Kismet: Network Sniffer

Kismet is a sniffer, WIDS, and wardriving tool for Wi-Fi, Bluetooth, Zigbee, RF, and more, which runs on Linux and macOS. PDF to display it's tutorial

Name: Vaibhav Mishra

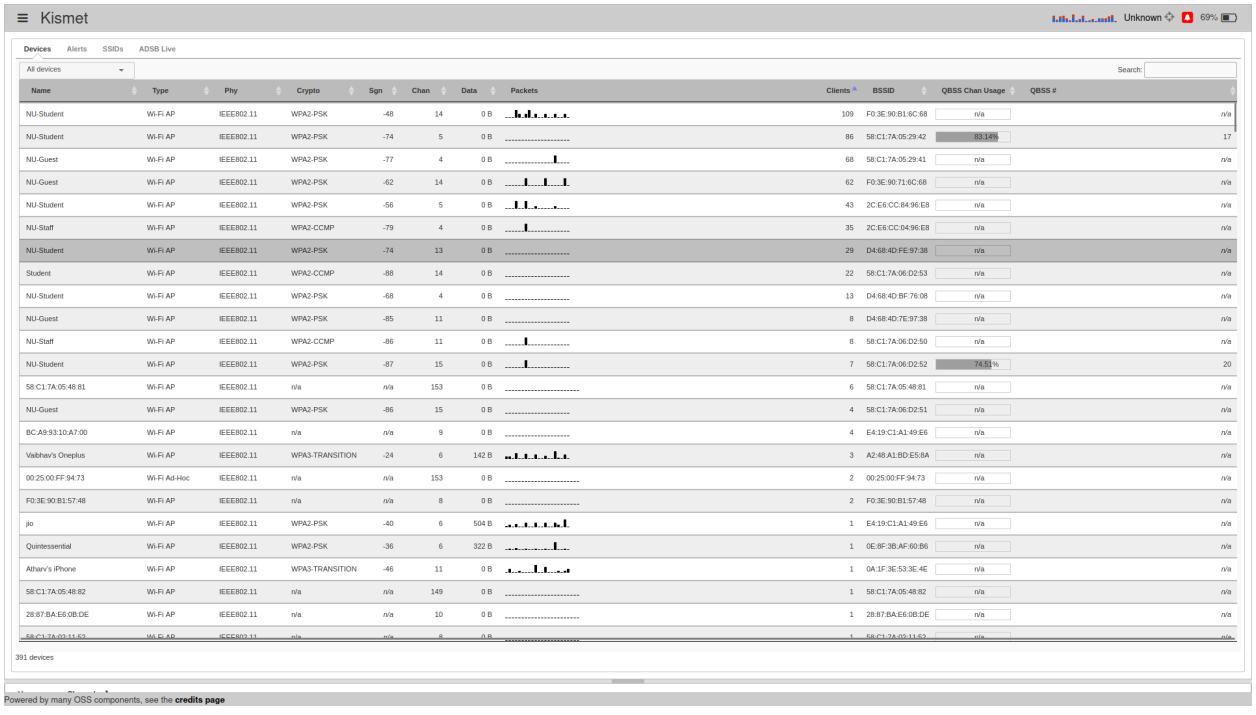
Enrollment No: BT20HCS202

Section: C3

Kismet

Kismet is a free and open-source sniffer, wardriver, and packet capture programme that may be used for Wi-Fi, Bluetooth, BTLE, wireless thermometers, aircraft, power meters, Zigbee, and other wireless protocols. Kismet is compatible with macOS, Linux, and Windows (via WSL). Both a headless operation as a standalone capture and WIDS system and a full contemporary web-based user interface are viable modes of operation for the Kismet platform.

The following are some of the numerous Wi-Fi devices that are currently being inspected at our university:



Kismet can be run on a wide range of hardware, from the very small to large servers, depending on the amount of traffic we plan to capture.

Passive Capture

Passive monitoring

Kismet works almost entirely without the user doing anything. There are a few exceptions, such as the Bluetooth scanning mode, which are explained in the documentation for those capture types.

Most of the time, Kismet is not an attack tool. If you want to test the security of your Wi-Fi network, you can use tools like Aircrack-NG or the Wi-Fi Pineapple.

Kismet is mostly about collecting, putting together, and organizing wireless data. The pcap, handshakes, and other data that Kismet generates can be fed into other tools like hashcat, aircrack, and more.

Wireless vs Wired monitoring

Wireless capture is often more difficult than wired capture, at several levels:

1. **Different physical characteristics**

   When connected to a wired network and capturing packets, all accessible packets will always be captured (assuming you have sufficient processing power and storage speed to log them, of course).

   When capturing packets from a wireless network, the situation is quite different; your receiver may not be able to see packets that the legitimate destination can receive perfectly, you may not be on the correct channel or portion of the spectrum when the packets are sent, there may be localized interference, or you may be in the center of reflected signals that cancel each other out.

2. **Drivers**

   To record raw packets from a Wi-Fi device, the "monitor mode" or "rfmon" mode is necessary; this mode disables packet filtering in the Wi-Fi card and sends raw data to the operating system.

   While the majority of Linux kernel drivers support this, not all do. Typically, mobile chipsets (such as those used in Android phones or Raspberry Pi devices) do not have the code in the device

firmware and cannot be utilized or require specific driver hacks to allow it.

Windows has almost no public monitor-mode-capable drivers, while macOS can enter monitor mode on internal Airport cards but not on other Wi-Fi types.

Other non-Wi-Fi protocols frequently lack radio capability or driver support. Sometimes the problem is resolved using specialized hardware and drivers, and sometimes software-defined radios are employed.

3. **Many protocols**
   Wi-Fi alone has at least six major modifications, each of which is virtually undetectable to previous-generation devices, in addition to three major spectrum bands. Each upgrade increases speed (decreasing effective signal) and signal complexity (MIMO, sub-channels, etc.), making data capture more difficult. Add Bluetooth, Zigbee, arbitrary RF protocols, and the amount of hardware and software required to collect what is in the air, and that's only Wi-Fi.

Smarter hopping

- Kismet tries to maximize channel hopping by two main ways:
  - Scrambling the channels. Channels are shuffled so that Kismet won’t hop to two overlapping channels in sequence
  - Offsetting the channel list between cards so that two cards won’t be on overlapping channels at the same time.

- As you add more cards, Kismet will automatically offset it so you cover as many unique channels at once as possible

Step 1- Install Kismet

To install Kismet on Kali Linux, we'll first clone the git repository with the command below.

```
git clone https://www.kismetwireless.net/git/kismet.git
```

Depending on your operating system, Kismet may not require any dependencies. To guarantee that Kismet operates successfully, however, we must install its extensive list of requirements. Kismet detects, decodes, logs, and sorts a large quantity of wireless data while operating a wireless card, which involves the installation of many libraries. You may accomplish this by using the following command in a terminal window.

```
sudo apt-get install build-essential git libmicrohttpd-dev zlib1g-dev
libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libncurses5-dev
libnm-dev libdw-dev libsqlite3-dev
```

Next, navigate to the Kismet directory we created using **cd**, and configure the installation.

```
cd kismet ./configure
```

This configures the installation for your specific operating system distribution. Upon completion of this procedure, make the installation by:

When this is complete, we will execute the generated file with the suidinstall option to complete the installation. This is necessary since Kismet receives and writes data directly to your computer. It is a poor idea to do this action as the root user since any malicious data might be executed as root.

When non-privileged users need to do actions that need rights, such as managing the wireless network adapter, Linux allows us to provide privileges to programmes instead of users so that we do not have to make everyone, even malware, root.

Step 2- Put Your Wireless Card in Monitor Mode

Connect your wireless network card to your computer, and if necessary, use the "USB" settings to connect it to the virtual machine as well. The ip a or ifconfig commands can be used to locate your card. Something like "wlan1" or "wlan0." should be the name of your card.

Using the command below, you can put your card in monitor mode once you know its name.

```
sudo airmon-ng start YourCardName
```

YourCardName (in my example, wlan0) will enter monitor mode as a result of this. Your card's name will be changed to include "mon" at the end. As a result, if it was previously called "wlan0" it will now be called

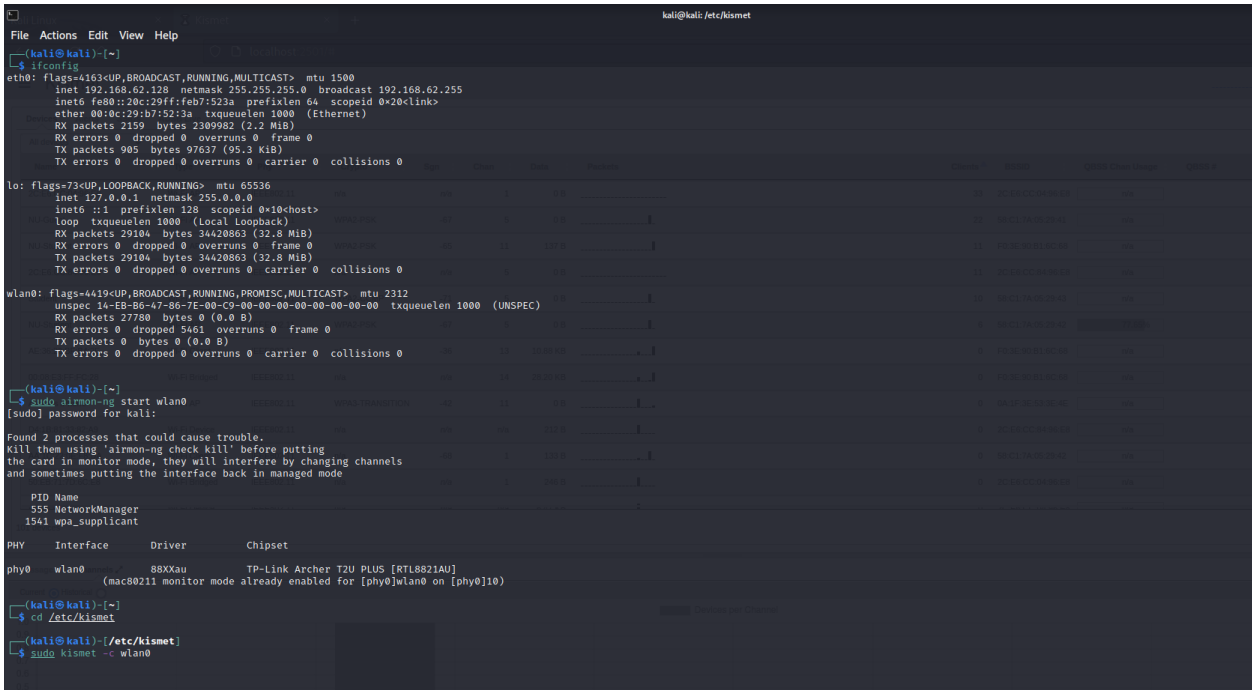
"wlan0mon." With this modification, we can now tell right away if a card is in wifi monitor mode.

Kismet will be introduced under this new name.

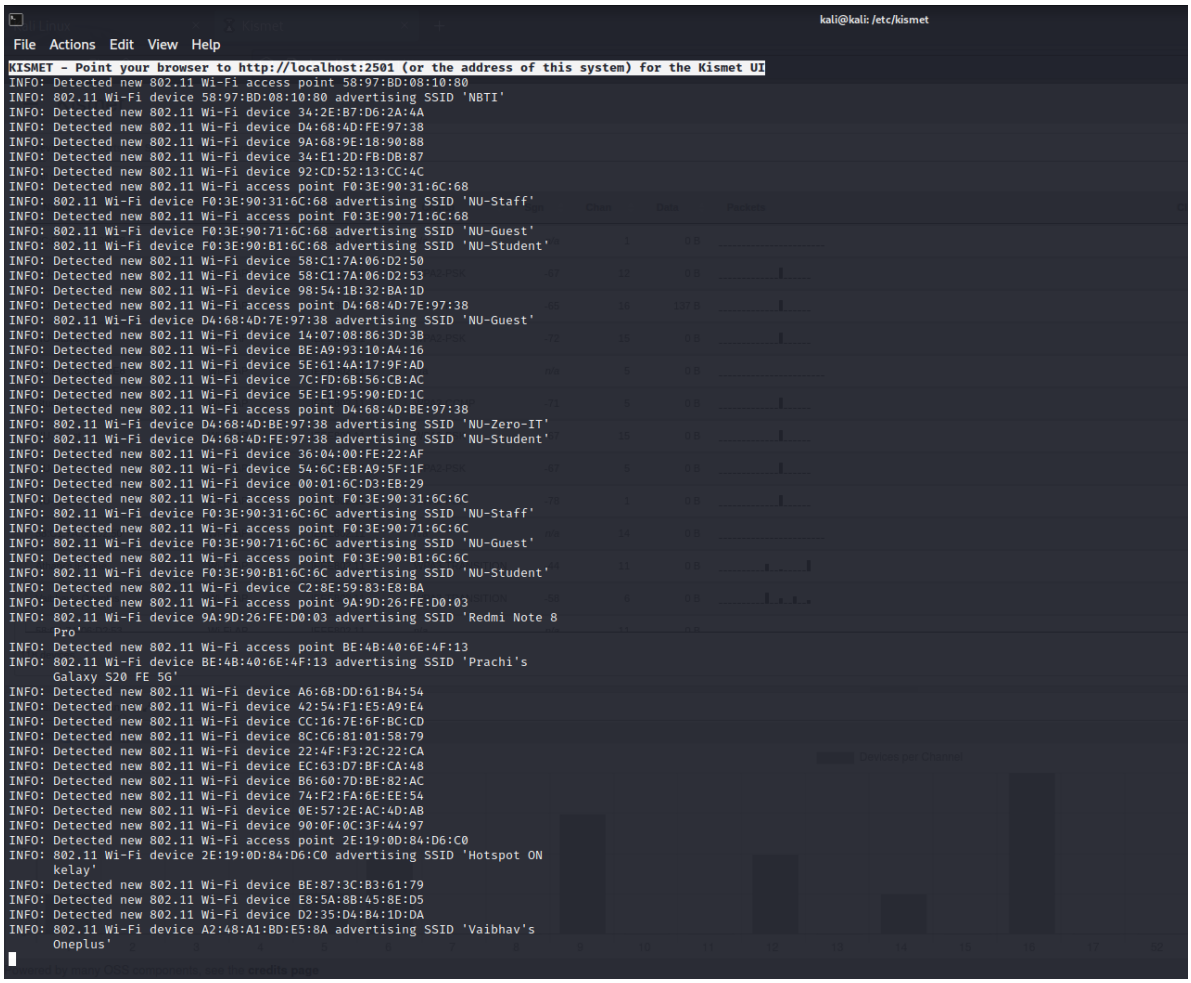
Step 3 Launch Kismet

Starting Kismet is simple. To start as a non-root user, you can simply type the following.

```
kismet -c YourCardNameMon
```



Be sure to put the name of the card you put in wireless monitor mode after the **-c**. Kismet uses the **-c** to specify the capture source.

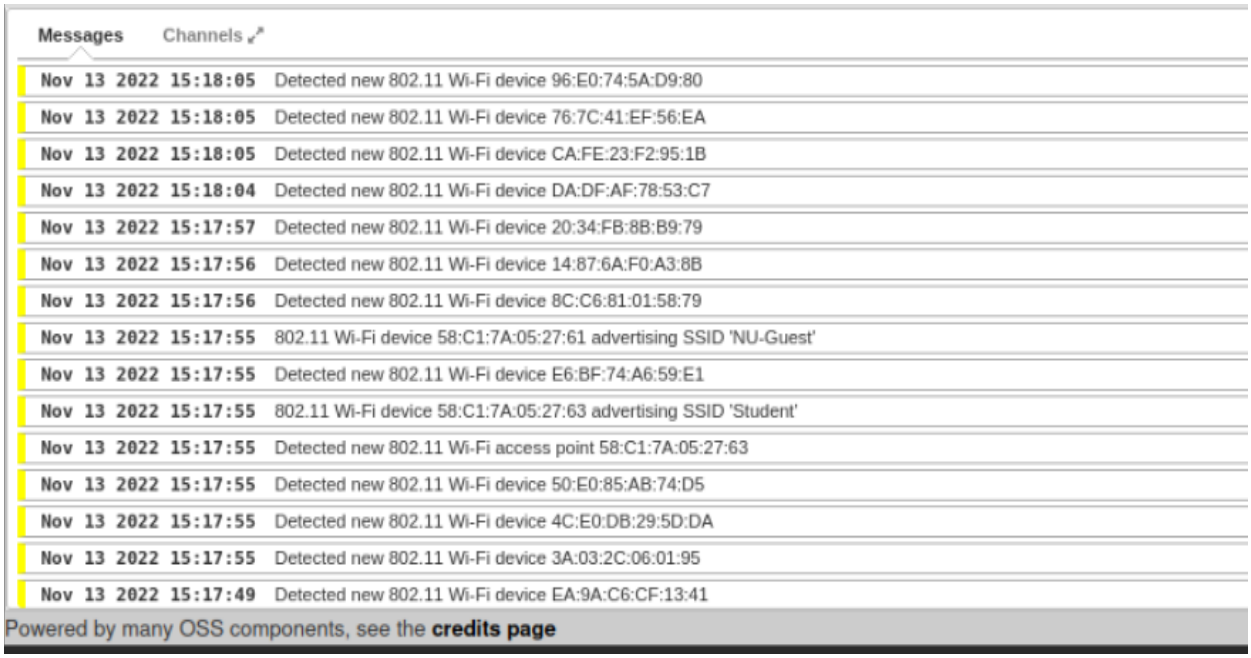


Kismet should power up and start gathering packets. To navigate the menu selections and get to the console window, hit return. Press the tab key to return to the main screen, and enter to hide the console view.

Messages

Although the raw data is also shown in the communications tab of the UI, Kismet is capable of showing bitrate and data transfer information through an easily understood UI.

As shown in the picture below, is an example of messages provided by Kismet Network Scanner:



Alerts

Alerts are used by Kismet to transmit crucial server events and wireless intrusion events.

Alerts are generated as both specific alert records and text messages on the messagebus.

See the eventbus API for monitoring alarms in real time.

Alert severities

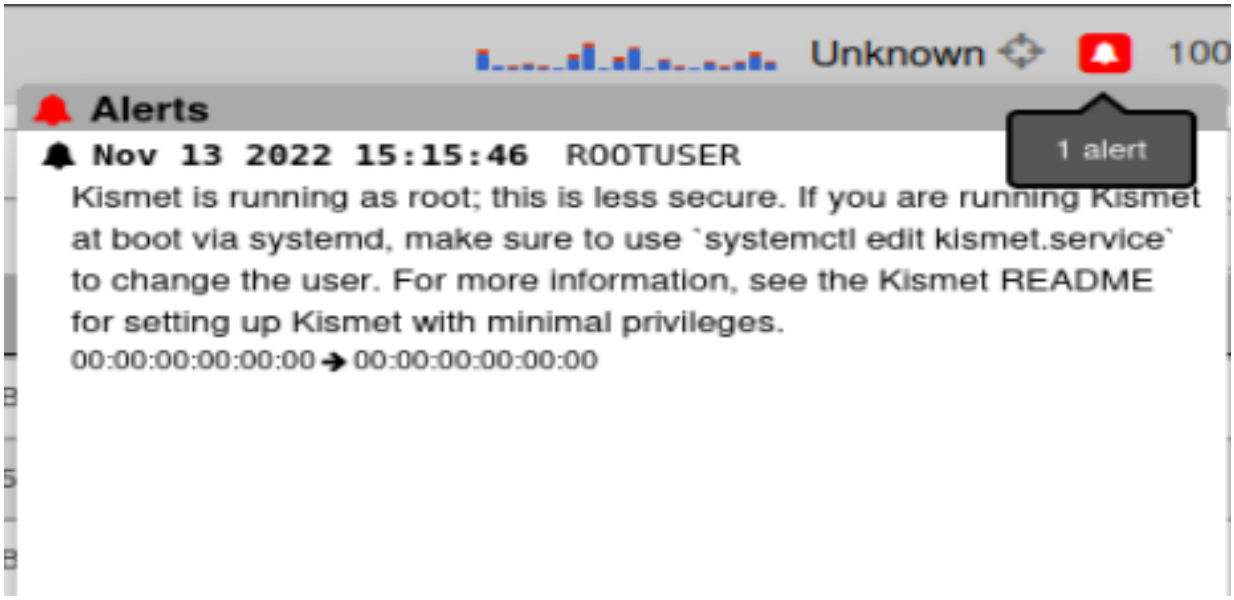
Alert severities are categorized by numerical value; a higher number is more severe.

Severity	Definition	Use
0	INFO	Informational alerts, such as datasource errors, Kismet state changes, etc
5	LOW	Low-risk events such as probe fingerprints
10	MEDIUM	Medium-risk events such as denial of service attempts
15	HIGH	High-risk events such as fingerprinted watched devices, denial of service attacks, and similar
20	CRITICAL	Critical errors such as fingerprinted known exploits

Alert types

Alerts are categorized by type; alert types are free-form strings, but include:

Type	Use
DENIAL	Possible denial of service attack
EXPLOIT	Known fingerprinted exploit attempt against a vulnerability
OTHER	General category for alerts which don't fit in any existing bucket
PROBE	Probe by known tools
SPOOF	Attempt to spoof an existing device
SYSTEM	System events, such as log changes, datasource errors, etc

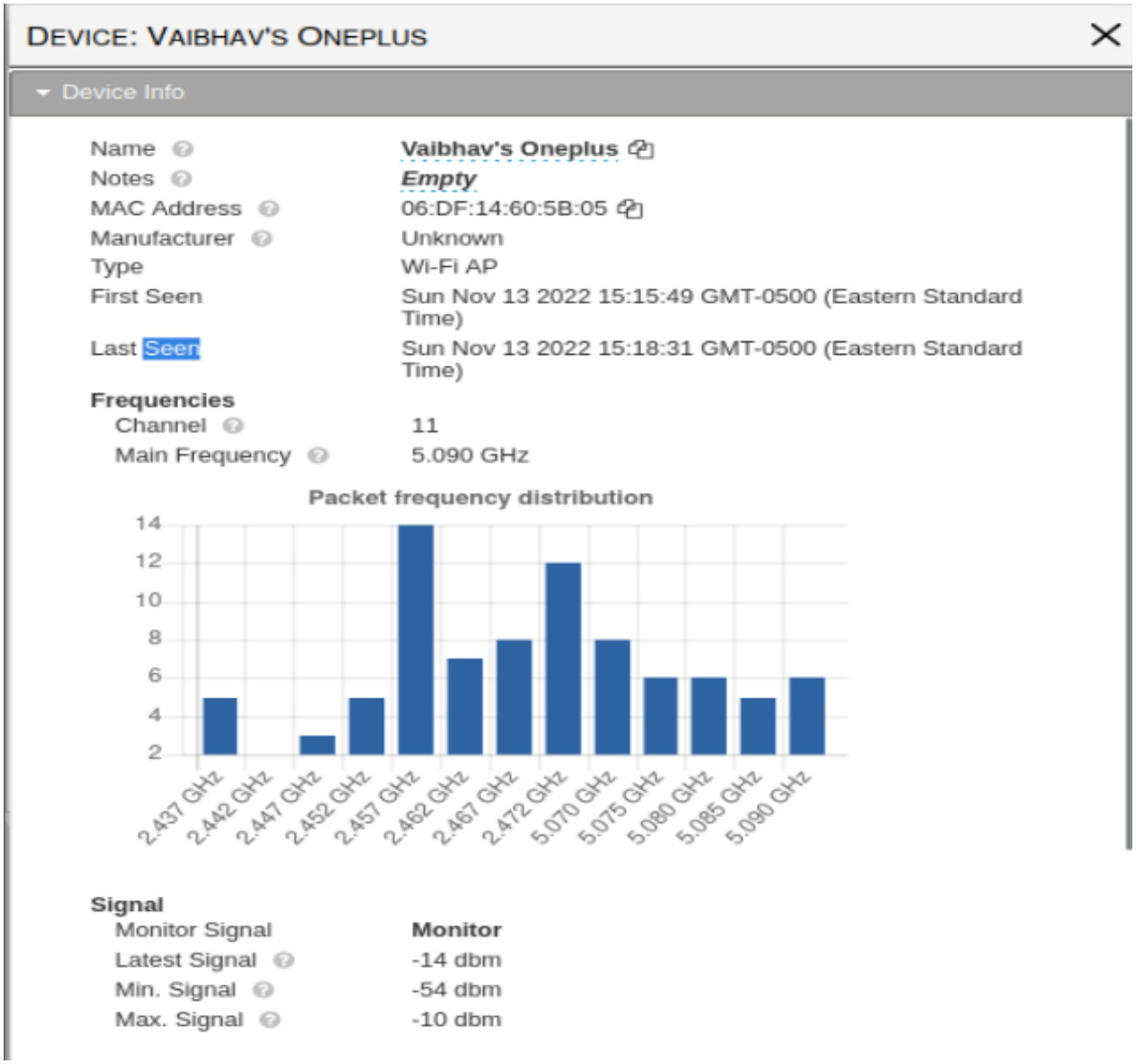


Device Information

The main record of a tracked entity in Kismet is a device. Every form of thing that Kismet observes, including clients, bridges, access points, wireless sensors, and others, will eventually turn out to be a device.

The device record will be expanded by each PHY layer, and the common fields will be filled in.

A list of related devices in the device record specifies the access point-client relationship, common hardware, etc. for complicated relationships (such as 802.11 Wi-Fi).

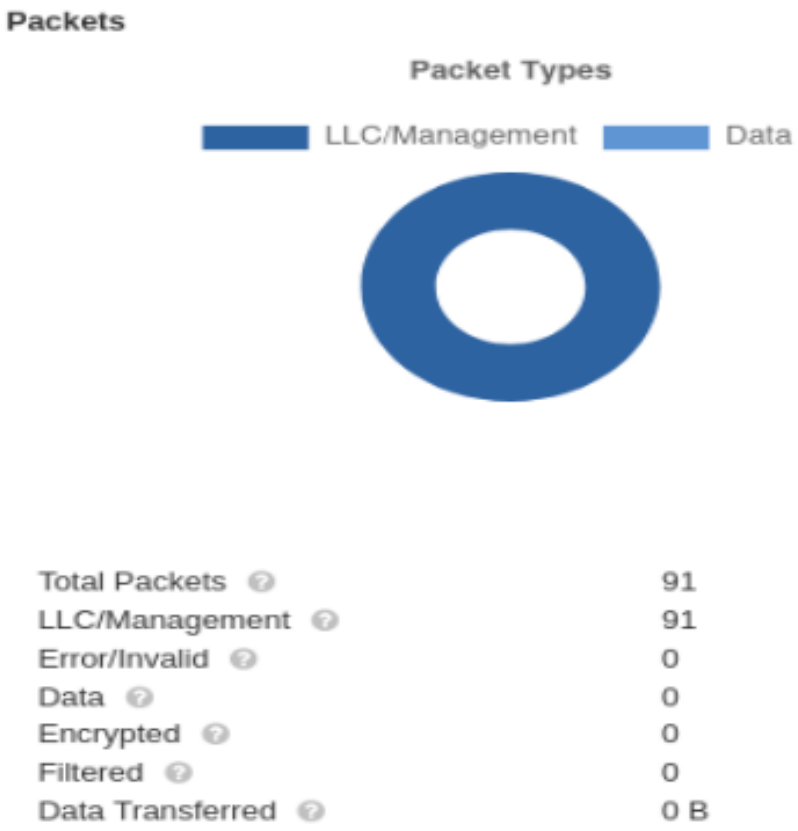


Here we can see the device details of my personal hotspot. Key information like:

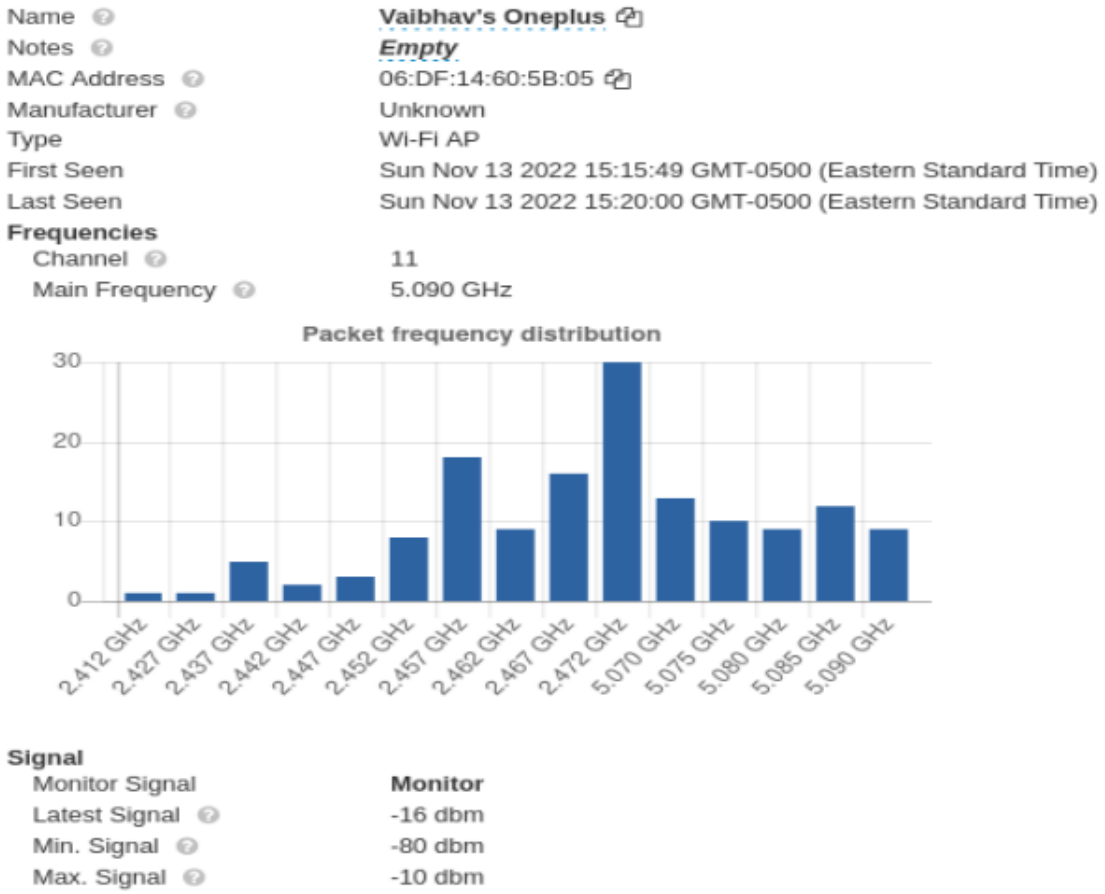
- Name
- Notes
- MAC Address

- Manufacturer
- Type
- First Seen
- Last Seen
- Packet Frequency Distribution Chart
- Signal Strength

And much more

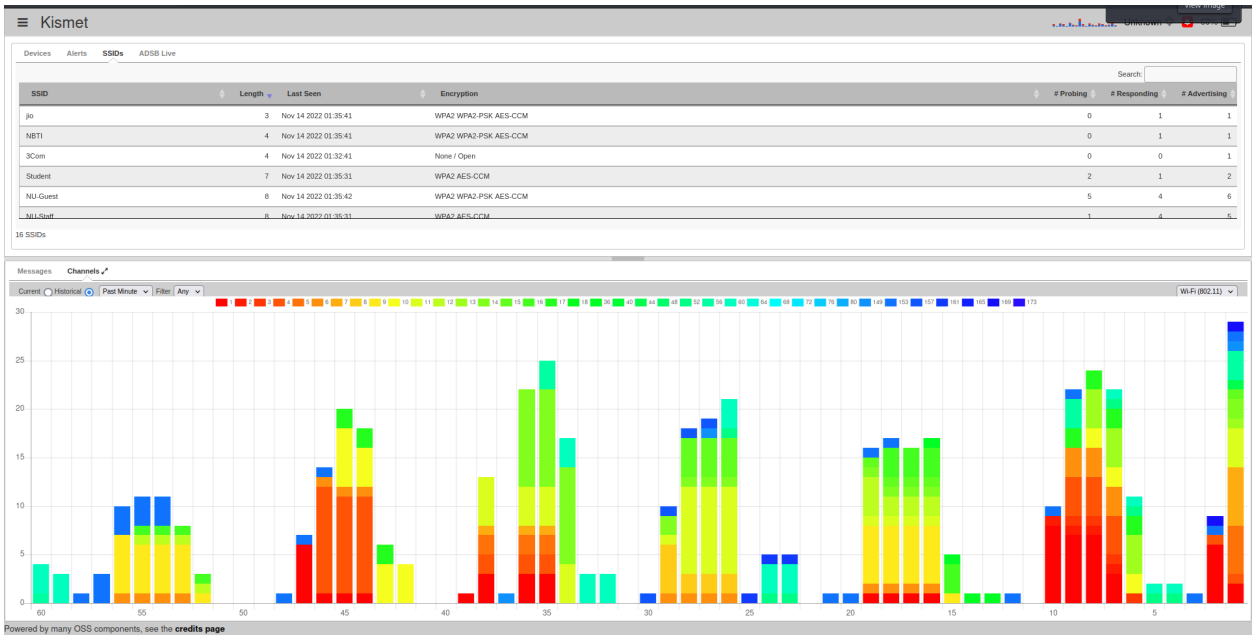


Here information about packets of through the device has been shown

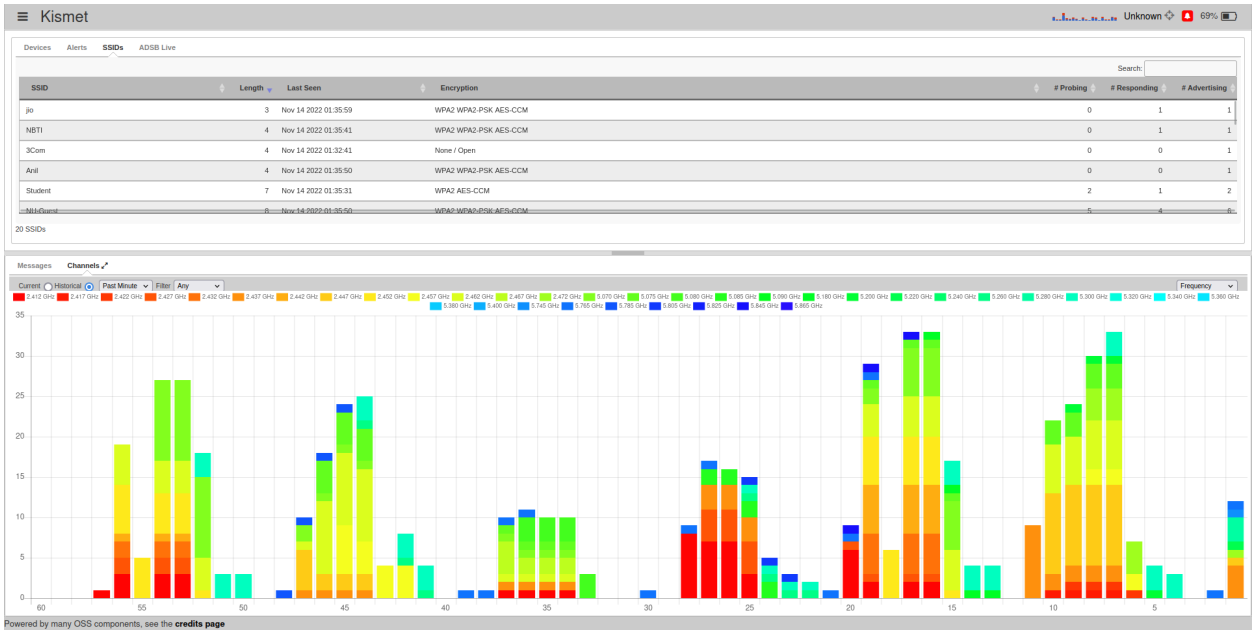


Information similar to the first image can be seen with the frequency distribution chart as well.

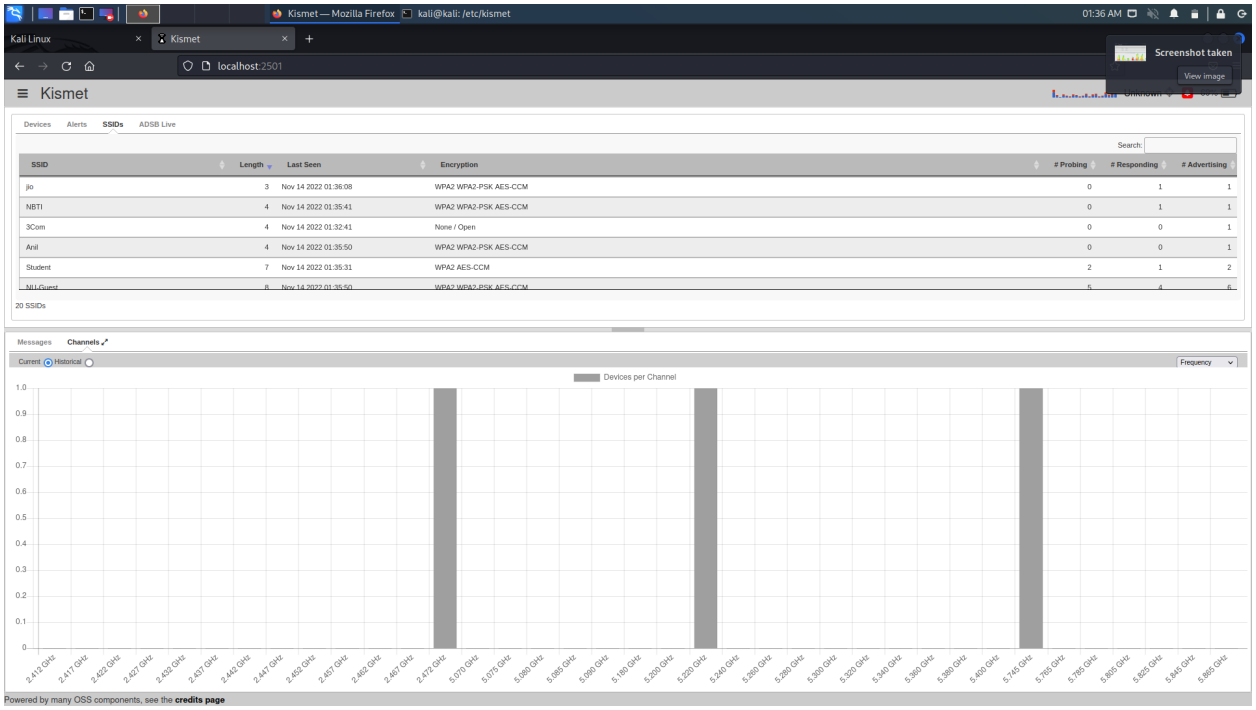
Graphical Representation



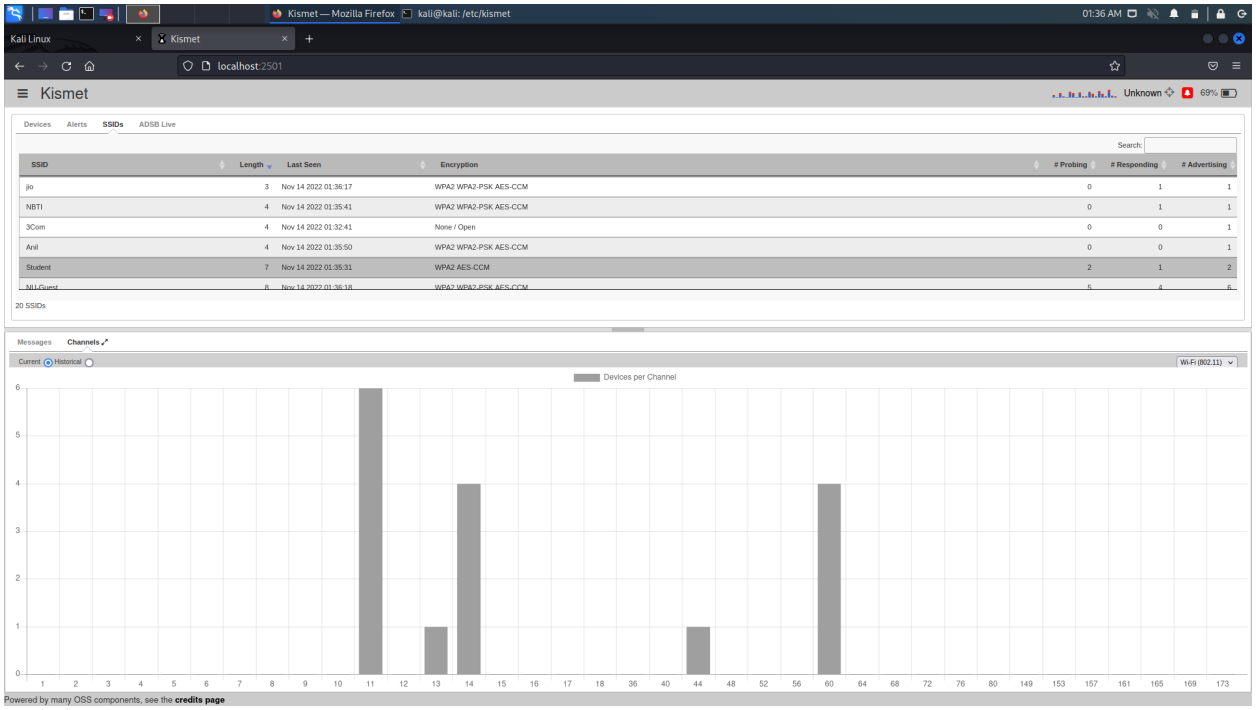
This is the Historical Graphical representation of Wi-Fi vs Clients in the past minute of kismet scanning the network.



This is the Historical Graphical representation of Frequency vs Wi-Fi clients in the past minute of kismet scanning the network.



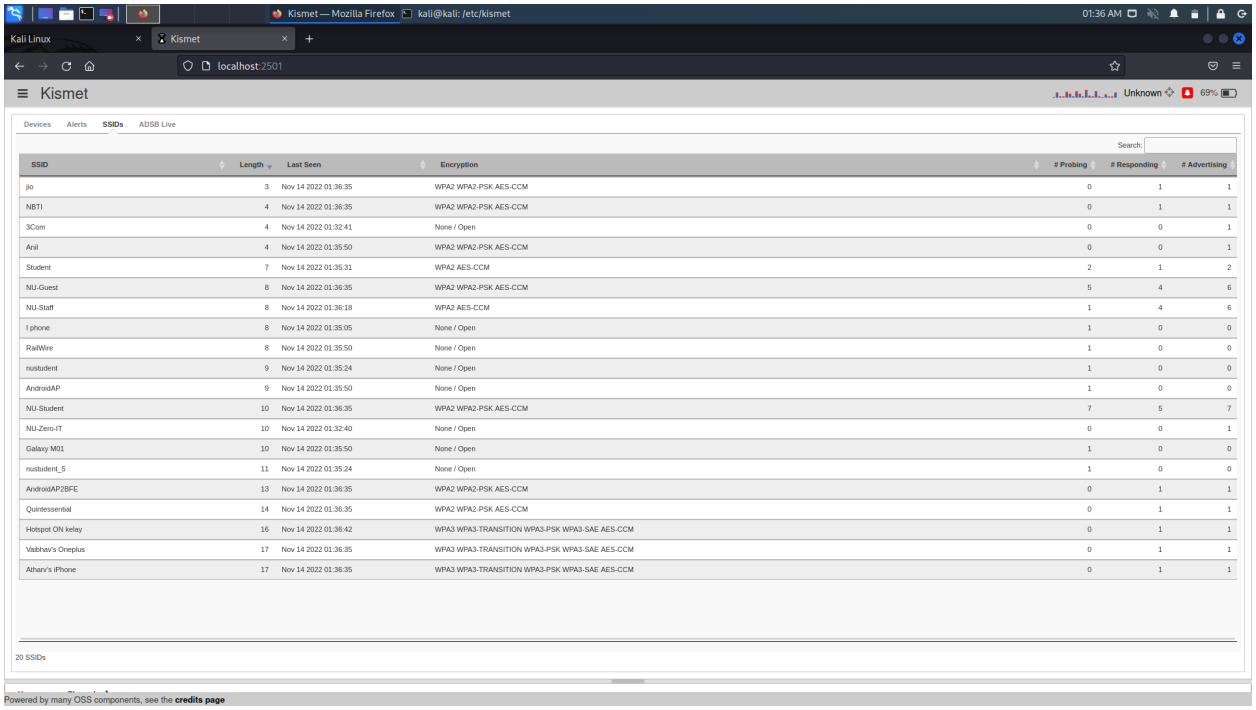
This is the current graph for Devices per client information represented in a graphical manner.



This is the current graph for Devices per channel information for Wi-Fi represented in a graphical manner.

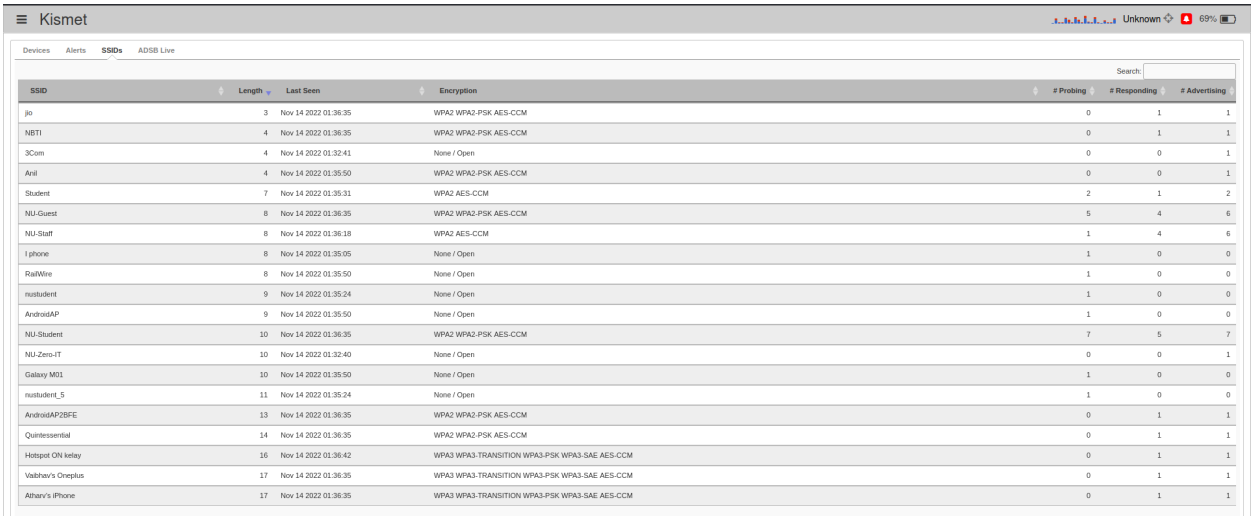
Step 4 Persistent Network Surveillance

When we launch Kismet, a list of all the nearby Wi-Fi devices should appear. Whether you are scanning at 2.4 GHz, 5 GHz, or both, the number of devices detected will change. If you have the option to do so, a higher gain (or directional) antenna can increase the number of devices detected and the range of your wireless network adapter.

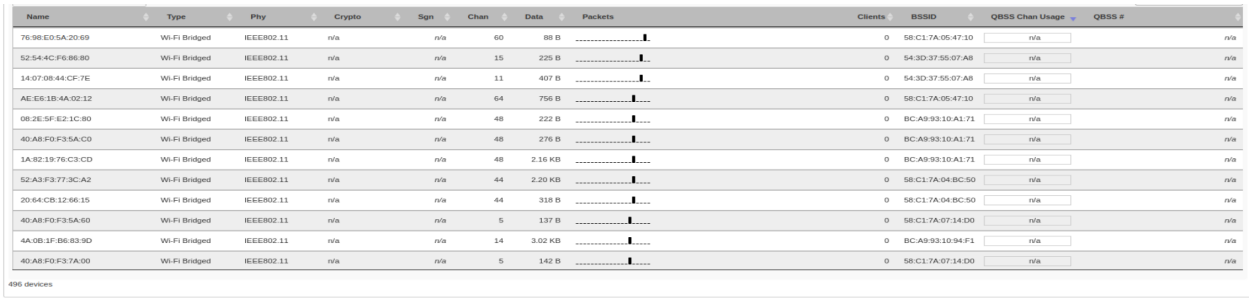


You can arrange these networks by

- Name

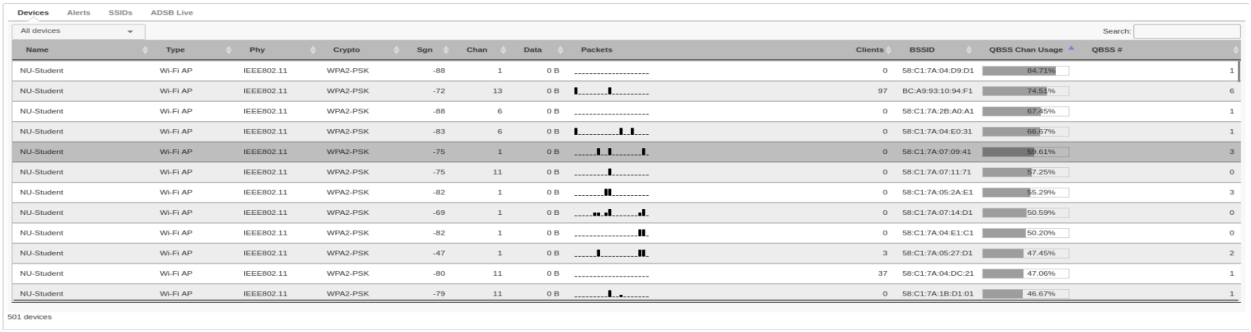


- Signal strength (It's advised that you do so by signal strength so that you can see what networks are strongest and thus closest first. Once you have a network you'd like to target, click on it (or scroll down to it) in Kismet to learn more information about it.)



Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS #
76:98:E0:5A:20:69	Wi-Fi Bridged	IEEE802.11	n/a	n/a	60	88 B		0	58:C1:7A:05:47:10	n/a	n/a
52:54:4C:F6:86:80	Wi-Fi Bridged	IEEE802.11	n/a	n/a	15	225 B		0	54:3D:37:55:07:A8	n/a	n/a
14:07:08:44:CF:7E	Wi-Fi Bridged	IEEE802.11	n/a	n/a	11	407 B		0	54:3D:37:55:07:A8	n/a	n/a
AE:E6:1B:4A:02:12	Wi-Fi Bridged	IEEE802.11	n/a	n/a	64	756 B		0	58:C1:7A:05:47:10	n/a	n/a
08:2E:5F:E2:1C:80	Wi-Fi Bridged	IEEE802.11	n/a	n/a	48	222 B		0	BC:A9:93:10:A1:71	n/a	n/a
40:A8:F0:F3:5A:C0	Wi-Fi Bridged	IEEE802.11	n/a	n/a	48	276 B		0	BC:A9:93:10:A1:71	n/a	n/a
1A:82:19:76:C3:CD	Wi-Fi Bridged	IEEE802.11	n/a	n/a	48	2.16 KB		0	BC:A9:93:10:A1:71	n/a	n/a
52:A3:F3:77:3C:A2	Wi-Fi Bridged	IEEE802.11	n/a	n/a	44	2.20 KB		0	58:C1:7A:04:BC:50	n/a	n/a
20:64:CB:12:66:15	Wi-Fi Bridged	IEEE802.11	n/a	n/a	44	318 B		0	58:C1:7A:04:BC:50	n/a	n/a
40:A8:F0:F3:5A:60	Wi-Fi Bridged	IEEE802.11	n/a	n/a	5	137 B		0	58:C1:7A:07:14:D0	n/a	n/a
4A:0B:1F:B6:83:9D	Wi-Fi Bridged	IEEE802.11	n/a	n/a	14	3.02 KB		0	BC:A9:93:10:94:F1	n/a	n/a
40:A8:F0:F3:7A:00	Wi-Fi Bridged	IEEE802.11	n/a	n/a	5	142 B		0	58:C1:7A:07:14:D0	n/a	n/a

496 devices



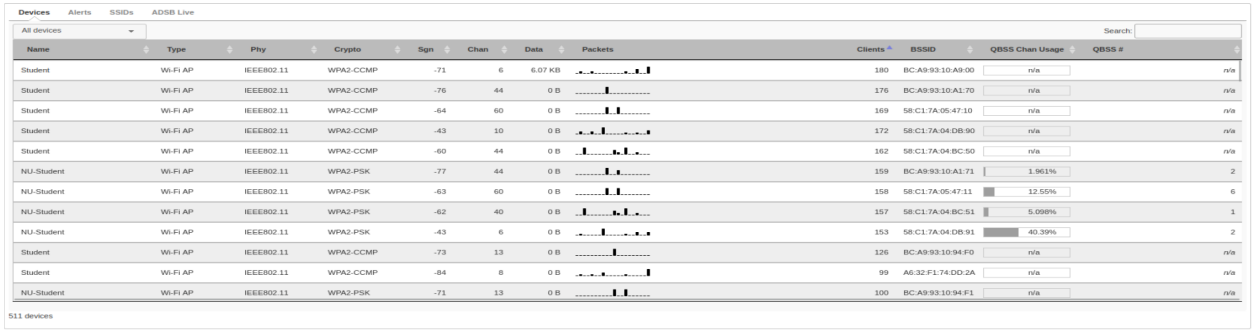
Devices Alerts SSIDs ADSB Live

All devices Search:

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS #
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-88	1	0 B		0	58:C1:7A:04:D9:D1	84.71%	1
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-72	13	0 B		97	BC:A9:93:10:94:F1	74.51%	6
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-88	6	0 B		0	58:C1:7A:2B:A0:A1	67.25%	1
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-83	6	0 B		0	58:C1:7A:04:E0:31	66.67%	1
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-75	1	0 B		0	58:C1:7A:07:09:41	59.61%	3
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-75	11	0 B		0	58:C1:7A:07:11:71	57.25%	0
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-82	1	0 B		0	58:C1:7A:05:2A:E1	55.29%	3
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-69	1	0 B		0	58:C1:7A:07:14:D1	50.59%	0
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-82	1	0 B		0	58:C1:7A:04:E1:C1	50.20%	0
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-47	1	0 B		3	58:C1:7A:05:27:D1	47.45%	2
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-80	11	0 B		37	58:C1:7A:04:DC:21	47.06%	1
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-79	11	0 B		0	58:C1:7A:1B:D1:01	46.67%	1

501 devices

- Other properties

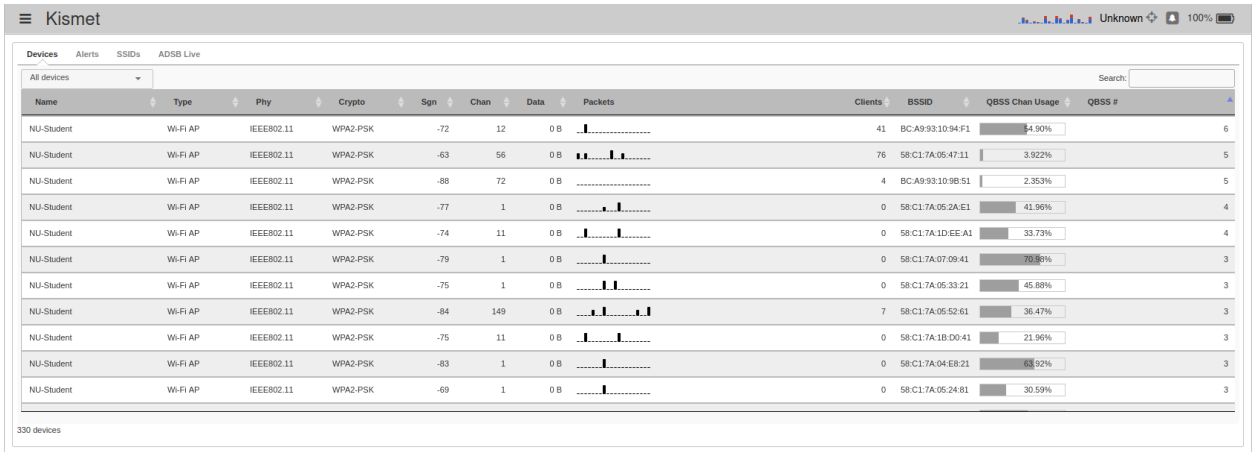


Devices Alerts SSIDs ADSB Live

All devices Search:

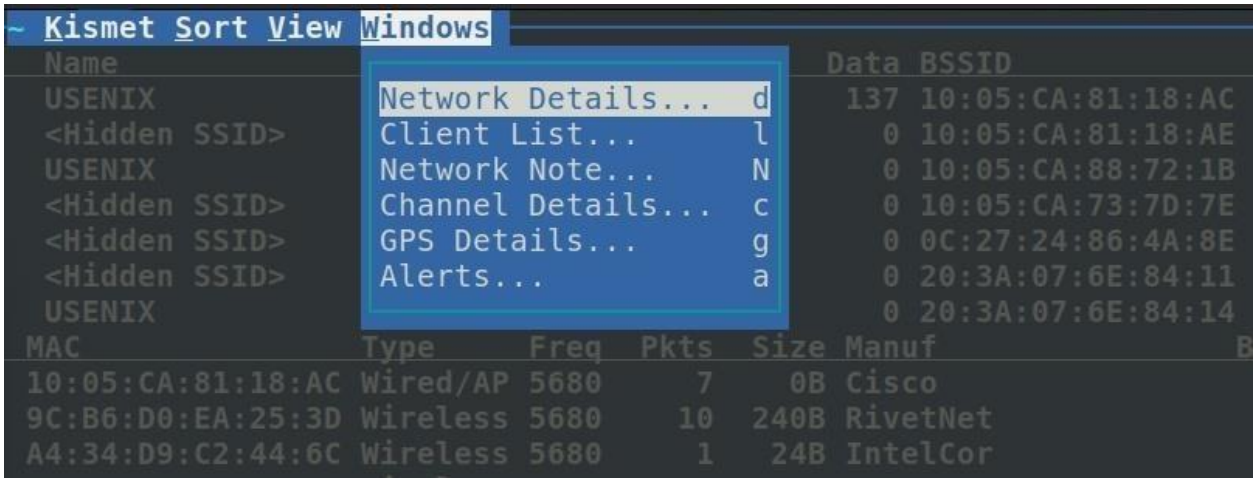
Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS #
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-71	6	6.07 KB		180	BC:A9:93:10:A9:00	n/a	n/a
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-76	44	0 B		176	BC:A9:93:10:A1:70	n/a	n/a
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-64	60	0 B		169	58:C1:7A:05:47:10	n/a	n/a
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-43	10	0 B		172	58:C1:7A:04:DB:90	n/a	n/a
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-60	44	0 B		162	58:C1:7A:04:BC:50	n/a	n/a
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-77	44	0 B		159	BC:A9:93:10:A1:71	1.961%	2
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-63	60	0 B		158	58:C1:7A:05:47:11	12.55%	6
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-62	40	0 B		157	58:C1:7A:04:BC:51	5.098%	1
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-43	6	0 B		153	58:C1:7A:04:DB:91	40.39%	2
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-73	13	0 B		126	BC:A9:93:10:94:F0	n/a	n/a
Student	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-84	8	0 B		99	A6:32:F1:74:DD:2A	n/a	n/a
NU-Student	Wi-Fi AP	IEEE802.11	WPA2-PSK	-71	13	0 B		100	BC:A9:93:10:94:F1	n/a	n/a

511 devices

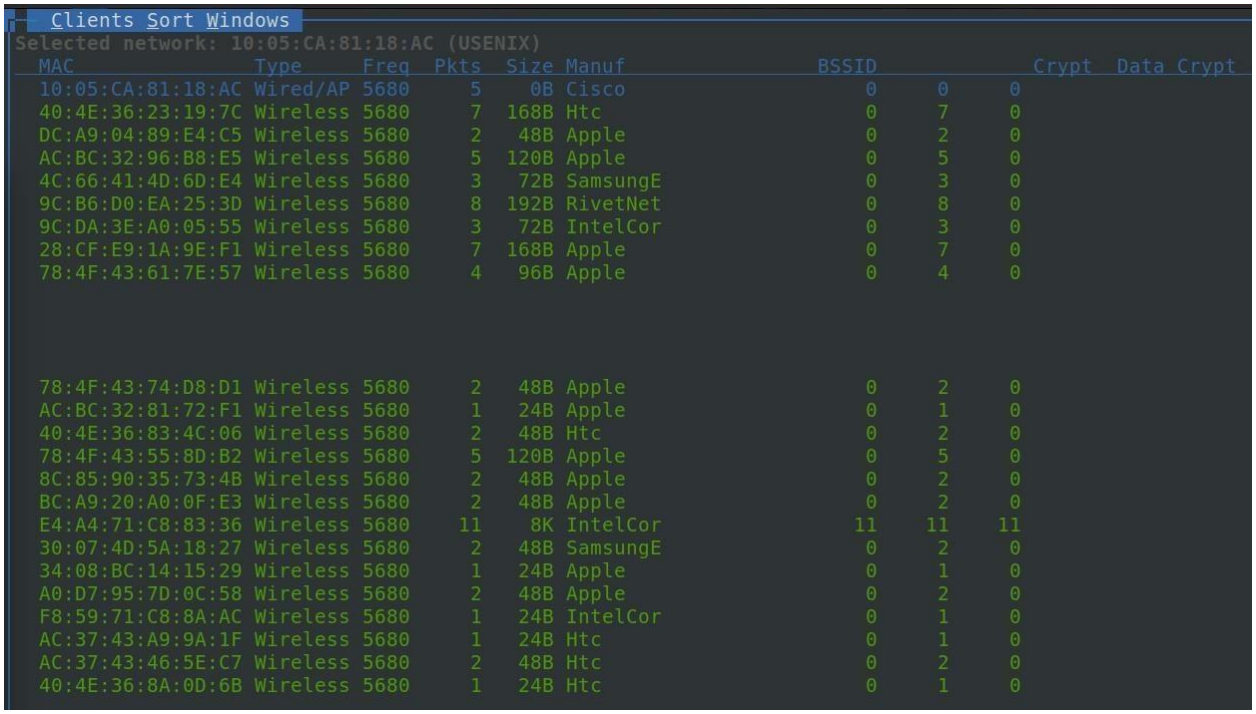


The list of wireless clients that appears in the main window as soon as a network has been highlighted is the first item we'll notice. These customers are connected to the network.

After highlighting a particular network, you can select "Windows" from the drop-down menu, and then select "Client List." from that menu to acquire additional information regarding that network's clientele.



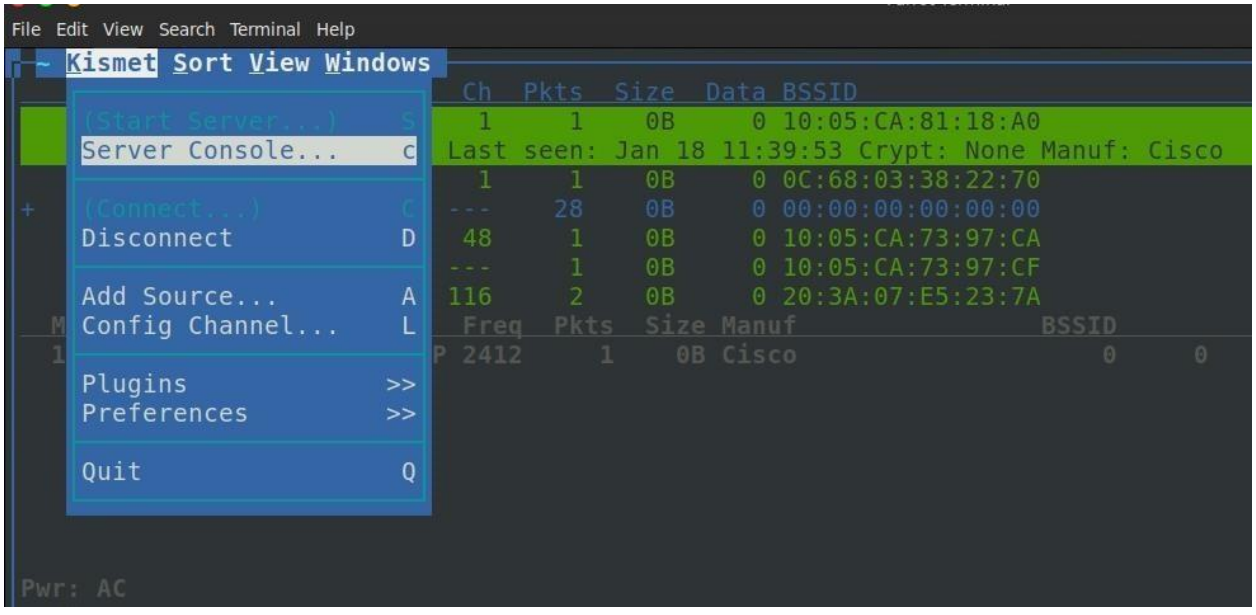
In the client window, we can see more information about each client in real time.



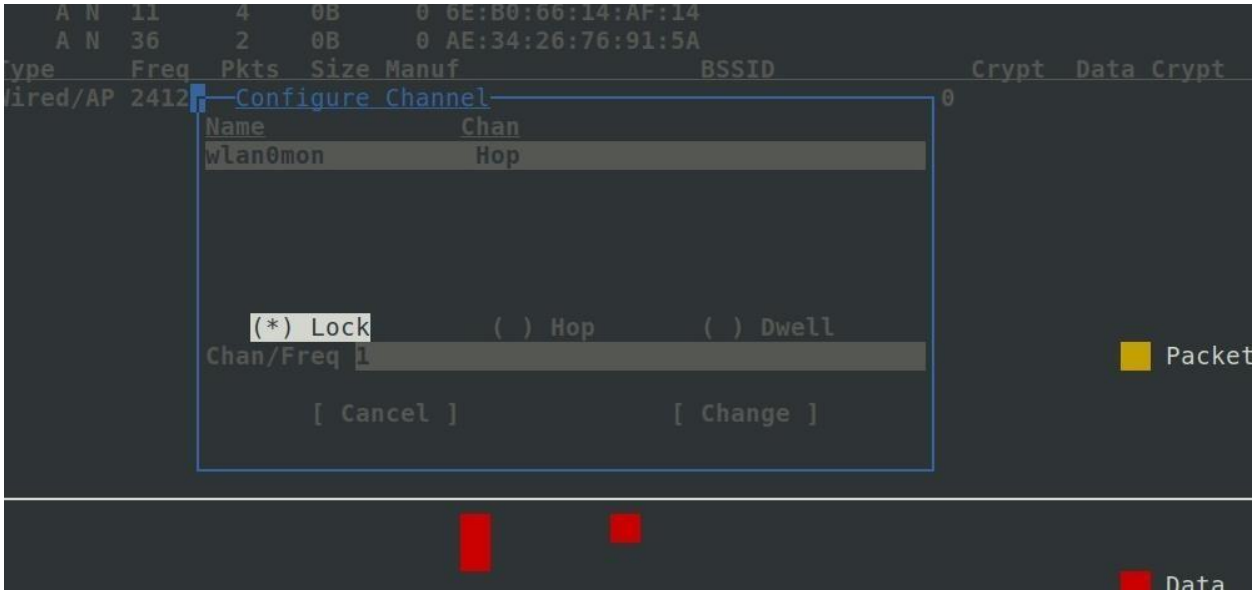
It is a good idea to make a note of the channel number if you have a network that you intend to monitor in a permanent manner. Because

Kismet hops from one channel to the next in order to scan them all, you will be unable to listen to any communications that take place on a given channel while Kismet is scanning another. Because of the possibility of losing data due to packet fragmentation, you should switch from "scanning" to permanently monitoring one channel as soon as you have identified the network you intend to keep an eye on. This will make it possible for you to record anything that happens on the channel.

To accomplish this, click the "Kismet" icon in the upper-left corner of the screen, and then click the "Config Channel." icon that appears.



In the configuration window, select "Lock," and then enter the number of the channel you want to monitor.



Watch for Patterns & Explore Around You

Kismet enables you to monitor the generally imperceptible changes in the wireless environment brought forth by human behavior. The relationships between these networks and the plaintext parts of packets are sufficient to reveal their true nature, therefore the encryption doesn't matter. The nature of the traffic traversing networks can tell us more about how and by whom these systems are utilized than any external observation ever could.

Kismet's "Alerts" submenu in the "Windows" menu is where you'll get notifications about any potentially malicious WiFi activity. Networks that are changing channels, APs that are rapidly changing names, deauth packets, and spoofing networks may all be detected using this method.

Hiding Your Activity from Cheap & Easy

Wireless Surveillance

I noted before that a directional Wi-Fi antenna may pick up signals from a mile away. The military uses these signals as a backup to GPS navigation through NAVSOP because of how powerful they are (Navigation via Signals of Opportunity). If the military can use your Wi-Fi network to guide planes across the sky, you might want to rethink whether you need it turned all the way up to 11 (which it almost certainly is right now) simply to receive Wi-Fi in your home or office.

The vast majority of users who have access to their router's administrative interface have only logged in once and have never made any changes beyond the minimum necessary. Power settings are available on virtually all router models, however instructions vary by manufacturer. You can decline at any time. A whole deal lower. To avoid customer complaints about weak signals, manufacturers typically set the default to maximum. If you're not having any issues with your Wi-range, Fi's you may decrease it so that it just extends where it's needed.

Just simply hard-wire whatever information you need to keep private. Don't broadcast signals outside your home if there's no way to prevent them from being picked up by a nearby sensitive antenna. In a pinch,

you may use Kismet to see how far away an intruder can get before they start picking up data from your network.

Hiding Your Devices from the Kismet List

Turn off the Wi-Fi option on all client devices, including cellphones, anytime you aren't going to be using the feature. Your Wi-Fi card may be used to monitor you not just at your place of employment or residence but also anyplace else. Even if you are not connected to a Wi-Fi network, this will still be the case. You don't have much control over the devices whose functionality is dependent on Wi-Fi.

The makers of smartphones make an effort to randomise the MAC address that your phone broadcasts when it is moving about, but this strategy is rendered useless the moment the phone attempts to identify itself with a network it believes it already knows. Because it is so simple to do this to a large group of individuals, it is not resilient in the face of a genuine assault. Don't trust me? If you alter the name of your mobile hotspot on your phone to "Google Starbucks," practically every smartphone in the surrounding area will connect to you and give its genuine MAC address, enabling you to follow it.