ECE 209 AS

Project Report

Is my host spying on me?

- Akash Deep Singh, 405228294

Introduction:

The number of surveillance devices (e.g., security cameras and microphones) available due to the proliferation of Internet-of-Things (IoT) and their ease of installation allows users to use them to secure the spaces that they live in. These devices ensure the physical security of the spaces that they are installed in. This trend can largely be attributed to the growth of IoT devices[1]. Further, wireless devices have outpaced the growth of wired devices and are set to overtake them in terms of internet traffic generated [2] [3]. This can be largely attributed to the fact that wireless devices are easier to install and can easily be integrated into the home network over Wifi. Moreover, with large improvements in battery technology, some security cameras and microphones can last as long as 2 years [4]. This means that wireless devices with long battery life allow users to simply put them anywhere they want and integrate them over the Wifi network. There is no need to connect them with bulky network wires or power cables. Leveraging this, most of the devices and sensors used in smart homes have wireless communication capabilities and long battery life which enables people to easily install them.

These devices can connect to the Wifi router or to any smartphone over Bluetooth or other wireless standards.

However, this also poses a challenge to both the safety and security of the individuals who are surrounded by these devices. An adversary may hack into one of these devices or compromise the outgoing traffic from the smart home to decipher the activities and location of the user. This sensitive information can be used to plan physical attacks (theft/robberies) or to blackmail the people being monitored. Moreover, these devices can also be used to carry out DDoS attacks such as the Mirai botnet case [5]. To mitigate this, the users who own these devices can either limit the amount of sensitive information that these devices record either by changing their settings or place them in areas where they cannot record any compromising personal information, to begin with.

Nonetheless, the above will not hold true for cases in which the owners of these devices are the adversaries. The advent of homestay apps like Airbnb where anyone can rent out their house to travelers for a few days has pushed owners towards buying surveillance devices to ensure that their properties are safe and are being used as they expect them to be while they are rented out. Over the last few years, a large number of cases have been reported where the Airbnb hosts try to spy on the residents [6]. This problem is not just limited to apps like Airbnb but also affects motels [7], rooms aboard cruise ships [8] and have the potential to even affect well-established hotel chains where one malicious employee can bug several rooms.

As the number of IoT devices continue to proliferate, this problem is going to become more and more prominent. The current state of the art of a bug detector which is an RF receiver which can sense if the received power in a particular frequency range is above a certain threshold. The problem with such devices is that they are not reliable and can go off even when the user is using them near his mobile phone. Secondly, they are not sensitive enough for low power signals like BLE (Bluetooth Low Energy) communication. Also, they give no information about the type of device and where it is located. The host may simply have a wireless device to monitor the power consumption of his property, but to the bug detector, it would seem similar to an IP camera.

In this project, we present a technique to discover hidden sensing devices that communicate over a wireless link in a room. This method leverages some key ideas of packet sniffing, ARP spoofing and bug detectors to find out what kind of device is present and where is it sending its information. If a privacy threat is found, we also opportunistically determine what physical state triggers it and how frequently it is sharing its information.

Detecting devices on the network

Adversarial techniques that analyze the network traffic coming out of a house and inferring what IoT devices are present in the room have been explored [9] that allow the adversary to predict what the activity the user was performing at a certain point in time. However, techniques have emerged [10] that mask the network traffic which makes it harder for an adversary to determine what devices are connected to the home network.

Devices on the same network

Although these methods are effective in masking the outgoing traffic, they fail when the adversary is connected to the same access point as all other devices. IoT-Inspector [9] is one such tool that when connected to any home network, can determine what devices are on the network and how they communicate with their servers on the cloud. While one can use a similar technique to determine hidden surveillance devices in a room, they fail if these devices are not on the same network or if these devices are not transmitting continuously but save their data and send it all at once. Also, these techniques cannot determine where a particular device is hidden and what they are looking at. For example, if there is a window camera that is pointed outwards, it will not be a privacy threat for the occupants. However, if the said camera is pointing inwards, it is a big issue.

To overcome the issues mentioned above, we propose our own method, which takes advantage of received signal strength, packet spoofing and opportunistic sensing to detect and locate all surveillance devices present in a room.

Possible scenarios

Depending upon the type of Wifi network, a user may have one of the following 4 types of access to it:

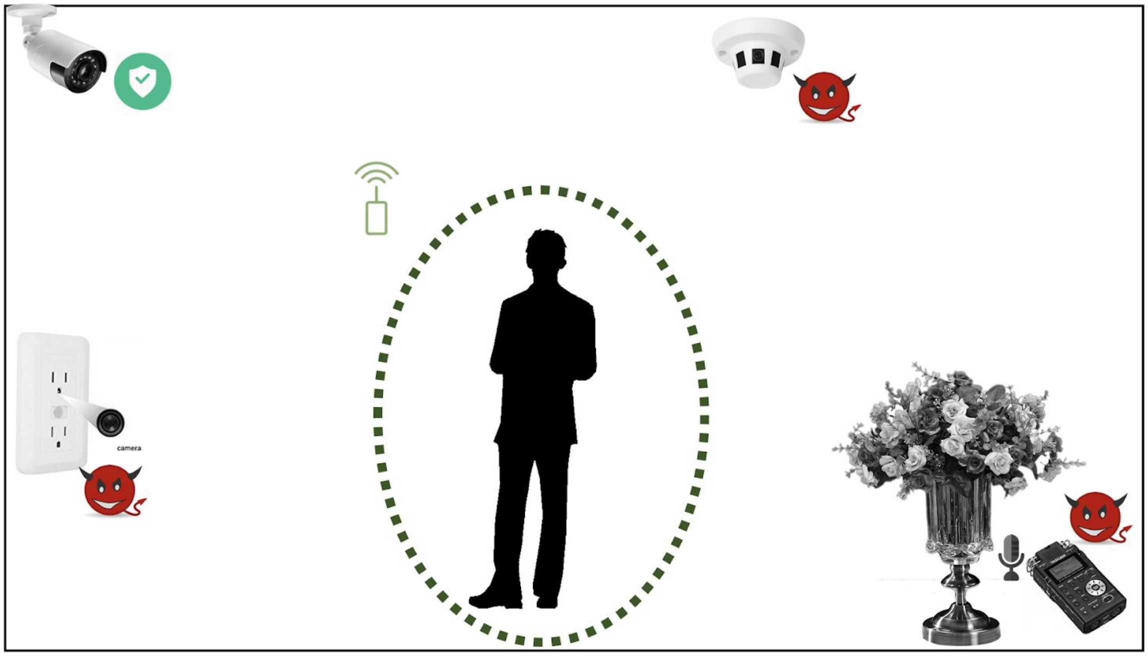
1. Open network: The network is open and anyone can look it up in the list of available networks and connect to it. They do not require any authentication.
2. Open network with web login: The network is similar to an open network but the user needs to login in through a web browser via some method (like a pin that is sent to his/her phone number)
3. Closed network with a password: The network is password protected but the host has given the password to the user. This case is similar to that of an open network.
4. Closed network: Either the user does not have the password to this network or this is an open network but only certain MAC address can connect to it or both.
5. Hidden network: There may be a hidden wifi network whose SSID is not visible on the list of available networks. Although these networks exist, it is very difficult to detect them using current tools. Hence we will use USRP for these cases.

Adversary Model

Based on the above possible cases, the adversary may have connected the hidden devices to the wifi in the following ways:

- The operator of the building or a 3rd party
- The adversary needs real-time access to information coming out of the room.

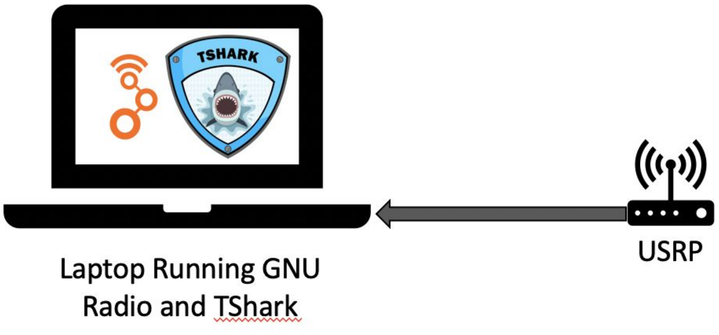
- The adversary is using wireless devices to spy on the user.

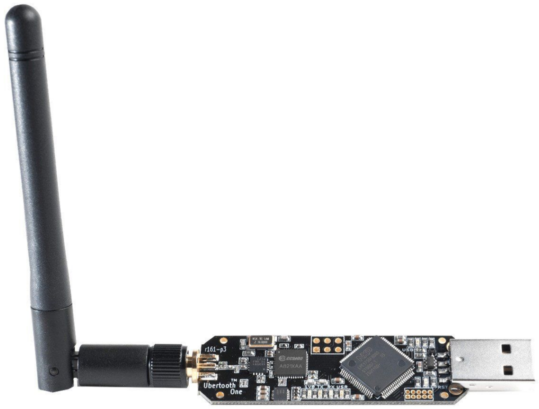


Hardware

In this work, we propose a varying set of hardware that one can make use of. This largely depends upon the adversary model as well as the amount of information the user wants to extract the adversarial devices.

- Laptop/Mobile: In our work, we have used a laptop running Wireshark, which is a network sniffing tool. There are similar apps available for smartphones too. It is not unfair to expect people to have either one of the two devices with them in today's day and age.
- USRP: a type of software-defined radio manufactured by Ettus Research. We are using the B205i-mini model.
- Ubertooth One: Software defined radio for Bluetooth packet sniffing.

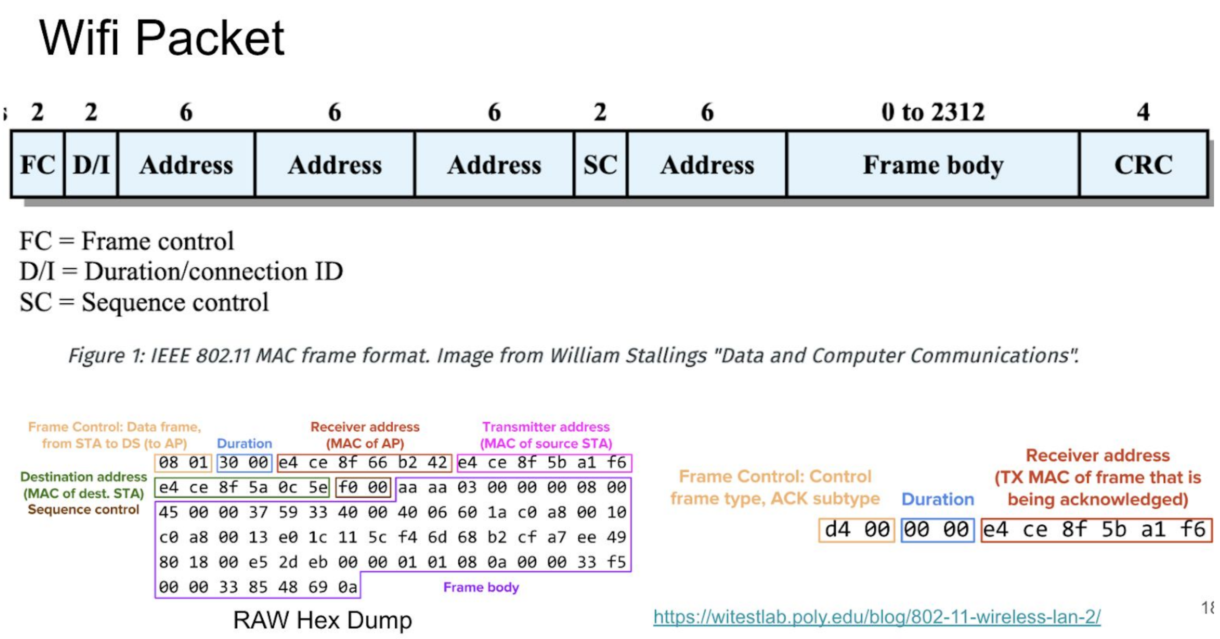




Software:

- Wireshark: Used for packet analysis
- Pyshark: Python library based on tshark which is a terminal based wireshark utility
- GNU Radio: is a free & open-source software development toolkit that provides signal processing blocks to implement software radios.

Wifi Packet:



Wifi Packet

2	2	6	6	6	2	6	0 to 2312	4
FC	D/I	Address	Address	Address	SC	Address	Frame body	CRC

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".

```
08 01 30 00 e4 ce 8f 66 b2 42 e4 ce 8f 5b a1 f6
e4 ce 8f 5a 0c 5e f0 00 aa aa 03 00 00 00 08 00
45 00 00 37 59 33 40 00 40 06 60 1a c0 a8 00 10
c0 a8 00 13 e0 1c 11 5c f4 6d 68 b2 cf a7 ee 49
80 18 00 e5 2d eb 00 00 01 01 08 0a 00 00 33 f5
00 00 33 85 48 69 0a
```

Frame Control: Data frame, from STA to DS (to AP)
Duration
Receiver address (MAC of AP)
Transmitter address (MAC of source STA)
Destination address (MAC of dest. STA)
Sequence control
Frame body

RAW Hex Dump

```
d4 00 00 00 e4 ce 8f 5b a1 f6
```

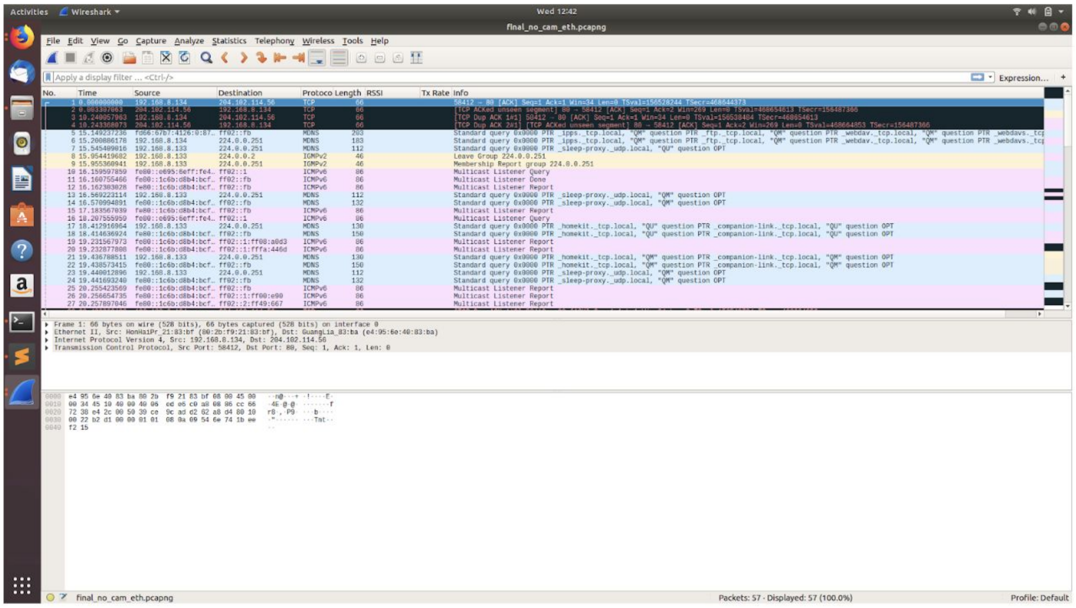
Frame Control: Control frame type, ACK subtype
Duration
Receiver address (TX MAC of frame that is being acknowledged)

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

Ways to sniff wifi packets:

- Wireshark packet sniffing using Wifi card in the laptop-
  - a large number of TCP/UDP packets show the presence of a video recorder.
  - Mac address lookup
  - Reverse DNS lookup
  - It has two modes:
    - Managed mode: when the laptop is connected to a wifi network and we can only listen to the traffic in that frequency range
    - Monitor: when we want to sniff all traffic in a given frequency range
- USRP used as a wifi receiver
  - Wifi receiver that can sniff packets in 2.4 and 5 GHz frequencies
  - Converted the received data into Wireshark readable format
  - Mac address lookup

Packet Sniffing in managed mode



Activities
Wireshark
Wed 12:42
final_no_cam_eth.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

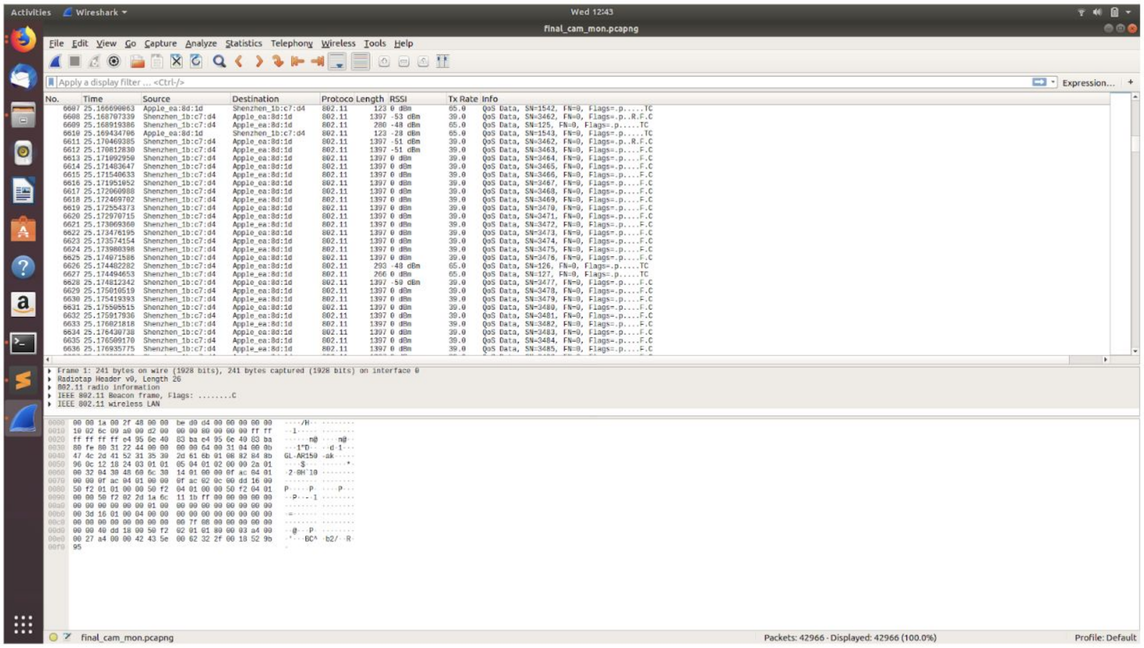
```
No.  Time         Source                Destination         Protoco Length RSSI  Tx Rate Info
   1 0.000000000  192.168.8.134         204.102.114.56      TCP       66          58412 → 80 [ACK] Seq=1 Ack=1 Win=34 Len=0 TSval=156528244 TSecr=468644373
   2 0.003307063  204.102.114.56        192.168.8.134       TCP       66          [TCP ACKed unseen segment] 80 → 58412 [ACK] Seq=1 Ack=2 Win=269 Len=0 TSval=468654613 TSecr=156487366
   3 10.240057963 192.168.8.134         204.102.114.56      TCP       66          [TCP Dup ACK 1#1] 58412 → 80 [ACK] Seq=1 Ack=1 Win=34 Len=0 TSval=156538484 TSecr=468654613
   4 10.243368073 204.102.114.56        192.168.8.134       TCP       66          [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 58412 [ACK] Seq=1 Ack=2 Win=269 Len=0 TSval=468664853 TSecr=156487366
   5 15.149237236 fd66:67b7:4126:0:87…  ff02::fb            MDNS     203          Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ftp._tcp.local, "QM" question PTR _webdav._tcp.local, "QM" question PTR _webdavs._tcp
   6 15.200886178 192.168.8.134         224.0.0.251         MDNS     183          Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ftp._tcp.local, "QM" question PTR _webdav._tcp.local, "QM" question PTR _webdavs._tcp
   7 15.545409016 192.168.8.133         224.0.0.251         MDNS     112          Standard query 0x0000 PTR _sleep-proxy._udp.local, "QU" question OPT
   8 15.954419682 192.168.8.133         224.0.0.2           IGMPv2    46          Leave Group 224.0.0.251
   9 15.955360941 192.168.8.133         224.0.0.251         IGMPv2    46          Membership Report group 224.0.0.251
  10 16.159597859 fe80::e695:6eff:fe4…  ff02::1             ICMPv6    86          Multicast Listener Query
  11 16.160755466 fe80::1c6b:d8b4:bcf…  ff02::fb            ICMPv6    86          Multicast Listener Done
  12 16.162303028 fe80::1c6b:d8b4:bcf…  ff02::fb            ICMPv6    86          Multicast Listener Report
  13 16.569223114 192.168.8.133         224.0.0.251         MDNS     112          Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
  14 16.570994891 fe80::1c6b:d8b4:bcf…  ff02::fb            MDNS     132          Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
  15 17.183567039 fe80::1c6b:d8b4:bcf…  ff02::fb            ICMPv6    86          Multicast Listener Report
  16 18.207555959 fe80::e695:6eff:fe4…  ff02::1             ICMPv6    86          Multicast Listener Query
  17 18.412916964 192.168.8.133         224.0.0.251         MDNS     130          Standard query 0x0000 PTR _homekit._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question OPT
  18 18.414636924 fe80::1c6b:d8b4:bcf…  ff02::fb            MDNS     150          Standard query 0x0000 PTR _homekit._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question OPT
  19 19.231567973 fe80::1c6b:d8b4:bcf…  ff02::1:ff08:a0d3   ICMPv6    86          Multicast Listener Report
  20 19.232877808 fe80::1c6b:d8b4:bcf…  ff02::1:fffa:446d   ICMPv6    86          Multicast Listener Report
  21 19.436788511 192.168.8.133         224.0.0.251         MDNS     130          Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question OPT
  22 19.438573415 fe80::1c6b:d8b4:bcf…  ff02::fb            MDNS     150          Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question OPT
  23 19.440012896 192.168.8.133         224.0.0.251         MDNS     112          Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
  24 19.441693240 fe80::1c6b:d8b4:bcf…  ff02::fb            MDNS     132          Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
  25 20.255423569 fe80::1c6b:d8b4:bcf…  ff02::fb            ICMPv6    86          Multicast Listener Report
  26 20.256654735 fe80::1c6b:d8b4:bcf…  ff02::1:ff00:e90    ICMPv6    86          Multicast Listener Report
  27 20.257897046 fe80::1c6b:d8b4:bcf…  ff02::2:ff49:667    ICMPv6    86          Multicast Listener Report
```

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_21:83:bf (80:2b:f9:21:83:bf), Dst: GuangLia_83:ba (e4:95:6e:40:83:ba)
▸ Internet Protocol Version 4, Src: 192.168.8.134, Dst: 204.102.114.56
▸ Transmission Control Protocol, Src Port: 58412, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  e4 95 6e 40 83 ba 80 2b  f9 21 83 bf 08 00 45 00   ··n@···+ ·!····E·
0010  00 34 45 10 40 00 40 06  ed e6 c0 a8 08 86 cc 66   ·4E·@·@· ·······f
0020  72 38 e4 2c 00 50 39 ce  9c ad d2 62 a8 d4 80 10   r8·,·P9· ···b····
0030  00 22 b2 d1 00 00 01 01  08 0a 09 54 6e 74 1b ee   ·"······ ···Tnt··
0040  f2 15                                              ··
```

final_no_cam_eth.pcapng   Packets: 57 · Displayed: 57 (100.0%)   Profile: Default

Packet sniffing in monitor mode



Activities
Wireshark
Wed 12:43
final_cam_mon.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

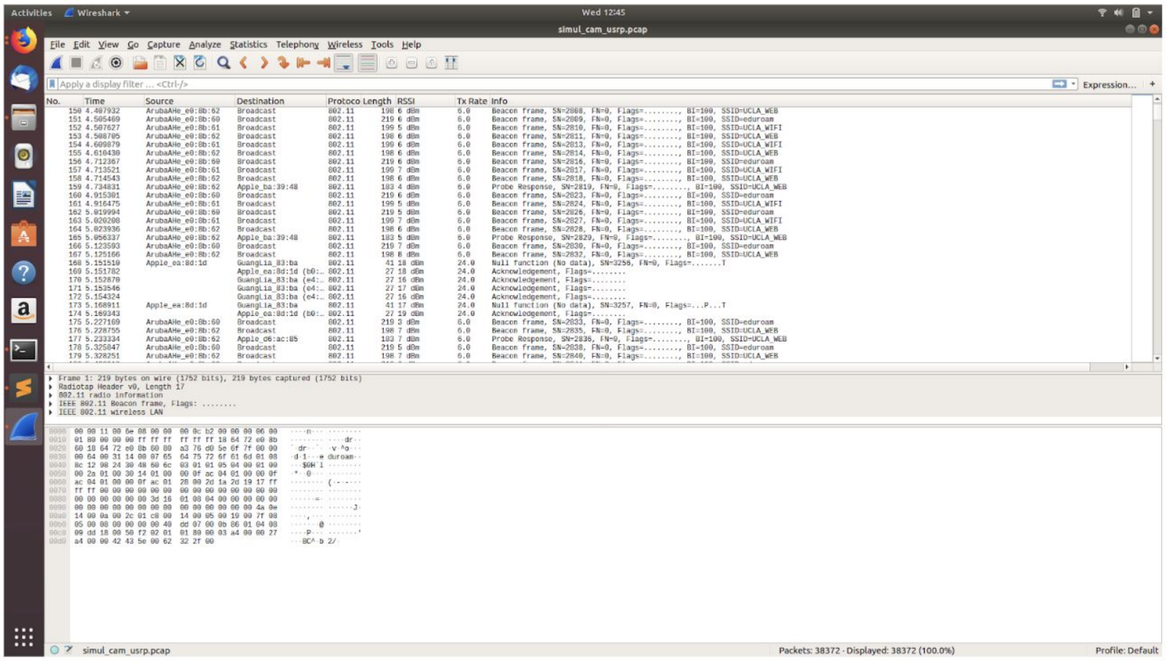
```
No.  Time         Source              Destination         Protoco Length RSSI     Tx Rate Info
6607 25.166690063 Apple_ea:8d:1d      Shenzhen_1b:c7:d4   802.11   123 0 dBm     65.0    QoS Data, SN=1542, FN=0, Flags=.p.....TC
6608 25.168707339 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 -53 dBm   39.0    QoS Data, SN=3462, FN=0, Flags=.p..R.F.C
6609 25.168919386 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11   280 -48 dBm   65.0    QoS Data, SN=125, FN=0, Flags=.p.....TC
6610 25.169434706 Apple_ea:8d:1d      Shenzhen_1b:c7:d4   802.11   123 -28 dBm   65.0    QoS Data, SN=1543, FN=0, Flags=.p.....TC
6611 25.170469385 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 -51 dBm   39.0    QoS Data, SN=3462, FN=0, Flags=.p..R.F.C
6612 25.170812830 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 -51 dBm   39.0    QoS Data, SN=3463, FN=0, Flags=.p....F.C
6613 25.171092950 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3464, FN=0, Flags=.p....F.C
6614 25.171483647 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3465, FN=0, Flags=.p....F.C
6615 25.171540633 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3466, FN=0, Flags=.p....F.C
6616 25.171951052 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3467, FN=0, Flags=.p....F.C
6617 25.172060988 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3468, FN=0, Flags=.p....F.C
6618 25.172469702 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3469, FN=0, Flags=.p....F.C
6619 25.172554373 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3470, FN=0, Flags=.p....F.C
6620 25.172970715 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3471, FN=0, Flags=.p....F.C
6621 25.173069360 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3472, FN=0, Flags=.p....F.C
6622 25.173476195 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3473, FN=0, Flags=.p....F.C
6623 25.173574154 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3474, FN=0, Flags=.p....F.C
6624 25.173980398 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3475, FN=0, Flags=.p....F.C
6625 25.174071586 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3476, FN=0, Flags=.p....F.C
6626 25.174482282 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11   293 -48 dBm   65.0    QoS Data, SN=126, FN=0, Flags=.p.....TC
6627 25.174494653 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11   266 0 dBm     65.0    QoS Data, SN=127, FN=0, Flags=.p.....TC
6628 25.174812342 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 -50 dBm   39.0    QoS Data, SN=3477, FN=0, Flags=.p....F.C
6629 25.175010519 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3478, FN=0, Flags=.p....F.C
6630 25.175419393 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3479, FN=0, Flags=.p....F.C
6631 25.175505515 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3480, FN=0, Flags=.p....F.C
6632 25.175917936 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3481, FN=0, Flags=.p....F.C
6633 25.176021818 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3482, FN=0, Flags=.p....F.C
6634 25.176430738 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3483, FN=0, Flags=.p....F.C
6635 25.176509170 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3484, FN=0, Flags=.p....F.C
6636 25.176935775 Shenzhen_1b:c7:d4   Apple_ea:8d:1d      802.11  1397 0 dBm     39.0    QoS Data, SN=3485, FN=0, Flags=.p....F.C
```

```
▸ Frame 1: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface 0
▸ Radiotap Header v0, Length 26
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▸ IEEE 802.11 wireless LAN
```

```
0000  00 00 1a 00 2f 48 00 00  be d0 d4 00 00 00 00 00   ····/H·· ········
0010  10 02 6c 09 a0 00 d2 00  00 00 80 00 00 00 ff ff   ··l····· ········
0020  ff ff ff ff e4 95 6e 40  83 ba e4 95 6e 40 83 ba   ······n@ ····n@··
0030  80 fe 80 31 22 44 00 00  00 00 64 00 31 04 00 0b   ···1"D·· ··d·1···
0040  47 4c 2d 41 52 31 35 30  2d 61 6b 01 08 82 84 8b   GL-AR150 -ak·····
0050  96 0c 12 18 24 03 01 01  05 04 01 02 00 00 2a 01   ····$··· ······*·
0060  00 32 04 30 48 60 6c 30  14 01 00 00 0f ac 04 01   ·2·0H`l0 ········
0070  00 00 0f ac 04 01 00 00  0f ac 02 0c 00 dd 16 00   ········ ········
0080  50 f2 01 01 00 00 50 f2  04 01 00 00 50 f2 04 01   P·····P· ····P···
0090  00 00 50 f2 02 2d 1a 6c  11 1b ff 00 00 00 00 00   ··P··-·l ········
00a0  00 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 3d 16 01 00 04 00 00  00 00 00 00 00 00 00 00   ·=······ ········
00c0  00 00 00 00 00 00 00 00  00 7f 08 00 00 00 00 00   ········ ········
00d0  00 00 40 dd 18 00 50 f2  02 01 01 80 00 03 a4 00   ··@···P· ········
00e0  00 27 a4 00 00 42 43 5e  00 62 32 2f 00 18 52 9b   ·'···BC^ ·b2/··R·
00f0  95                                                 ·
```

final_cam_mon.pcapng   Packets: 42966 · Displayed: 42966 (100.0%)   Profile: Default

Packet sniffing using USRP


Activities
Wireshark
Wed 12:45
simul_cam_usrp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

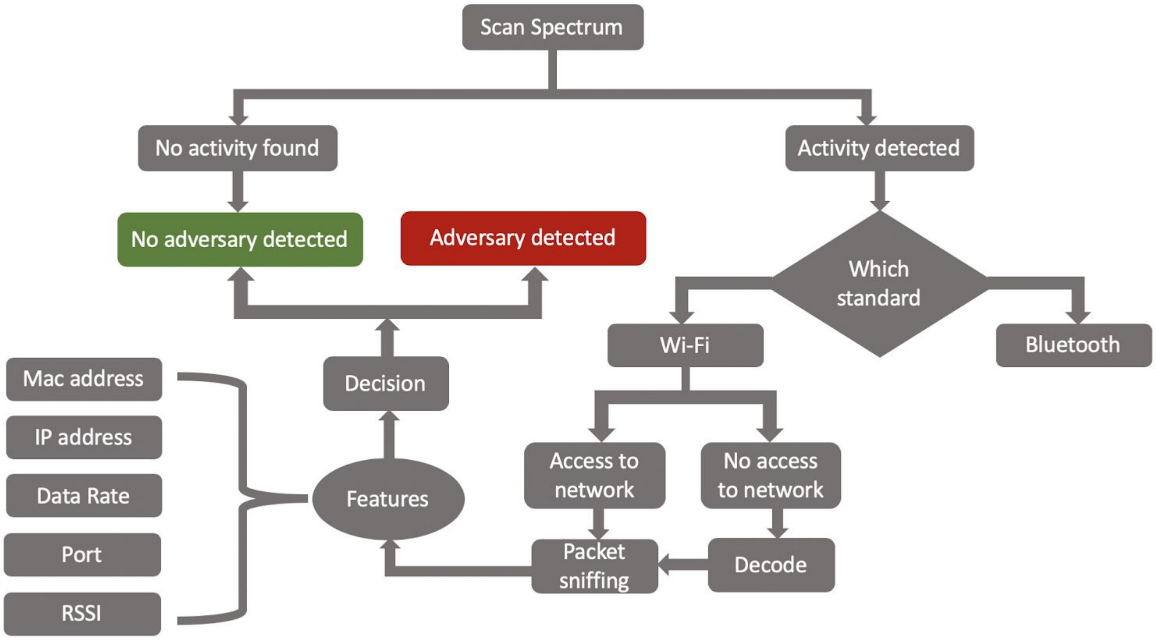
```
No.  Time      Source                Destination             Protoco Length RSSI     Tx Rate Info
 150 4.407932  ArubaAHe_e0:8b:62     Broadcast               802.11   198 6 dBm      6.0    Beacon frame, SN=2808, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 151 4.505469  ArubaAHe_e0:8b:60     Broadcast               802.11   219 6 dBm      6.0    Beacon frame, SN=2809, FN=0, Flags=........, BI=100, SSID=eduroam
 152 4.507627  ArubaAHe_e0:8b:61     Broadcast               802.11   199 5 dBm      6.0    Beacon frame, SN=2810, FN=0, Flags=........, BI=100, SSID=UCLA_WIFI
 153 4.508705  ArubaAHe_e0:8b:62     Broadcast               802.11   198 6 dBm      6.0    Beacon frame, SN=2811, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 154 4.609879  ArubaAHe_e0:8b:61     Broadcast               802.11   199 6 dBm      6.0    Beacon frame, SN=2813, FN=0, Flags=........, BI=100, SSID=UCLA_WIFI
 155 4.610430  ArubaAHe_e0:8b:62     Broadcast               802.11   198 6 dBm      6.0    Beacon frame, SN=2814, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 156 4.712367  ArubaAHe_e0:8b:60     Broadcast               802.11   219 6 dBm      6.0    Beacon frame, SN=2816, FN=0, Flags=........, BI=100, SSID=eduroam
 157 4.713521  ArubaAHe_e0:8b:61     Broadcast               802.11   199 7 dBm      6.0    Beacon frame, SN=2817, FN=0, Flags=........, BI=100, SSID=UCLA_WIFI
 158 4.714543  ArubaAHe_e0:8b:62     Broadcast               802.11   198 6 dBm      6.0    Beacon frame, SN=2818, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 159 4.734831  ArubaAHe_e0:8b:62     Apple_ba:39:48          802.11   183 4 dBm      6.0    Probe Response, SN=2819, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 160 4.915301  ArubaAHe_e0:8b:60     Broadcast               802.11   219 6 dBm      6.0    Beacon frame, SN=2823, FN=0, Flags=........, BI=100, SSID=eduroam
 161 4.916475  ArubaAHe_e0:8b:61     Broadcast               802.11   199 5 dBm      6.0    Beacon frame, SN=2824, FN=0, Flags=........, BI=100, SSID=UCLA_WIFI
 162 5.019994  ArubaAHe_e0:8b:60     Broadcast               802.11   219 5 dBm      6.0    Beacon frame, SN=2826, FN=0, Flags=........, BI=100, SSID=eduroam
 163 5.020208  ArubaAHe_e0:8b:61     Broadcast               802.11   199 7 dBm      6.0    Beacon frame, SN=2827, FN=0, Flags=........, BI=100, SSID=UCLA_WIFI
 164 5.023936  ArubaAHe_e0:8b:62     Broadcast               802.11   198 6 dBm      6.0    Beacon frame, SN=2828, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 165 5.056337  ArubaAHe_e0:8b:62     Apple_ba:39:48          802.11   183 5 dBm      6.0    Probe Response, SN=2829, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 166 5.123593  ArubaAHe_e0:8b:60     Broadcast               802.11   219 7 dBm      6.0    Beacon frame, SN=2830, FN=0, Flags=........, BI=100, SSID=eduroam
 167 5.125166  ArubaAHe_e0:8b:62     Broadcast               802.11   198 8 dBm      6.0    Beacon frame, SN=2832, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 168 5.151510  Apple_ea:8d:1d        GuangLia_83:ba          802.11    41 18 dBm    24.0    Null function (No data), SN=3256, FN=0, Flags=.......T
 169 5.151782                        Apple_ea:8d:1d (b0:…    802.11    27 18 dBm    24.0    Acknowledgement, Flags=........
 170 5.152870                        GuangLia_83:ba (e4:…    802.11    27 16 dBm    24.0    Acknowledgement, Flags=........
 171 5.153546                        GuangLia_83:ba (e4:…    802.11    27 17 dBm    24.0    Acknowledgement, Flags=........
 172 5.154324                        GuangLia_83:ba (e4:…    802.11    27 16 dBm    24.0    Acknowledgement, Flags=........
 173 5.168911  Apple_ea:8d:1d        GuangLia_83:ba          802.11    41 17 dBm    24.0    Null function (No data), SN=3257, FN=0, Flags=...P...T
 174 5.169343                        Apple_ea:8d:1d (b0:…    802.11    27 19 dBm    24.0    Acknowledgement, Flags=........
 175 5.227169  ArubaAHe_e0:8b:60     Broadcast               802.11   219 3 dBm      6.0    Beacon frame, SN=2833, FN=0, Flags=........, BI=100, SSID=eduroam
 176 5.228755  ArubaAHe_e0:8b:62     Broadcast               802.11   198 7 dBm      6.0    Beacon frame, SN=2835, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 177 5.233334  ArubaAHe_e0:8b:62     Apple_d6:ac:85          802.11   183 7 dBm      6.0    Probe Response, SN=2836, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
 178 5.325847  ArubaAHe_e0:8b:60     Broadcast               802.11   219 5 dBm      6.0    Beacon frame, SN=2838, FN=0, Flags=........, BI=100, SSID=eduroam
 179 5.328251  ArubaAHe_e0:8b:62     Broadcast               802.11   198 7 dBm      6.0    Beacon frame, SN=2840, FN=0, Flags=........, BI=100, SSID=UCLA_WEB
```

```
▸ Frame 1: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits)
▸ Radiotap Header v0, Length 17
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........
▸ IEEE 802.11 wireless LAN
```

```
0000  00 00 11 00 6e 08 00 00  00 0c b2 00 00 00 06 00   ····n··· ········
0010  01 80 00 00 00 ff ff ff  ff ff ff 18 64 72 e0 8b   ········ ····dr··
0020  60 18 64 72 e0 8b 60 80  a3 76 d0 5e 6f 7f 00 00   `·dr··`· ·v·^o···
0030  00 64 00 31 14 00 07 65  64 75 72 6f 61 6d 01 08   ·d·1···e duroam··
0040  8c 12 98 24 30 48 60 6c  03 01 01 05 04 00 01 00   ···$0H`l ········
0050  00 2a 01 00 30 14 01 00  00 0f ac 04 01 00 00 0f   ·*··0··· ········
0060  ac 04 01 00 00 0f ac 01  28 00 2d 1a 2d 19 17 ff   ········ (·-·-···
0070  ff ff 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 3d 16  01 08 04 00 00 00 00 00   ······=· ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 4a 0e   ········ ······J·
00a0  14 00 0a 00 2c 01 c8 00  14 00 05 00 19 00 7f 08   ····,··· ········
00b0  05 00 08 00 00 00 00 40  dd 07 00 0b 86 01 04 08   ·······@ ········
00c0  09 dd 18 00 50 f2 02 01  01 80 00 03 a4 00 00 27   ····P··· ·······'
00d0  a4 00 00 42 43 5e 00 62  32 2f 00                  ···BC^·b 2/·
```

simul_cam_usrp.pcap   Packets: 38372 · Displayed: 38372 (100.0%)   Profile: Default

Proposed algorithm for wifi detection

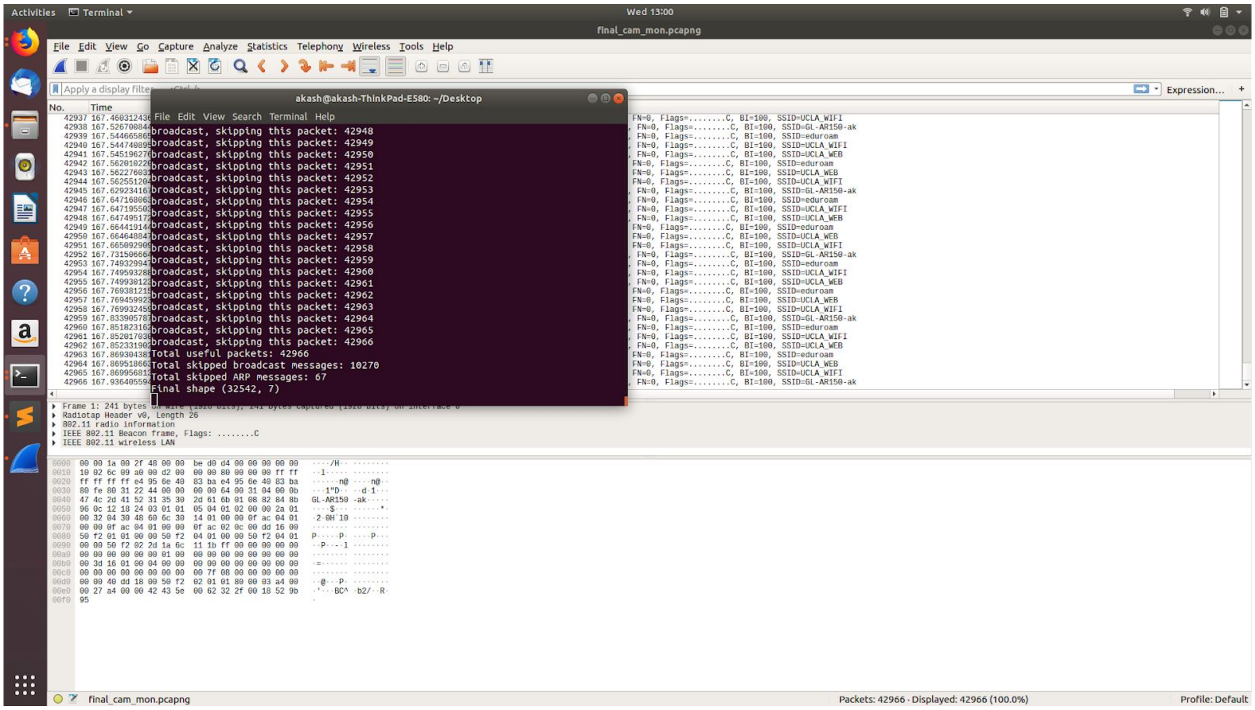


Features:

- **Mac Address:** You can know about the manufacture of a device
- **RSSI:** You can find out if you're moving closer to the device or not
- **Data Rate:** Cannot use this because access points can dynamically adjust their data rate to match channel conditions.
- **Bits sent per packet:** If we sum all bits sent by a particular device over time, we can know about how much traffic it has generated.

The tool:

1. We iterate over all the packets sent and find out how much traffic has been generated by a particular device.
2. Then we plot the transmitter and receiver with highest traffic generated and received.



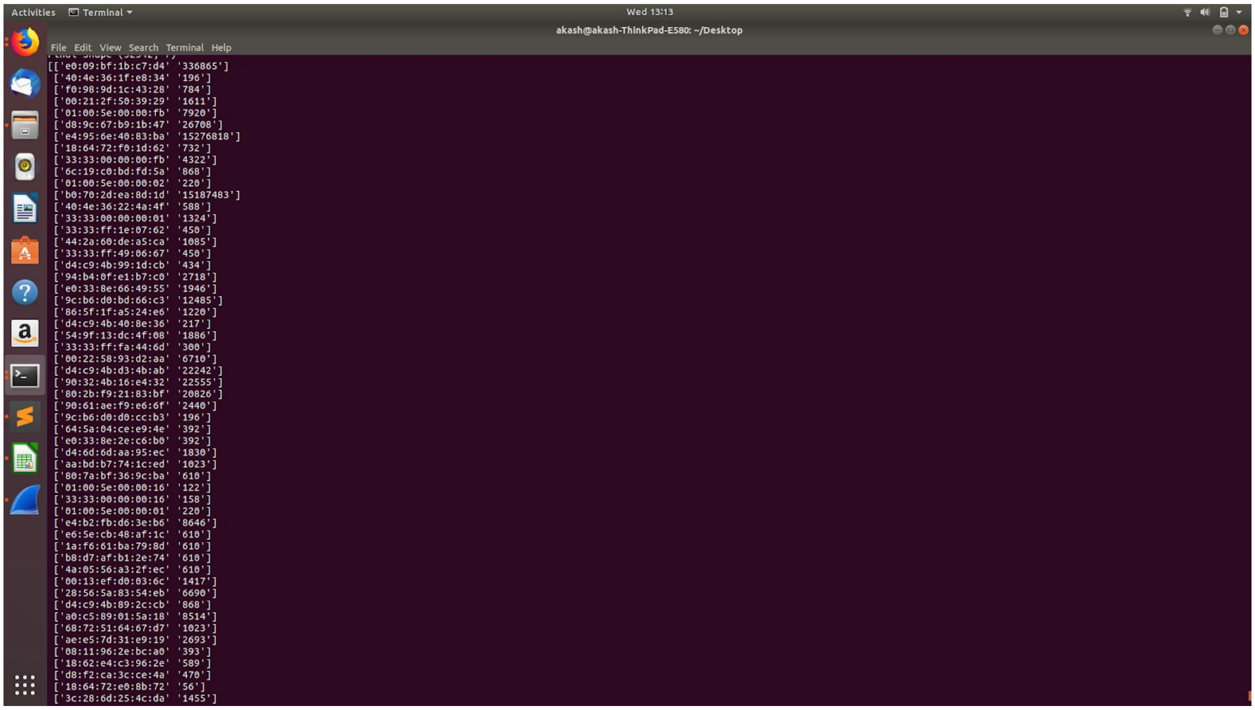
```
broadcast, skipping this packet: 42948
broadcast, skipping this packet: 42949
broadcast, skipping this packet: 42950
broadcast, skipping this packet: 42951
broadcast, skipping this packet: 42952
broadcast, skipping this packet: 42953
broadcast, skipping this packet: 42954
broadcast, skipping this 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

0000  00 00 1a 00 2f 48 00 00  be d0 d4 00 00 00 00 00   ····/H·· ········
0010  10 02 6c 09 a0 00 d2 00  00 00 80 00 00 00 ff ff   ··l····· ········
0020  ff ff ff ff e4 95 6e 40  83 ba e4 95 6e 40 83 ba   ······n@ ····n@··
0030  80 fe 80 31 22 44 00 00  00 00 64 00 31 04 00 0b   ···1"D·· ··d·1···
0040  47 4c 2d 41 52 31 35 30  2d 61 6b 01 08 82 84 8b   GL-AR150 -ak·····
0050  96 0c 12 18 24 03 01 01  05 04 01 02 00 00 2a 01   ····$··· ······*·
0060  00 32 04 30 48 60 6c 30  14 01 00 00 0f ac 04 01   ·2·0H`l0 ········
0070  00 00 0f ac 04 01 00 00  0f ac 02 0c 00 dd 16 00   ········ ········
0080  50 f2 01 01 00 00 50 f2  04 01 00 00 50 f2 04 01   P·····P· ····P···
0090  00 00 50 f2 02 2d 1a 6c  11 1b ff 00 00 00 00 00   ··P··-·l ········
00a0  00 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 3d 16 01 00 04 00 00  00 00 00 00 00 00 00 00   ·=······ ········
00c0  00 00 00 00 00 00 00 00  00 7f 08 00 00 00 00 00   ········ ········
00d0  00 00 40 dd 18 00 50 f2  02 01 01 80 00 03 a4 00   ··@···P· ········
00e0  00 27 a4 00 00 42 43 5e  00 62 32 2f 00 18 52 9b   ·'···BC^ ·b2/··R·
00f0  95                                                 ·
```

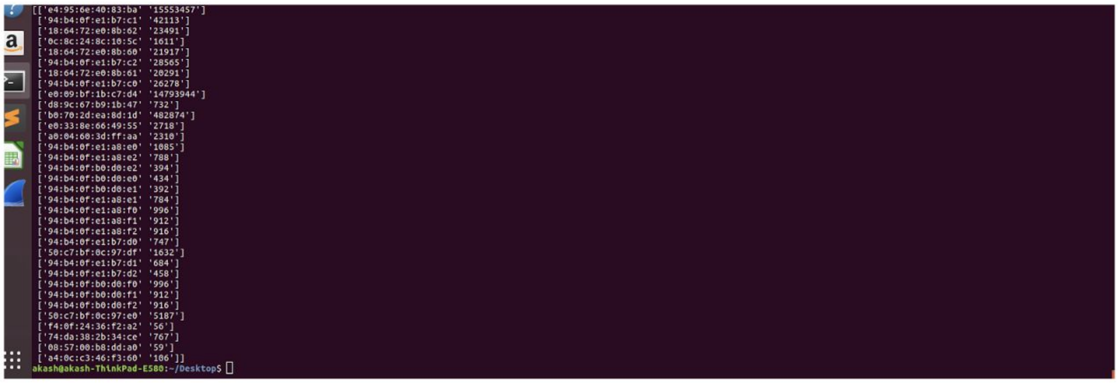
Activities
Terminal
Wed 13:00
final_cam_mon.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter
akash@akash-ThinkPad-E580: ~/Desktop
File Edit View Search Terminal Help
No.
Time
Expression…
final_cam_mon.pcapng
Packets: 42966 · Displayed: 42966 (100.0%)
Profile: Default

3. The list of top transmitters:


Activities
Terminal
Wed 13:13
akash@akash-ThinkPad-E580: ~/Desktop
File Edit View Search Terminal Help

```
[['e0:09:bf:1b:c7:d4' '336865']
 ['40:4e:36:1f:e8:34' '196']
 ['f0:98:9d:1c:43:28' '784']
 ['00:21:2f:50:39:29' '1611']
 ['01:00:5e:00:00:fb' '7920']
 ['d8:9c:67:b9:1b:47' '26708']
 ['e4:95:6e:40:83:ba' '15276818']
 ['18:64:72:f0:1d:62' '732']
 ['33:33:00:00:00:fb' '4322']
 ['6c:19:c0:bd:fd:5a' '868']
 ['01:00:5e:00:00:02' '220']
 ['b0:70:2d:ea:8d:1d' '15187483']
 ['40:4e:36:22:4a:4f' '588']
 ['33:33:00:00:00:01' '1324']
 ['33:33:ff:1e:07:62' '450']
 ['44:2a:60:de:a5:ca' '1085']
 ['33:33:ff:49:06:67' '450']
 ['d4:c9:4b:99:1d:cb' '434']
 ['94:b4:0f:e1:b7:c0' '2718']
 ['e0:33:8e:66:49:55' '1946']
 ['9c:b6:d0:bd:66:c3' '12485']
 ['86:5f:1f:a5:24:e6' '1220']
 ['d4:c9:4b:40:8e:36' '217']
 ['54:9f:13:dc:4f:08' '1886']
 ['33:33:ff:fa:44:6d' '300']
 ['00:22:58:93:d2:aa' '6710']
 ['d4:c9:4b:d3:4b:ab' '22242']
 ['90:32:4b:16:e4:32' '22555']
 ['80:2b:f9:21:83:bf' '20826']
 ['90:61:ae:f9:e6:6f' '2440']
 ['9c:b6:d0:d0:cc:b3' '196']
 ['64:5a:04:ce:e9:4e' '392']
 ['e0:33:8e:2e:c6:b0' '392']
 ['d4:6d:6d:aa:95:ec' '1830']
 ['aa:bd:b7:74:1c:ed' '1023']
 ['80:7a:bf:36:9c:ba' '610']
 ['01:00:5e:00:00:16' '122']
 ['33:33:00:00:00:16' '158']
 ['01:00:5e:00:00:01' '220']
 ['e4:b2:fb:d6:3e:b6' '8646']
 ['e6:5e:cb:48:af:1c' '610']
 ['1a:f6:61:ba:79:8d' '610']
 ['b8:d7:af:b1:2e:74' '610']
 ['4a:05:56:a3:2f:ec' '610']
 ['00:13:ef:d0:03:6c' '1417']
 ['28:56:5a:83:54:eb' '6690']
 ['d4:c9:4b:89:2c:cb' '868']
 ['a0:c5:89:01:5a:18' '8514']
 ['68:72:51:64:67:d7' '1023']
 ['ae:e5:7d:31:e9:19' '2693']
 ['08:11:96:2e:bc:a0' '393']
 ['18:62:e4:c3:96:2e' '589']
 ['d8:f2:ca:3c:ce:4a' '470']
 ['18:64:72:e0:8b:72' '56']
 ['3c:28:6d:25:4c:da' '1455']
```

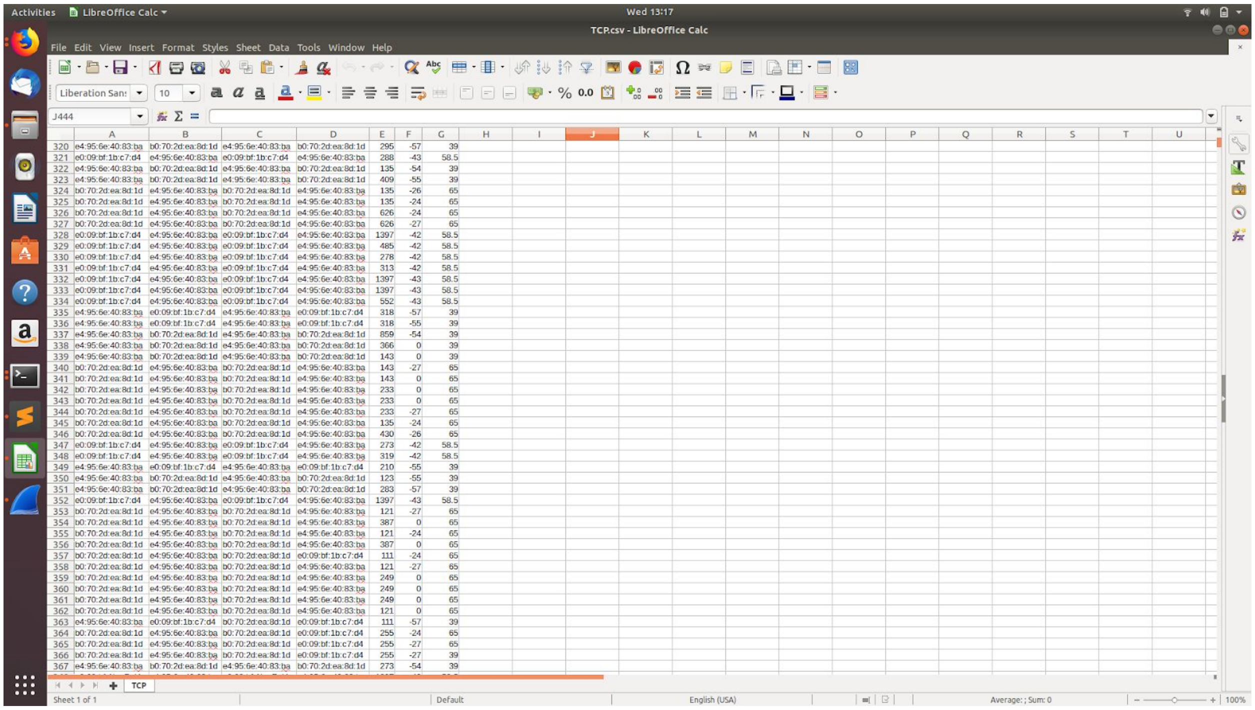
4. The list of top receivers:



```
[['e4:95:6e:40:83:ba' '15553457']
 ['94:b4:0f:e1:b7:c1' '42113']
 ['18:64:72:e0:8b:62' '23491']
 ['0c:8c:24:8c:10:5c' '1611']
 ['18:64:72:e0:8b:60' '21917']
 ['94:b4:0f:e1:b7:c2' '28565']
 ['18:64:72:e0:8b:61' '20291']
 ['94:b4:0f:e1:b7:c0' '26278']
 ['e0:09:bf:1b:c7:d4' '14793944']
 ['d8:9c:67:b9:1b:47' '732']
 ['b0:70:2d:ea:8d:1d' '482874']
 ['e0:33:8e:66:49:55' '2718']
 ['a0:04:60:3d:ff:aa' '2310']
 ['94:b4:0f:e1:a8:e0' '1085']
 ['94:b4:0f:e1:a8:e2' '788']
 ['94:b4:0f:b0:d0:e2' '394']
 ['94:b4:0f:b0:d0:e0' '434']
 ['94:b4:0f:b0:d0:e1' '392']
 ['94:b4:0f:e1:a8:e1' '784']
 ['94:b4:0f:e1:a8:f0' '996']
 ['94:b4:0f:e1:a8:f1' '912']
 ['94:b4:0f:e1:a8:f2' '916']
 ['94:b4:0f:e1:b7:d0' '747']
 ['50:c7:bf:0c:97:df' '1632']
 ['94:b4:0f:e1:b7:d1' '684']
 ['94:b4:0f:e1:b7:d2' '458']
 ['94:b4:0f:b0:d0:f0' '996']
 ['94:b4:0f:b0:d0:f1' '912']
 ['94:b4:0f:b0:d0:f2' '916']
 ['50:c7:bf:0c:97:e0' '5187']
 ['f4:0f:24:36:f2:a2' '56']
 ['74:da:38:2b:34:ce' '767']
 ['08:57:00:b8:dd:a0' '59']
 ['a4:0c:c3:46:f3:60' '106']]
akash@akash-ThinkPad-E580:~/Desktop$ 
```

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

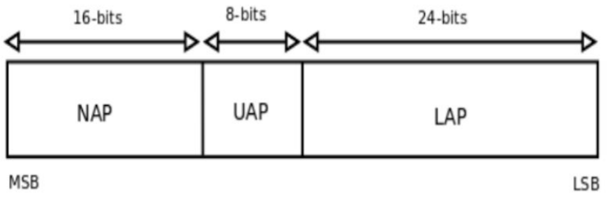
5. We also save these statistics to a csv file:



	A	B	C	D	E	F	G
320	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	295	-57	39
321	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	288	-43	58.5
322	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	135	-54	39
323	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	409	-55	39
324	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	135	-26	65
325	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	135	-24	65
326	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	626	-24	65
327	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	626	-27	65
328	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	1397	-42	58.5
329	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	485	-42	58.5
330	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	278	-42	58.5
331	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	313	-42	58.5
332	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	1397	-43	58.5
333	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	1397	-43	58.5
334	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	552	-43	58.5
335	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	318	-57	39
336	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	318	-55	39
337	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	859	-54	39
338	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	366	0	39
339	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	143	0	39
340	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	143	-27	65
341	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	143	0	65
342	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	233	0	65
343	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	233	0	65
344	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	233	-27	65
345	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	135	-24	65
346	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	430	-26	65
347	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	273	-42	58.5
348	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	319	-42	58.5
349	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	210	-55	39
350	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	123	-55	39
351	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	283	-57	39
352	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	e4:95:6e:40:83:ba	1397	-43	58.5
353	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	121	-27	65
354	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	387	0	65
355	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	121	-24	65
356	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	387	0	65
357	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:d4	111	-24	65
358	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	121	-27	65
359	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	249	0	65
360	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	249	0	65
361	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	249	0	65
362	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	121	0	65
363	e4:95:6e:40:83:ba	e0:09:bf:1b:c7:d4	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:d4	111	-57	39
364	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:d4	255	-24	65
365	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:d4	255	-27	65
366	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:d4	255	-27	39
367	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:ba	b0:70:2d:ea:8d:1d	273	-54	39

Bluetooth Sniffing

Bluetooth Address - 48 bits



The three parts of a Bluetooth MAC address.

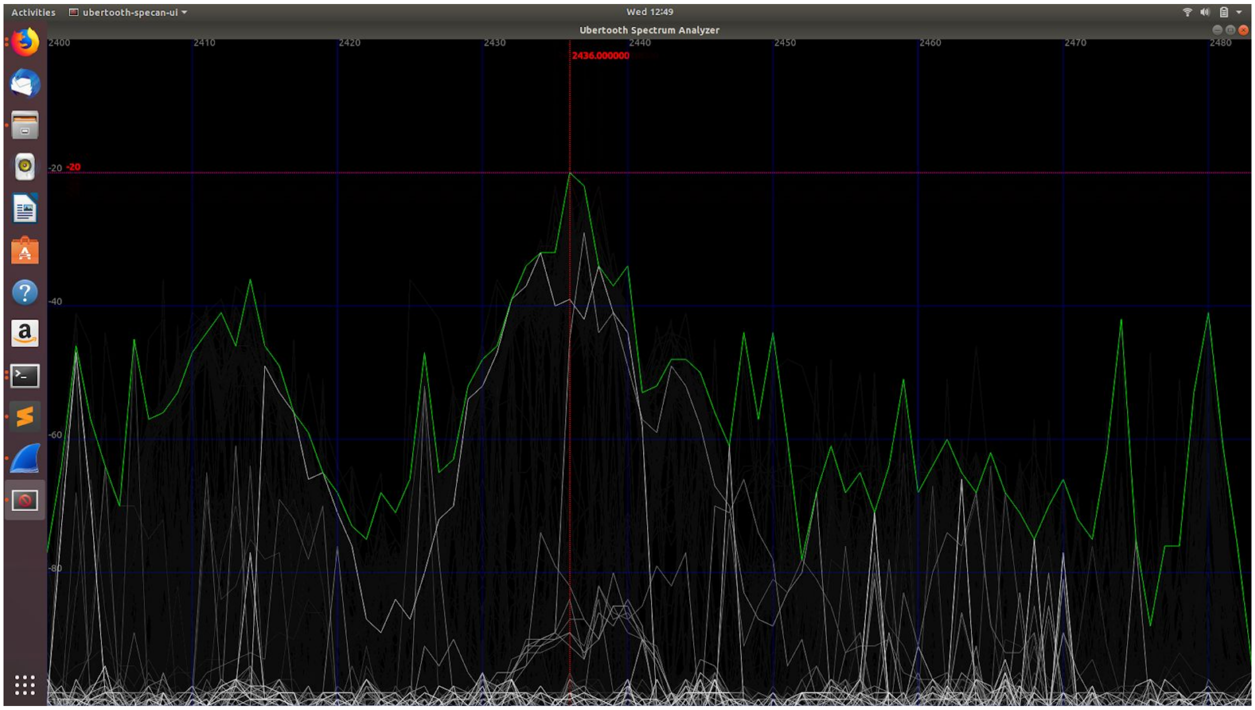
- LAP: Lower Address Part -> Transmitted with every packet
- Upper Address Part -> Only transmitted during handshake
- Non significant Address Part -> ignored during initial connection

79 channels of 1 MHz each

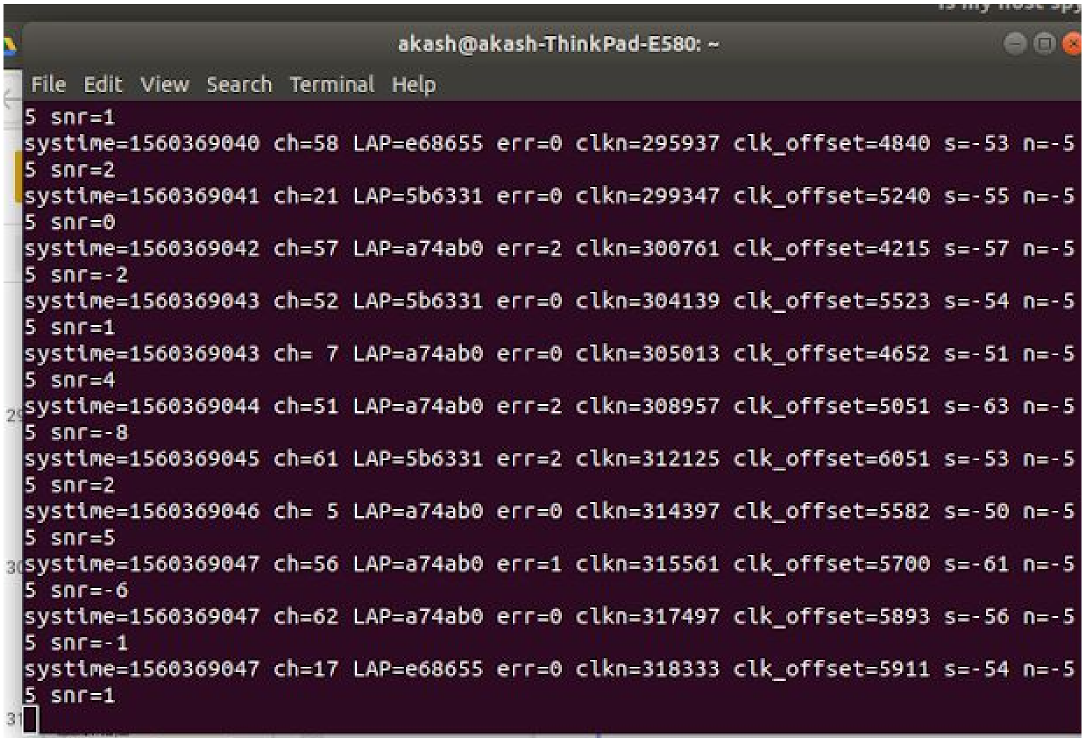
1600 hops a second in pseudo random manner

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

1. We use Ubertooth One to scan the spectrum for Bluetooth transmissions:

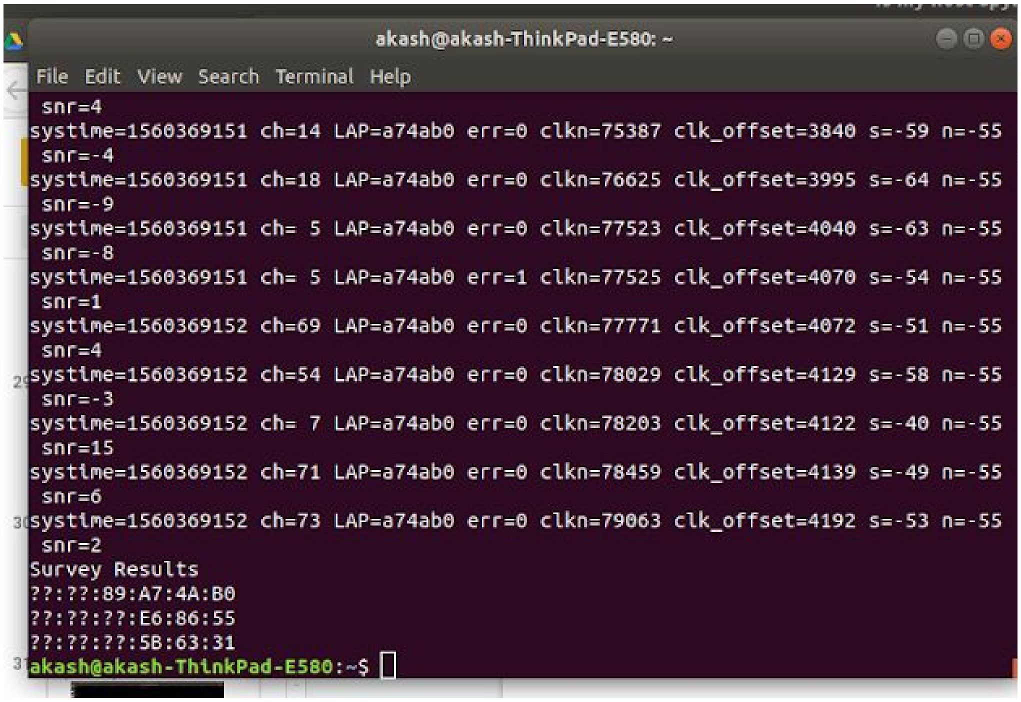


2. If a transmission is found, we passive listen to all Bluetooth packets being sent:


akash@akash-ThinkPad-E580: ~
File Edit View Search Terminal Help

```
5 snr=1
systime=1560369040 ch=58 LAP=e68655 err=0 clkn=295937 clk_offset=4840 s=-53 n=-5
5 snr=2
systime=1560369041 ch=21 LAP=5b6331 err=0 clkn=299347 clk_offset=5240 s=-55 n=-5
5 snr=0
systime=1560369042 ch=57 LAP=a74ab0 err=2 clkn=300761 clk_offset=4215 s=-57 n=-5
5 snr=-2
systime=1560369043 ch=52 LAP=5b6331 err=0 clkn=304139 clk_offset=5523 s=-54 n=-5
5 snr=1
systime=1560369043 ch= 7 LAP=a74ab0 err=0 clkn=305013 clk_offset=4652 s=-51 n=-5
5 snr=4
systime=1560369044 ch=51 LAP=a74ab0 err=2 clkn=308957 clk_offset=5051 s=-63 n=-5
5 snr=-8
systime=1560369045 ch=61 LAP=5b6331 err=2 clkn=312125 clk_offset=6051 s=-53 n=-5
5 snr=2
systime=1560369046 ch= 5 LAP=a74ab0 err=0 clkn=314397 clk_offset=5582 s=-50 n=-5
5 snr=5
systime=1560369047 ch=56 LAP=a74ab0 err=1 clkn=315561 clk_offset=5700 s=-61 n=-5
5 snr=-6
systime=1560369047 ch=62 LAP=a74ab0 err=0 clkn=317497 clk_offset=5893 s=-56 n=-5
5 snr=-1
systime=1560369047 ch=17 LAP=e68655 err=0 clkn=318333 clk_offset=5911 s=-54 n=-5
5 snr=1
```

3. Then we enter a survey mode and find BR address all devices that are transmitting:


akash@akash-ThinkPad-E580: ~
File Edit View Search Terminal Help

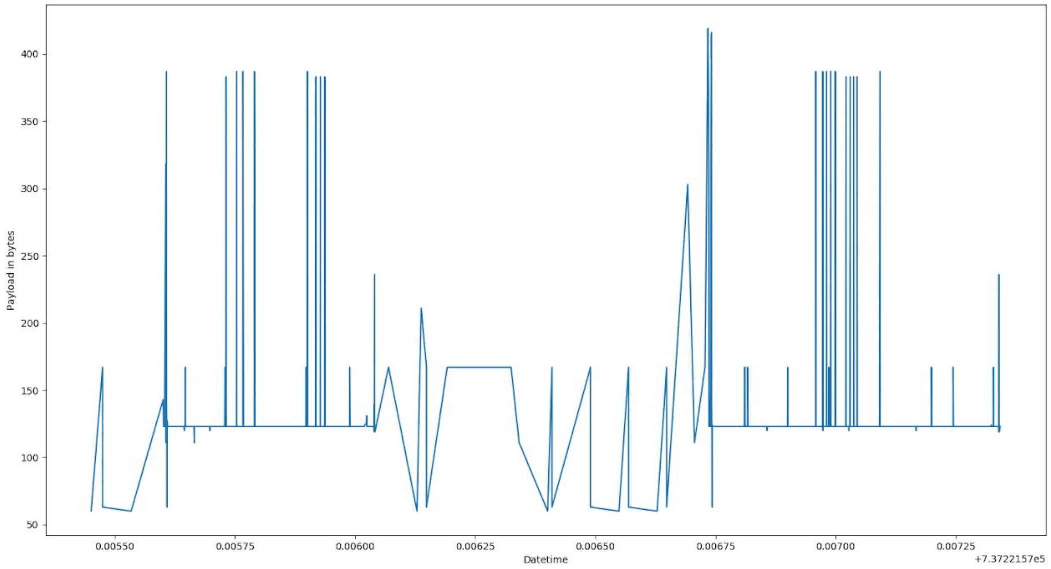
```
 snr=4
systime=1560369151 ch=14 LAP=a74ab0 err=0 clkn=75387 clk_offset=3840 s=-59 n=-55
 snr=-4
systime=1560369151 ch=18 LAP=a74ab0 err=0 clkn=76625 clk_offset=3995 s=-64 n=-55
 snr=-9
systime=1560369151 ch= 5 LAP=a74ab0 err=0 clkn=77523 clk_offset=4040 s=-63 n=-55
 snr=-8
systime=1560369151 ch= 5 LAP=a74ab0 err=1 clkn=77525 clk_offset=4070 s=-54 n=-55
 snr=1
systime=1560369152 ch=69 LAP=a74ab0 err=0 clkn=77771 clk_offset=4072 s=-51 n=-55
 snr=4
systime=1560369152 ch=54 LAP=a74ab0 err=0 clkn=78029 clk_offset=4129 s=-58 n=-55
 snr=-3
systime=1560369152 ch= 7 LAP=a74ab0 err=0 clkn=78203 clk_offset=4122 s=-40 n=-55
 snr=15
systime=1560369152 ch=71 LAP=a74ab0 err=0 clkn=78459 clk_offset=4139 s=-49 n=-55
 snr=6
systime=1560369152 ch=73 LAP=a74ab0 err=0 clkn=79063 clk_offset=4192 s=-53 n=-55
 snr=2
Survey Results
??:??:89:A7:4A:B0
??:??:??:E6:86:55
??:??:??:5B:63:31
akash@akash-ThinkPad-E580:~$
```

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
- The 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:

Suppose you buy a device and you want to monitor when it is active, you can use our tool to plot its statistics over time like the one shown below:



References:

1. Staff, SSI. “Smart Home Devices Market Forecast to Be Growing Globally at 31% Annual Clip.” *Security Sales & Integration*, Security Sales & Integration, 2 Oct. 2018, www.securitysales.com/research/smart-home-devices-market-forecast/.

2. Cisco, V. N. I. "Cisco Visual Networking Index: Forecast and Trends, 2017–2022." White Paper (2018).
3. “New Wireless Technologies Create More Agility and Security.” *MTM Technologies*, 12 June 2019, www.mtm.com/new-wireless-technologies-creating-agility-security/.
4. Heater, Brian, and Brian Heater. “Amazon Upgrades Its Blink Outdoor Security Camera with Better Battery, Two-Way Talk.” *TechCrunch*, TechCrunch, 8 May 2019, techcrunch.com/2019/05/08/amazon-upgrades-its-blink-outdoor-security-camera-with-better-battery-two-way-talk/.
5. Antonakakis, Manos, et al. "Understanding the mirai botnet." 26th {USENIX} Security Symposium ({USENIX} Security 17). 2017.
6. Fussell, Sidney. “Airbnb Has a Hidden-Camera Problem.” The Atlantic, Atlantic Media Company, 26 Mar. 2019, www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/.
7. Jeong, Sophie, and James Griffiths. “Hundreds of South Korean Motel Guests Were Secretly Filmed and Live-Streamed Online.” *CNN*, Cable News Network, 21 Mar. 2019, www.cnn.com/2019/03/20/asia/south-korea-hotel-spy-cam-intl/index.html.
8. Staff, Inside Edition. “Couple Says They Found Hidden Camera Pointing at Their Bed in Carnival Cruise Room.” *Inside Edition*, Inside Edition, 26 Oct. 2018, www.insideedition.com/couple-says-they-found-hidden-camera-pointing-their-bed-carnival-cruise-room-47948.
9. Apthorpe, Noah, Dillon Reisman, and Nick Feamster. "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic." *arXiv preprint arXiv:1705.06805* (2017).
10. Apthorpe, Noah, Dillon Reisman, and Nick Feamster. "Closing the blinds: Four strategies for protecting smart home privacy from network observers." *arXiv preprint arXiv:1705.06809*(2017)