

# Is my host spying on me?

Akash Deep Singh





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

Live TV • U.S. Edit



World » Africa | Americas | Asia | Australia | China | Europe | Middle East | India | UK



# 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



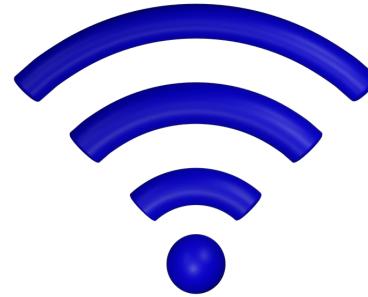
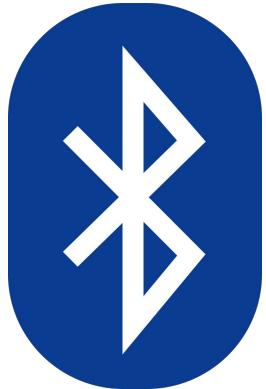
# AirBnB policies on surveillance for hosts

- 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.

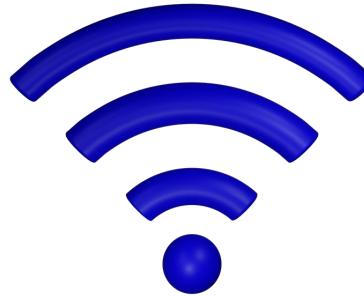
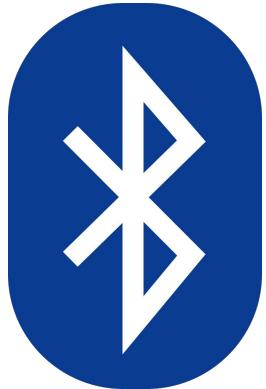
# AirBnB policies on surveillance for guests

- 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”



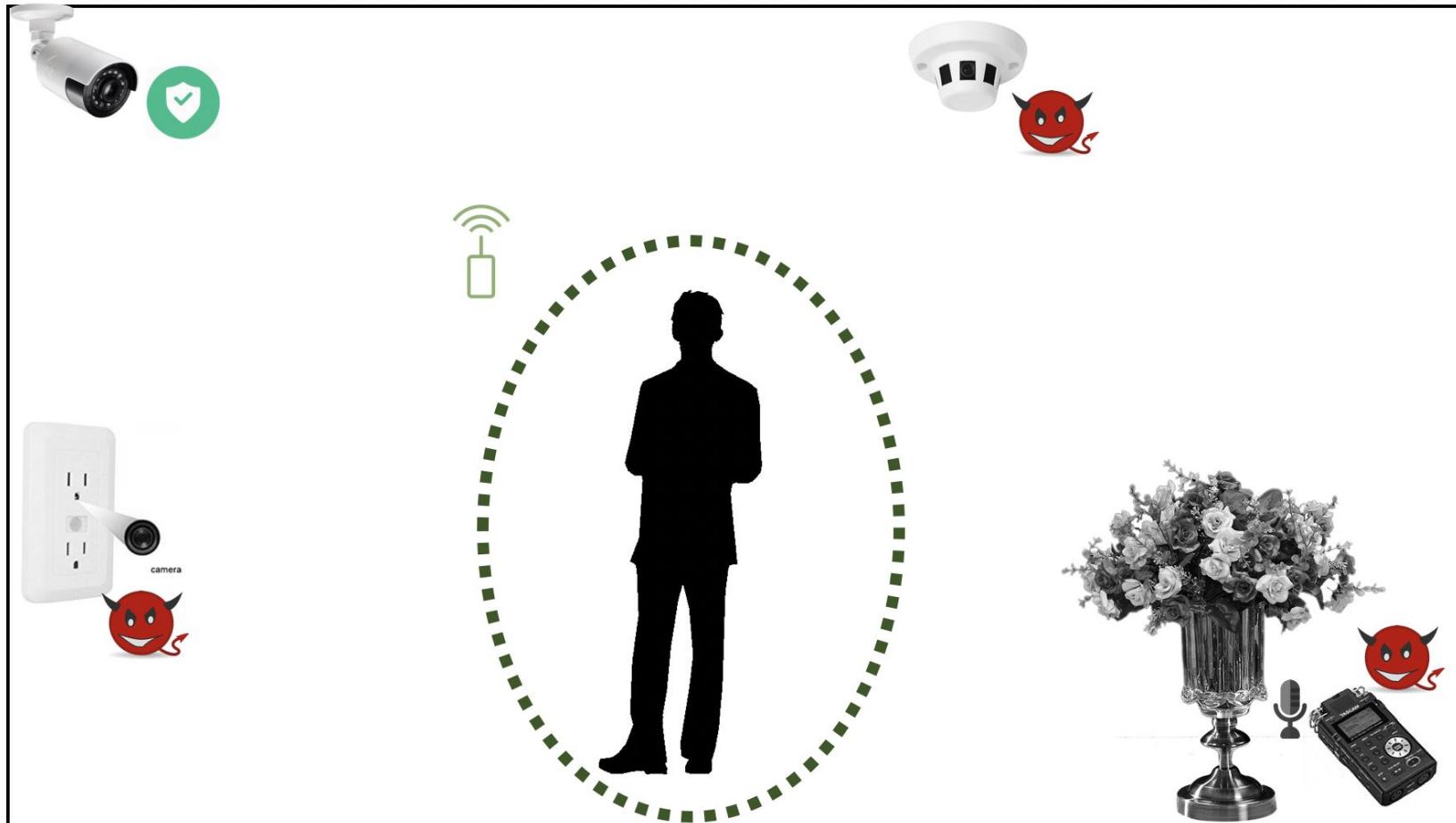
**zigbee**



zigbee

# 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.



# 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

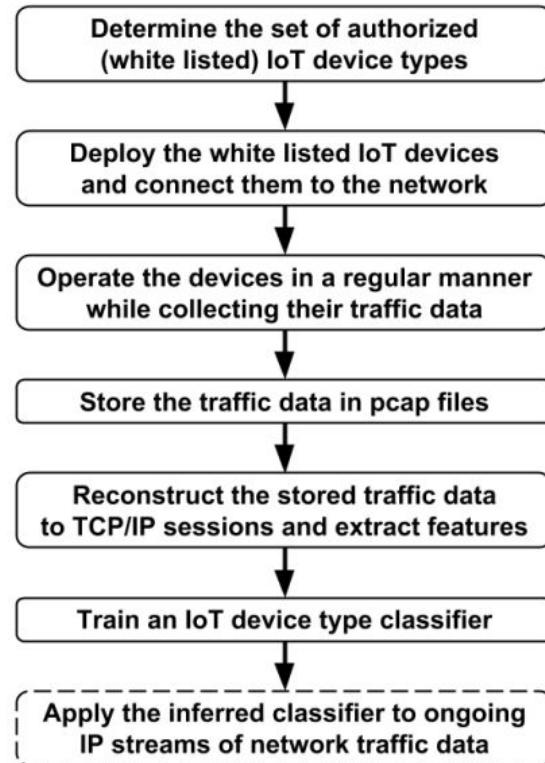


From IoT-Inspector website

# IoT Inspector works through ARP-spoofing



# Detection of Unauthorized IoT Devices Using Machine Learning Techniques

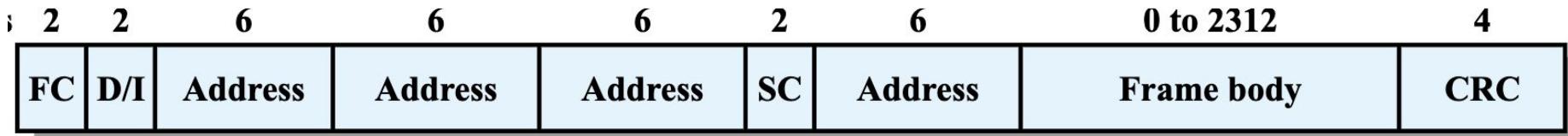


WiFi

# 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".

Frame Control: Data frame, from STA to DS (to AP)	Duration	Receiver address (MAC of AP)	Transmitter address (MAC of source STA)
08 01	30 00	e4 ce 8f 66 b2 42	e4 ce 8f 5b a1 f6
Destination address (MAC of dest. STA)	e4 ce 8f 5a 0c 5e	f0 00	aa aa 03 00 00 00 08 00
Sequence control	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 body

RAW Hex Dump

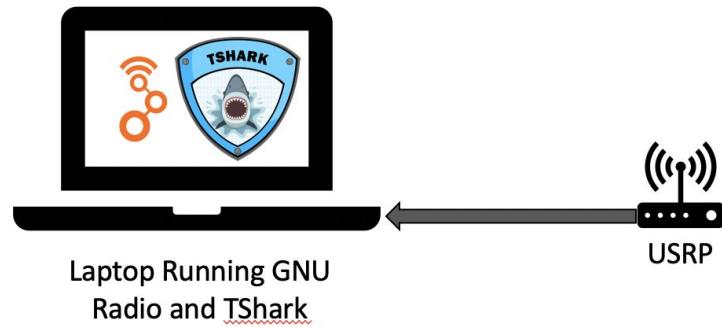
Frame Control: Control frame type, ACK subtype	Duration	Receiver address (TX MAC of frame that is being acknowledged)
d4 00	00 00	e4 ce 8f 5b a1 f6

<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



# Packet Sniffing in managed mode

Activities Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl/>

final\_no\_cam\_eth.pcapng

Wed 12:42

No. Time Source Destination Proto Length RSSI Tx Rate Info

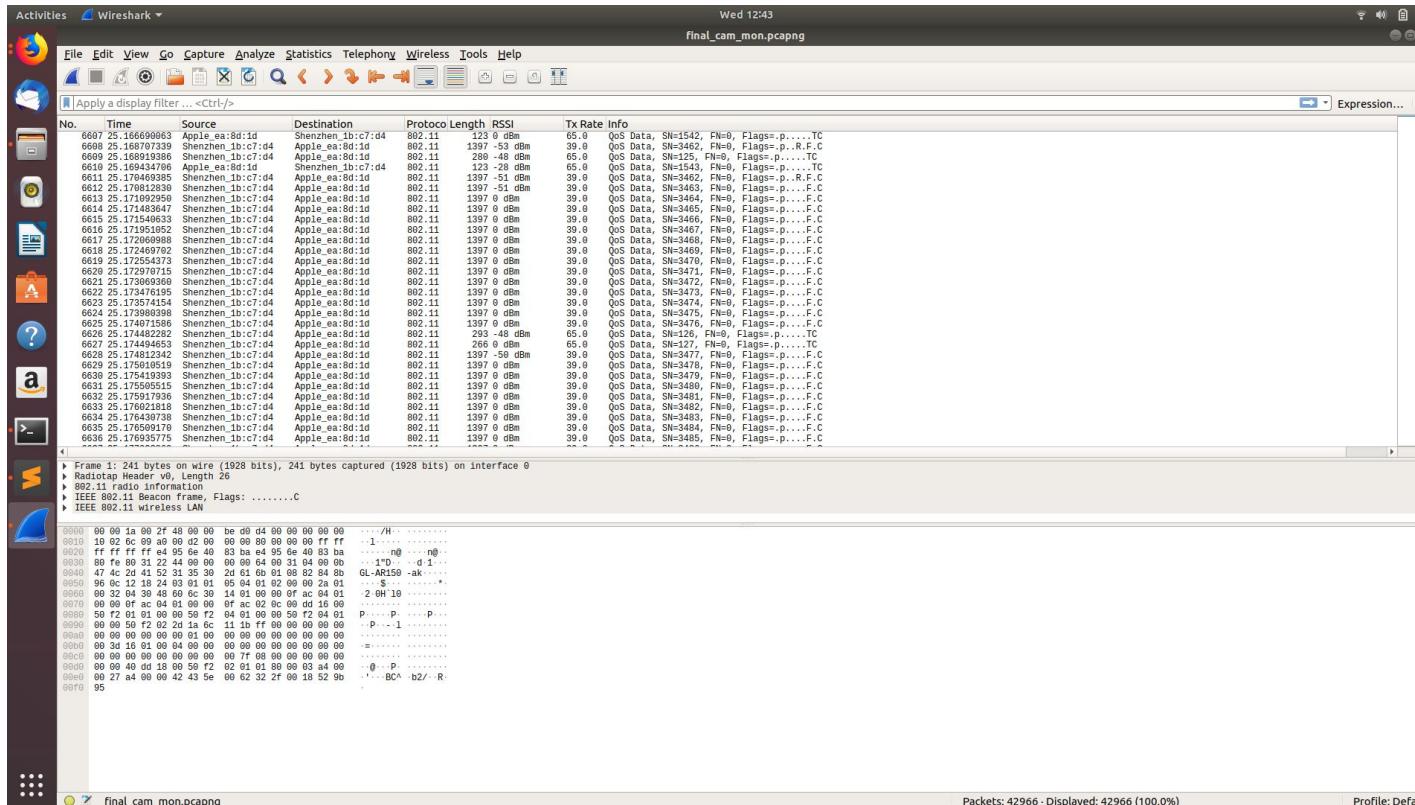
No.	Time	Source	Destination	Proto	Length	RSSI	Tx Rate Info
1	8.000685000	192.168.8.133	264.102.114.56	TCP	66	-68	58412 - 80 [ACK] Seq=1 Ack=1 Win=34 Len=8 Tsvl=165302241 TSer=468644678
2	8.000685000	192.168.8.133	264.102.114.56	TCP	66	-68	[TCP ACK Dup] Seq=1 Ack=1 Win=34 Len=8 Tsvl=165302241 TSer=468644678
3	8.000685000	192.168.8.134	264.102.114.56	TCP	66	-68	[TCP ACK Dup ACK 1w1] 58412 - 80 [ACK] Seq=1 Ack=1 Win=34 Len=8 Tsvl=165302241 TSer=468644678
4	8.000685000	192.168.8.134	264.102.114.56	TCP	66	-68	[TCP ACK Dup ACK 2w1] 58412 - 80 [ACK] Seq=1 Ack=1 Win=34 Len=8 Tsvl=165302241 TSer=468644678
5	14.049237238	fd06:1007:0:0:0:0:0:0:87::ff02::fb	MDNS	203	-68	Standard query 0x0000 PTR _ippss._tcp.local, "QM" question PTR _ftp._tcp.local, "QM" question PTR _webdav._tcp.local, "QM" question PTR _webdavs._tcp.local, "QM" question PTR _sntp._tcp.local, "QM" question PTR _tftp._tcp.local, "QM" question PTR _webdav._tcp.local, "QM" question PTR _webdavs._tcp.local, "QM" question OPT	
6	14.049237238	fd06:1007:0:0:0:0:0:0:87::ff02::fb	MDNS	112	-68	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT	
7	15.545499116	192.168.8.133	224.0.0.251	MDNS	112	-68	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
8	15.954419682	192.168.8.133	224.0.0.2	ICMPv2	46	-68	Leave Group 224.0.0.251
9	15.954419682	192.168.8.133	224.0.0.251	ICMPv2	46	-68	Membership Report group 224.0.0.251
10	15.954419682	192.168.8.133	224.0.0.251	ICMPv6	86	-68	Multicast Listener Done
11	16.168755460	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Done	
12	16.168755460	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Report	
13	16.168755460	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Report	
14	16.569223114	192.168.8.133	224.0.0.251	MDNS	112	-68	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
15	16.569223114	192.168.8.133	224.0.0.251	MDNS	112	-68	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
16	17.183567839	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Report	
17	18.207555959	fe80::e695:6eff:fe..ff02::1	ICMPv6	86	-68	Multicast Listener Query	
18	18.207555959	fe80::e695:6eff:fe..ff02::1	ICMPv6	86	-68	Standard query 0x0000 PTR _homekit._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question OPT	
19	18.207555959	fe80::e695:6eff:fe..ff02::1	ICMPv6	86	-68	Standard query 0x0000 PTR _homekit._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question OPT	
20	19.1991694	fe80::1c6b:db04:bcf..ff02::1:ffff:addr:ad33	ICMPv6	86	-68	Multicast Listener Report	
21	19.232877808	fe80::1c6b:db04:bcf..ff02::1:ffff:addr:446d	ICMPv6	86	-68	Multicast Listener Report	
22	19.436788514	192.168.8.133	224.0.0.251	MDNS	130	-68	Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question OPT
23	19.440912890	192.168.8.133	224.0.0.251	MDNS	130	-68	Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question OPT
24	19.441693240	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Report	
25	20.255423569	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Report	
26	20.255423569	fe80::1c6b:db04:bcf..ff02::fb	ICMPv6	86	-68	Multicast Listener Report	
27	20.257897048	fe80::1c6b:db04:bcf..ff02::2:ffff:667	ICMPv6	86	-68	Multicast Listener Report	

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: HonHaiPc\_21:83:bf (80:20:f9:21:83:bf), Dst: Guanglia\_83:ba (e4:95:6e:40:83:ba)  
Internet Protocol Version 4, Src: 192.168.8.134, Dst: 264.102.114.56  
Transmission Control Protocol, Src Port: 58412, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

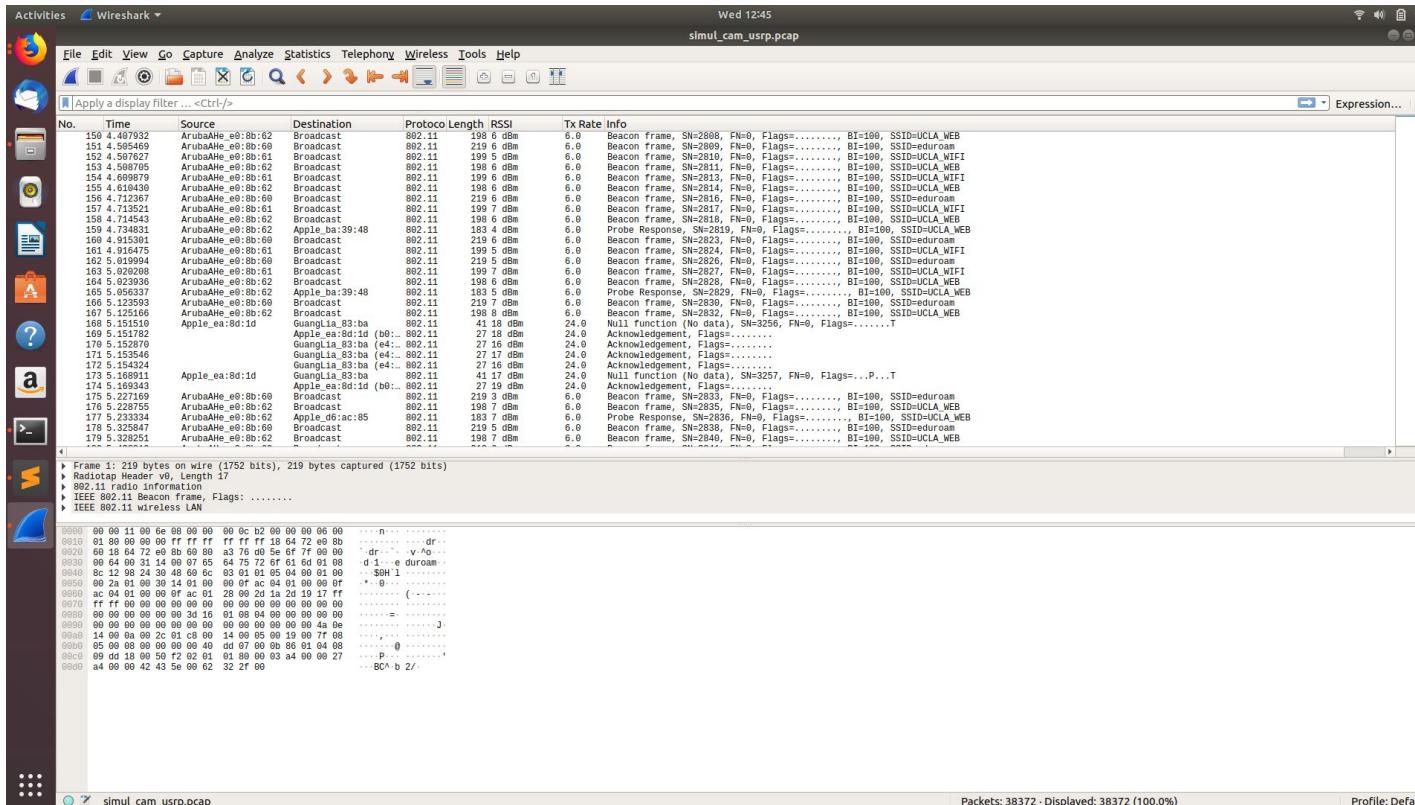
0000 e4 95 6e 40 83 ba 80 2b f9 21 83 bf 08 00 45 00 n0 + :! E:  
0010 00 34 45 10 40 00 90 66 ed e6 c9 a8 08 66 cc 66 4E 0 0 .....T  
0020 72 38 e4 2c 00 50 39 ce 9c ad d2 62 a8 04 80 10 r8 , p9 ..b...  
0030 69 22 b2 d1 00 00 01 01 08 0a 09 54 6e 74 bb ee . = ..Tnt:  
0040 f2 15 ..

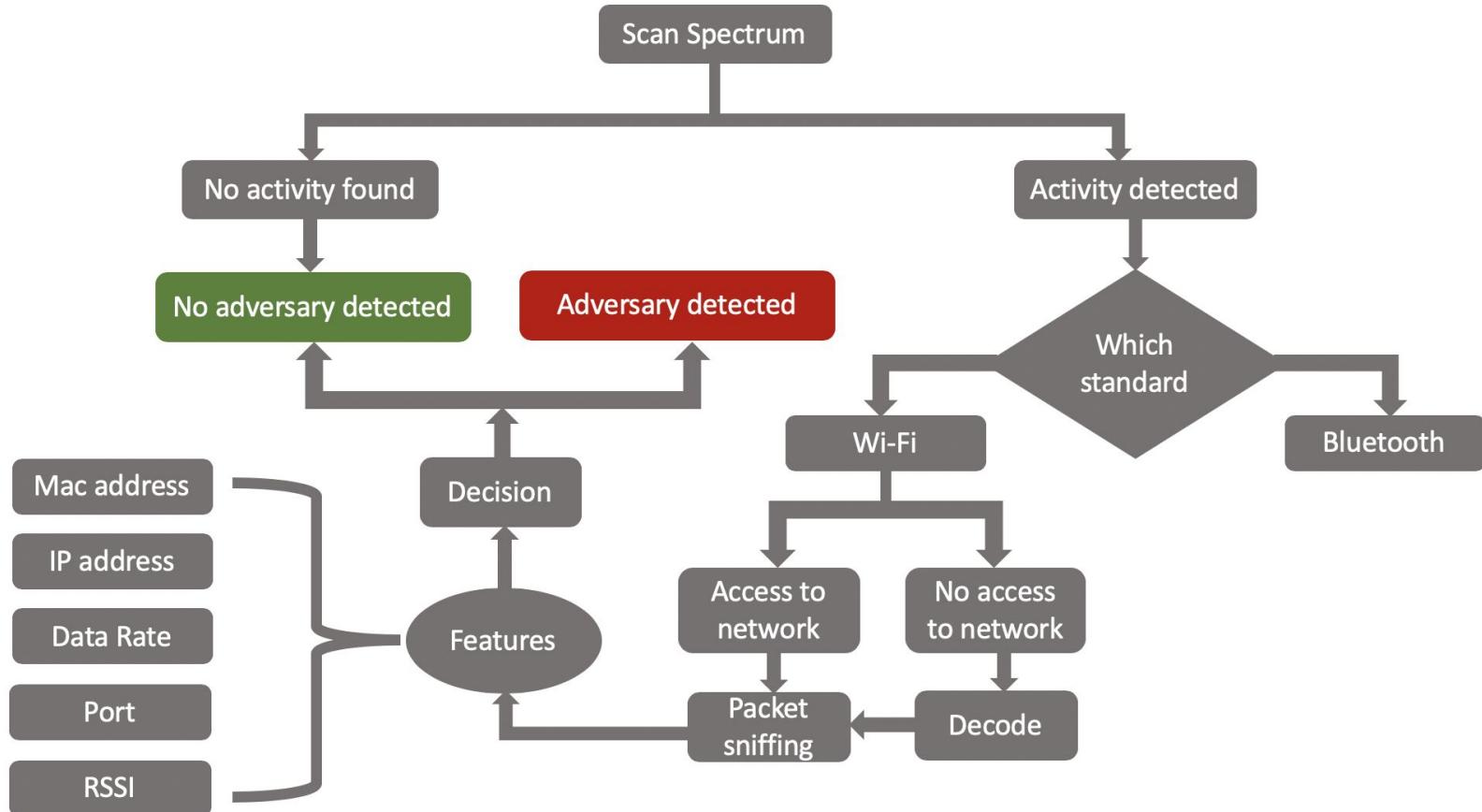
Packets: 57 · Displayed: 57 (100.0%) Profile: Default

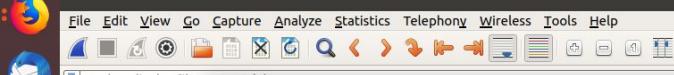
# Packet sniffing in monitor mode



# Packet sniffing using USRP







Apply a display filter... ▾ Expression... +

akash@akash-ThinkPad-E580: ~/Desktop

```
No. Time File Edit View Search Terminal Help
42937 167.460312436 broadcast, skipping this packet: 42948
42938 167.526709844 broadcast, skipping this packet: 42949
42939 167.544665896 broadcast, skipping this packet: 42950
42940 167.545193776 broadcast, skipping this packet: 42951
42941 167.562276062 broadcast, skipping this packet: 42952
42944 167.562551264 broadcast, skipping this packet: 42953
42945 167.647168863 broadcast, skipping this packet: 42954
42946 167.647195583 broadcast, skipping this packet: 42955
42947 167.647495172 broadcast, skipping this packet: 42956
42948 167.664419144 broadcast, skipping this packet: 42957
42951 167.664648847 broadcast, skipping this packet: 42958
42953 167.731382909 broadcast, skipping this packet: 42959
42953 167.731382994 broadcast, skipping this packet: 42959
42954 167.740503288 broadcast, skipping this packet: 42960
42955 167.74930123 broadcast, skipping this packet: 42961
42956 167.769381218 broadcast, skipping this packet: 42962
42957 167.769459923 broadcast, skipping this packet: 42963
42958 167.833965789 broadcast, skipping this packet: 42964
42961 167.852617836 broadcast, skipping this packet: 42965
42961 167.852617836 broadcast, skipping this packet: 42966
42963 167.885943438 Total useful packets: 42966
42964 167.890518685 Total skipped broadcast messages: 10270
42965 167.890956818 Total skipped ARP messages: 67
42966 167.93640559 Final shape (32542, 7)
```

```
Frame 1: 241 bytes on wire (1920 bits), 242 bytes captured (1920 bits) on interface 0
Radiotap Header v0, Length 26
  IEEE 802.11 radio information
    IEEE 802.11 Beacon frame, Flags: .....
    IEEE 802.11 wireless LAN
```

0000	00	00	10	00	2f	48	00	00	be	d0	d4	00	00	00	00	00	/H
0019	10	02	66	09	a6	09	d2	00	00	00	88	00	00	00	ff	ff	
0029	ff	ff	ff	f4	95	6e	40	83	ba	e4	95	6e	40	83	ba	.n@.....n@..	
0030	88	fe	80	31	22	44	00	00	00	64	00	31	04	00	00	.1"D ..d 1..	
0049	47	4c	2d	41	52	31	35	2d	61	6b	01	08	82	84	8b	GL-AR150 -ak..	
0050	96	0c	12	18	24	03	01	05	04	01	02	00	00	2a	01	..\$.....*	
0069	09	32	04	39	48	63	6c	30	14	01	00	00	07	ac	04	01	
0069	09	32	04	39	48	63	6c	30	14	01	00	00	07	ac	04	01	
0069	09	32	04	39	48	63	6c	30	14	01	00	00	07	ac	04	01	
0069	59	00	01	04	61	65	60	00	00	00	00	00	00	00	00	00	
0069	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0069	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0069	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0069	00	3d	16	01	08	04	00	00	00	00	00	00	00	00	00	=.....	
0069	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0069	00	00	40	dd	18	00	50	f2	02	01	01	00	00	03	a4	00	
0069	00	27	a4	00	00	42	c3	5e	00	62	32	2f	00	18	52	9b	
0069	95																

# Top Tx

```
Activities Terminal Wed 13:13
akash@akash-ThinkPad-E580: ~/Desktop

File Edit View Search Terminal Help
[[{"e8:09:bf:1:b:c7:d4": "336865"}, {"40:a:e36:1:f:e8:34": "196"}, {"f6:98:9d:1:c:43:28": "784"}, {"06:21:2f:50:39:29": "1611"}, {"01:00:5e:00:00:fb": "7920"}, {"d8:9c:67:b9:1b:47": "26798"}, {"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"}, {"b6:70:2d:e8:8d:1d": "15187483"}, {"40:a:e36:22:4a:4f": "588"}, {"33:33:00:00:00:01": "1324"}, {"33:33:ff:1:e:07:62": "450"}, {"44:2a:00:de:a5:ca": "1085"}, {"33:33:ff:49:06:67": "450"}, {"d4:c9:4b:99:id:cb": "434"}, {"94:b4:0f:e1:b7:cb": "2718"}, {"e0:33:8e:66:49:55": "1946"}, {"9c:b6:d0:bd:66:ca": "12885"}, {"86:5f:1f:a5:24:e6": "120"}, {"10:00:00:00:00:36": "247"}, {"5d:9f:13:cc:1c:06": "1806"}, {"33:33:ff:1:f44:6d": "300"}, {"08:22:58:93:d2:2a": "6710"}, {"d4:c9:4b:d3:4b:ab": "2242"}, {"98:32:4b:16:e4:32": "22555"}, {"88:7b:f9:21:83:bf": "28026"}, {"98:61:ae:f9:e6:6f": "2440"}, {"9c:b6:d0:0:cc:b3": "196"}, {"64:5a:04:ce:e9:4e": "392"}, {"e0:33:8e:2e:c6:b0": "392"}, {"d4:0d:0d:0:aa:95:ec": "1830"}, {"aa:bd:b7:74:1:c:ed": "1023"}, {"86:7a: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:d0:3e:b0": "8646"}, {"e6:se: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:b3:54:eb": "6696"}, {"d4:c9:4b:89:2:c:cb": "868"}, {"a0:c5:89:01:5a:18": "8514"}, {"68:72:51:64:67:d7": "1023"}, {"ae:e5:7d:31:e9:19": "2693"}, {"08:11:96:20:bc:a0": "393"}, {"18:02:e4:c3:96:2e": "588"}, {"d8:f2:ca:3:c:ce:4a": "478"}, {"18:64:72:e0:8b:72": "56"}, {"3c:28:6d:25:4c:de": "1455"}]
```

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

# Top Rx



The screenshot shows a terminal window with a dark background and light-colored text. It displays a list of network interface statistics, likely from a tool like `top` or `iftop`. The list includes various MAC addresses and their associated values. The first few lines of the output are as follows:

```
[['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'],
 ['e0:89:bf:1b:c7:d4', '14793944'],
 ['d8:9c:67:b9:1b:47', '732'],
 ['be:70:2d:ea:8d:1d', '482874'],
 ['e0:33:8e:66:49:55', '2718'],
 ['a0:04:60:3d:ff:a0', '2310'],
 ['94:b4:0f:e1:a8:ed', '1085'],
 ['94:b4:0f:e1:a8:e2', '788'],
 ['94:b4:0f:b0:d0:e2', '394'],
 ['94:b4:0f:b0:d0:ed', '434'],
 ['94:b4:0f:b0:d0:el', '392'],
 ['94:b4:0f:e1:a8:el', '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:b7:00', '747'],
 ['50:c7:bf:00:97:d1', '1632'],
 ['94:b4:0f:e1:b7:d1', '684'],
 ['94:b4:0f:e1:b7:f2', '458'],
 ['94:b4:0f:b0:d0:f0', '996'],
 ['94:b4:0f:b0:d0:f1', '919'],
 ['94:b4:0f:b0:d0:f2', '916'],
 ['50:c7:bf:0c:97:e0', '5187'],
 ['fa:0f:24:36:f2:a2', '56'],
 ['74:da:39:2b:34:ce', '767'],
 ['08:57:00:bb:dd:a0', '59'],
 ['a4:8c:c3:46:f3:60', '106']]
```

At the bottom of the terminal window, the prompt `akash@akash-ThinkPad-E580:~/Desktop\$` is visible.

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

# Statistics

Activities LibreOffice Calc ▾

Wed 13:17

TCRcsv - LibreOffice Calc

File Edit View Insert Format Styles Sheet Data Tools Window Help

Liberation Sans 10

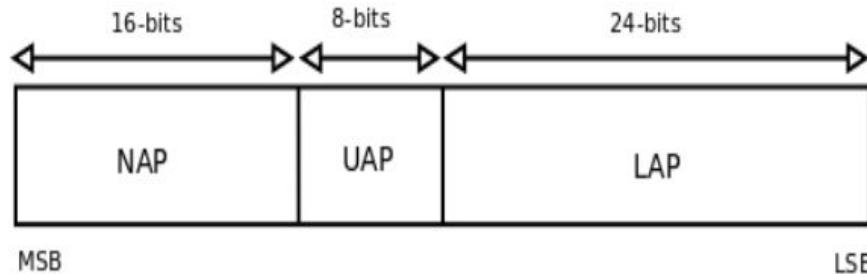
J444

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
320	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	295	-57	39													
321	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	288	-43	58.5													
322	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	135	-43	59													
323	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	409	-55	39													
324	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	135	-26	65													
325	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	135	-24	65													
326	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	626	-24	65													
327	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	626	-27	65													
328	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	1397	-42	58.5													
329	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	485	-42	58.5													
330	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	278	-42	58.5													
331	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	313	-42	58.5													
332	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	1397	-43	58.5													
333	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	1397	-43	58.5													
334	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	562	-43	58.5													
335	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	318	-57	39													
336	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	318	-55	39													
337	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	859	-54	39													
338	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	366	0	39													
339	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	143	0	39													
340	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	143	-27	65													
341	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	143	0	65													
342	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	233	0	65													
343	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	233	0	65													
344	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	233	-27	65													
345	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	135	-24	65													
346	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	430	-26	65													
347	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	273	-42	58.5													
348	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	319	-42	58.5													
349	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	210	-55	39													
350	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	123	-55	39													
351	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	283	-57	39													
352	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	e4:95:6e:40:83:93	1397	-43	58.5													
353	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	121	-27	65													
354	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	387	0	65													
355	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	121	-24	65													
356	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	387	0	65													
357	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	111	-24	65													
358	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	121	-27	65													
359	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	249	0	65													
360	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	249	0	65													
361	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	249	0	65													
362	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	121	0	65													
363	e4:95:6e:40:83:93	e0:09:bf:1b:c7:04	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	111	-57	39													
364	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	255	-24	65													
365	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	255	-27	65													
366	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e0:09:bf:1b:c7:04	255	-27	39													
367	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	e4:95:6e:40:83:93	b0:70:2d:ea:8d:1d	273	-54	39													

Sheet 1 of 1 | Default | English (USA) | Average: ; Sum: 0 | 100% | 28

# Bluetooth

# Bluetooth Address - 48 bits



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

The three parts of a Bluetooth MAC address.

79 channels of 1 MHz each

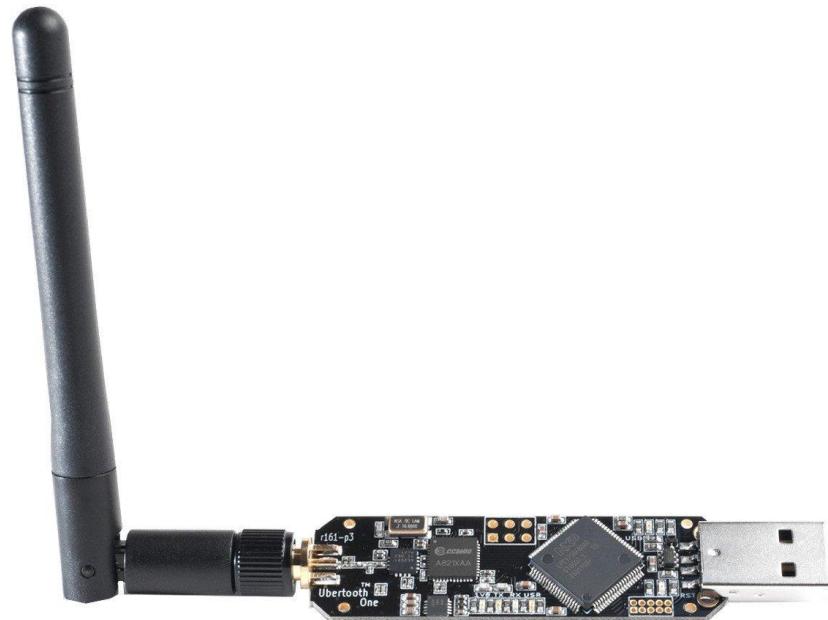
1600 hops a second in pseudo random manner

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

# Detection

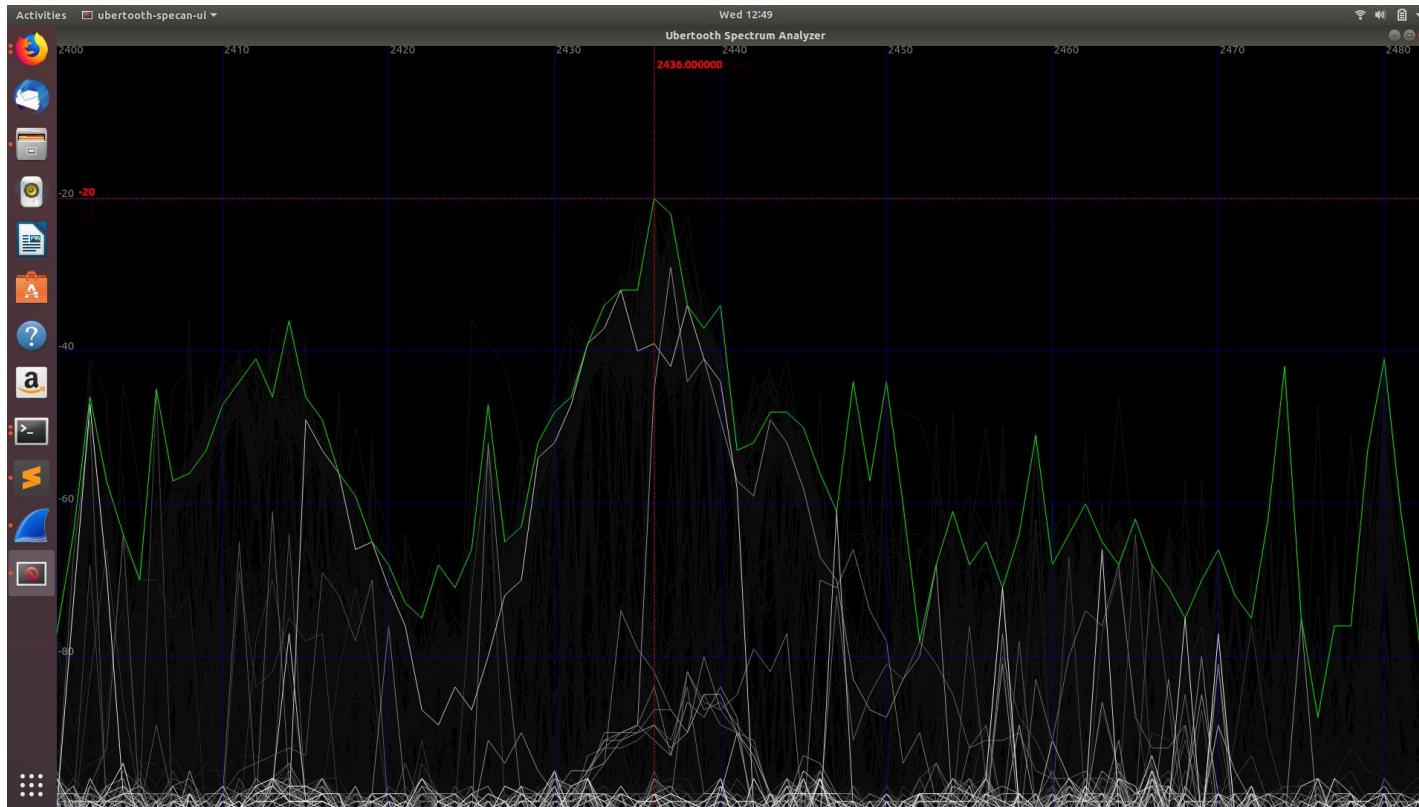
- Wireshark packet sniffing -
  - a large number of TCP/UDP packets show the presence of a video recorder.
  - Mac address lookup
  - Reverse DNS lookup
- USRP
  - Wifi receiver that can sniff packets in 2.4 and 5 GHz frequencies
  - Converted the received data into wireshark readable format
  - Mac address lookup

# Hardware

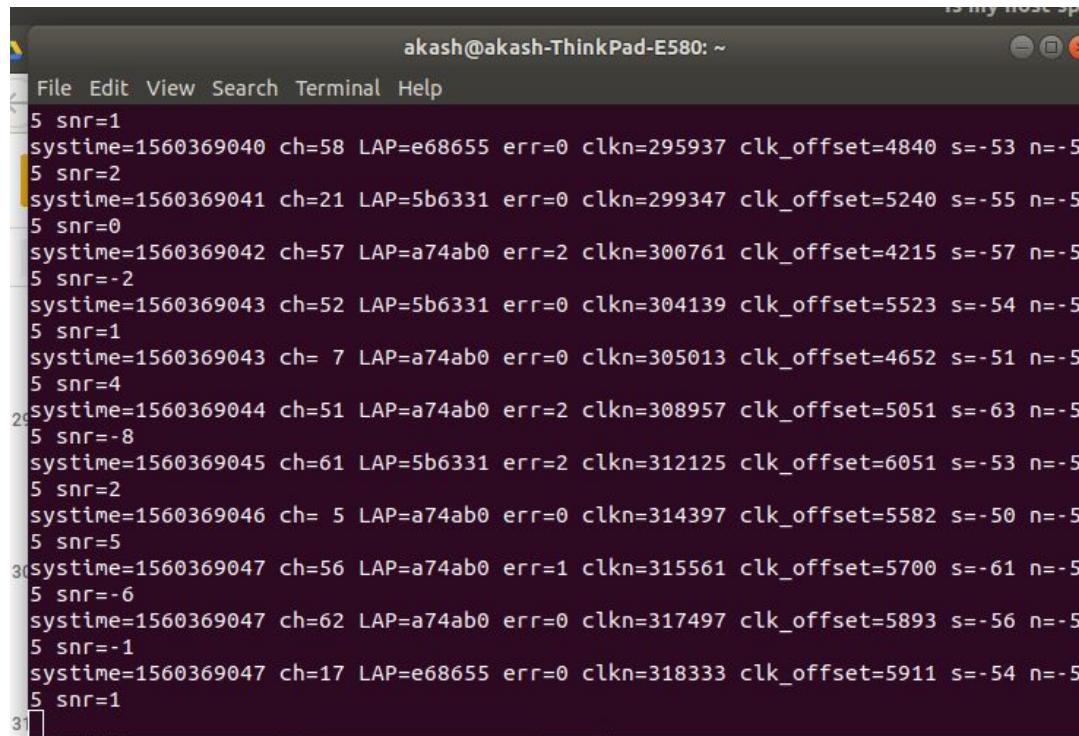


Ubertooth One

# Spectrum Analysis



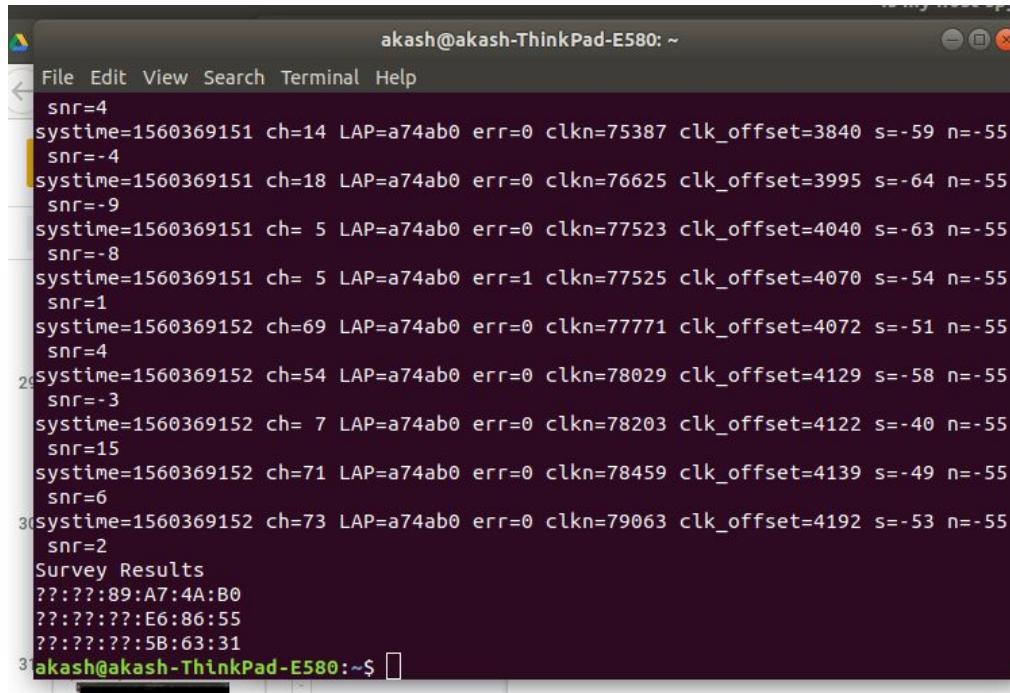
# Passive sniffing



A screenshot of a terminal window titled "akash@akash-ThinkPad-E580: ~". The window contains a list of log entries from a passive sniffing process. Each entry includes a timestamp, channel number, LAP identifier, error code, clock number, clock offset, sequence number, and a noise-to-signal ratio (snr). The entries are numbered 5, 29, 30, and 31.

```
5 snr=1
systime=1560369040 ch=58 LAP=e68655 err=0 clk_n=295937 clk_offset=4840 s=-53 n=-5
5 snr=2
systime=1560369041 ch=21 LAP=5b6331 err=0 clk_n=299347 clk_offset=5240 s=-55 n=-5
5 snr=0
systime=1560369042 ch=57 LAP=a74ab0 err=2 clk_n=300761 clk_offset=4215 s=-57 n=-5
5 snr=-2
systime=1560369043 ch=52 LAP=5b6331 err=0 clk_n=304139 clk_offset=5523 s=-54 n=-5
5 snr=1
systime=1560369043 ch= 7 LAP=a74ab0 err=0 clk_n=305013 clk_offset=4652 s=-51 n=-5
5 snr=4
systime=1560369044 ch=51 LAP=a74ab0 err=2 clk_n=308957 clk_offset=5051 s=-63 n=-5
29 5 snr=-8
systime=1560369045 ch=61 LAP=5b6331 err=2 clk_n=312125 clk_offset=6051 s=-53 n=-5
5 snr=2
systime=1560369046 ch= 5 LAP=a74ab0 err=0 clk_n=314397 clk_offset=5582 s=-50 n=-5
5 snr=5
30 systime=1560369047 ch=56 LAP=a74ab0 err=1 clk_n=315561 clk_offset=5700 s=-61 n=-5
5 snr=-6
systime=1560369047 ch=62 LAP=a74ab0 err=0 clk_n=317497 clk_offset=5893 s=-56 n=-5
5 snr=-1
systime=1560369047 ch=17 LAP=e68655 err=0 clk_n=318333 clk_offset=5911 s=-54 n=-5
5 snr=1
31
```

# Device discovery



A screenshot of a terminal window titled "akash@akash-ThinkPad-E580: ~". The window contains a list of device discovery logs. The logs show various entries with fields such as snr, systime, ch, LAP, err, clk\_n, and clk\_offset. The logs are color-coded: green for most entries and red for the last two. The logs are as follows:

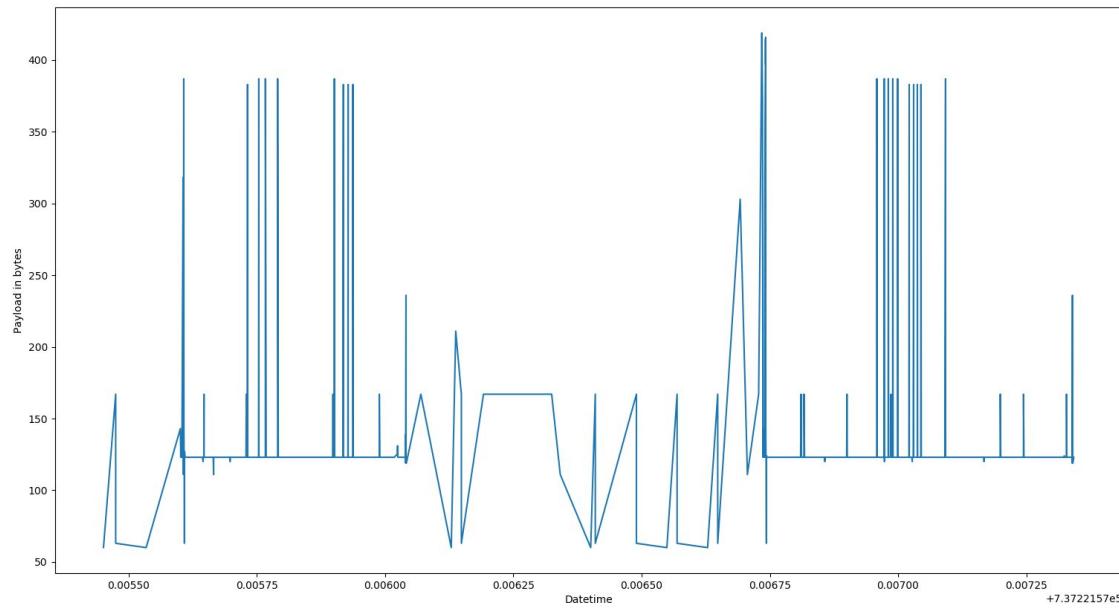
```
snr=4
systime=1560369151 ch=14 LAP=a74ab0 err=0 clk_n=75387 clk_offset=3840 s=-59 n=-55
snr=-4
systime=1560369151 ch=18 LAP=a74ab0 err=0 clk_n=76625 clk_offset=3995 s=-64 n=-55
snr=-9
systime=1560369151 ch= 5 LAP=a74ab0 err=0 clk_n=77523 clk_offset=4040 s=-63 n=-55
snr=-8
systime=1560369151 ch= 5 LAP=a74ab0 err=1 clk_n=77525 clk_offset=4070 s=-54 n=-55
snr=1
systime=1560369152 ch=69 LAP=a74ab0 err=0 clk_n=77771 clk_offset=4072 s=-51 n=-55
snr=4
systime=1560369152 ch=54 LAP=a74ab0 err=0 clk_n=78029 clk_offset=4129 s=-58 n=-55
snr=-3
systime=1560369152 ch= 7 LAP=a74ab0 err=0 clk_n=78203 clk_offset=4122 s=-40 n=-55
snr=15
systime=1560369152 ch=71 LAP=a74ab0 err=0 clk_n=78459 clk_offset=4139 s=-49 n=-55
snr=6
systime=1560369152 ch=73 LAP=a74ab0 err=0 clk_n=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
- 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.