KisMAC Manual - The Details View and the Client Table

The Details View

- **SSID**
  The Service Set IDentifier is used to identify a network in the 802.11 standard. It is set by the admin of the network and may be broadcasted by the network as its name. Every client needs to know the SSID of the network he wants to join.
- **BSSID**
  The Basic Service Set IDentifier is used to identify a BSS (Basic Service Set) within a network area. In Infrastructure BSS networks, the BSSID is the MAC address of the hardware used as AP. With Independent BSS and in Ad-Hoc mode the BSSID is randomly generated.
- **Vendor**
  If possible KisMAC determines the vendor of the device the above BSSID belongs to. Hint: If you sort the scanned networks by BSSID you sometimes find networks with explizit manufacturers SSID next to some with custom SSIDs. Take a closer look at the MACs and maybe you can determine the vendor that way yourself, if KisMAC doesn't.
- **First Seen**
  The time and date the network was first seen in this dataset.
- **Last Seen**
  The time and date the network was last seen in this dataset.
- **Channel**
  Shows the Channel KisMAC detects the network on during scan. Networks are hopping between different channels around their main channel.
- **Main Channel**
  Each network uses one main channel. If you want to examine or work on a network disable channel hopping and switch to the channel the network mainly uses.
- **Signal**
  Shows the strength of the signal during scan.
- **MaxSignal**
  Indicates the peak of signal strength.
- **AvgSignal**
  Shows the average signal strength.
- **Type**
  There are different types of modes a wireless device can operate in. "Managed" (means the station is in infrastructure mode), "Ad-Hoc" (-mode), "probe" (device is seeking for access if not associated or device is in active stumbling mode), "tunnel" is a fixed connection between two stations (bridge-mode).
- **Encryption**
  Shows the type of encryption the network is using. Disabled, WEP, LEAP or WPA.

- **Packets**
  How many packets have been detected in this network.
- **Data Packets**
  The number of data-packets that have been detected.
- **Unique IVs**
  During the WEP encryption the station generates randomly initialization vectors (IV), which are transmitted unencrypted in the frame body. The recieving unit uses the IV and the shared secret key to decrypt the content of the frame body. IVs can be changed for every frame by the sending station.
- **Inj. Packets**
  The number of packets which might be might be injectable.
- **Bytes**
  The amount of data that was monitored by KisMAC in the above network.
- **Key**
  The resolved key, if you did well.
- **LastIV**
  The last caught Initialization Vectors from WEP encryption.
- **Latitude**
  Longitude
  If you use or used GPS during your scan, the global position of the network will be shown here.
- **Comment**
  KisMAC will save the notes you type in here for each network.

The Client Table

The table shows the different addresses involved in the network (MAC, broadcast, multicast etc).

back Tell me more