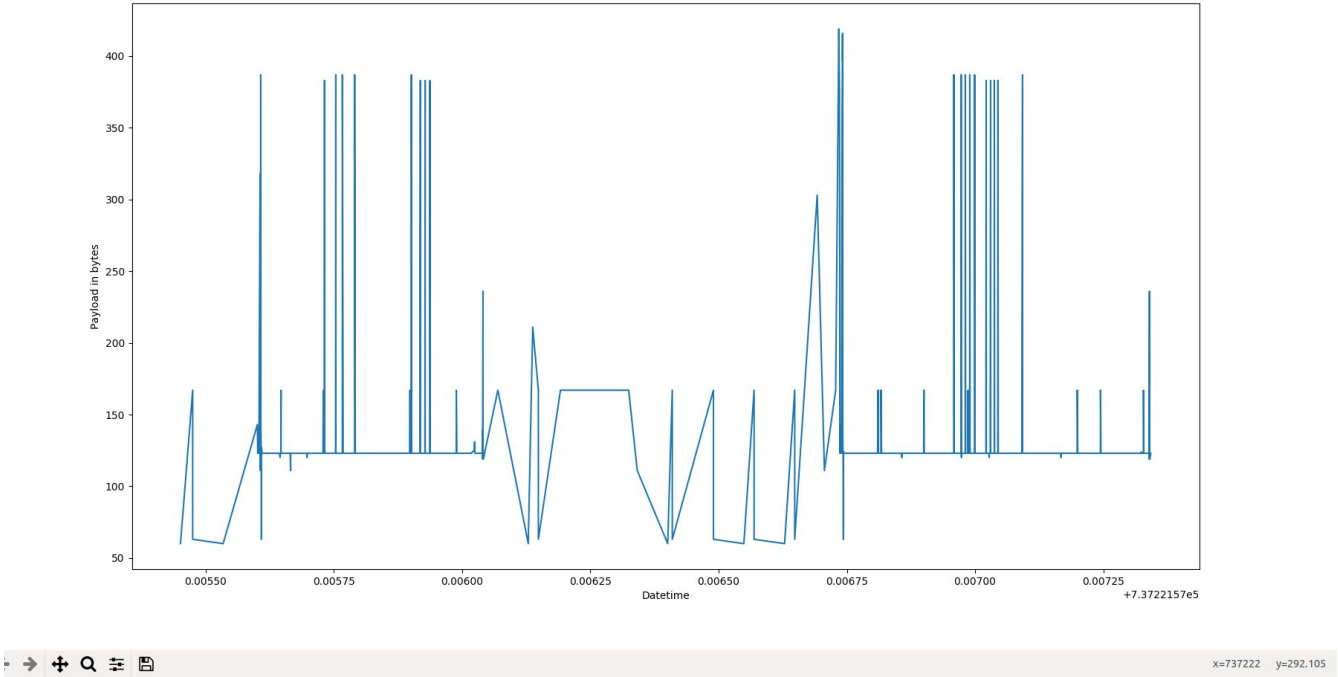


Localization

- The user walks in a room with the usrp
- We are filtering packets by mac address
- Increase in received power: moving closer to the device
- Decrease in received power: moving away from the device
- Packets being sent when the user crosses a particular region - further helps in recognizing the device.

Monitoring your own devices

What if you want to monitor how your own device works?



Challenges

➔ EAPOL stands for Extensible Authentication Protocol(EAP) over LAN. A simple 4-way handshake. Cannot sniff packets if device is connected before the start of sniffing.