

KISMET дополнительные заметки

Конфигурационные файлы для KISMET:

```
# sudo gedit /etc/kismet/kismet.conf  
# sudo gedit /usr/local/etc/kismet.conf
```

Быстрый запуск сервера, клиента:

```
# sudo kismet kismet_server -c wlan0
```

Фильтрация точек:

```
# Packet filtering options:  
# filter_tracker - Packets filtered from the tracker are not processed or  
# recorded in any way.  
# filter_export - Controls what packets influence the exported CSV, network,  
# xml, gps, etc files.  
# All filtering options take arguments containing the type of address and  
# addresses to be filtered. Valid address types are 'ANY', 'BSSID',  
# 'SOURCE', and 'DEST'. Filtering can be inverted by the use of '!' before  
# the address. For example,  
# filter_tracker=ANY(!"00:00:DE:AD:BE:EF")  
  
filter_tracker=BSSID(A4:22:B0:E5:40:5C)
```

При не верном описании переменных в файле конфигурации, сервер не запустится.

Фильтрация APSPOOF alert:

```
# Controls behavior of the APSPOOF alert. SSID may be a literal match (ssid=) or  
# a regex (ssidregex=) if PCRE was available when kismet was built. The allowed  
# MAC list must be comma-separated and enclosed in quotes if there are multiple  
# MAC addresses allowed. MAC address masks are allowed.
```

```
apspoof=Foo1:ssidregex="(?!i:foobar)",validmacs=60:73:27:5E:94:1A  
apspoof=Foo2:ssid="CrimeaKarro",validmacs="00:11:22:33:44:55,aa:bb:cc:dd:ee:ff"
```

Голосовые оповещения:

Does the server have speech? (Again, not to be confused with the GUI's speech)

enablespeech=true

Binary used for speech (if not in path, full path must be specified)

speechbin=flite

#speechbin=spd-say

Specify raw or festival; Flite (and anything else that doesn't need formatting
around the string to speak) is 'raw', festival requires the string be wrapped in
SayText("...")

speechtype=raw

Звуковые события:

Do we use sound?

Not to be confused with GUI sound parameter, this controls whether or not the
server itself will play sound. Primarily for headless or automated systems.

enablesound=false

Path to sound player

soundbin=play

Отладка GPS навигации:

Do we have a GPS?

gps=false

Do we use a locally serial attached GPS, or use a gpsd server, or

use a fixed virtual gps?

(Pick only one)

gpstype=gpsd

Host:port that GPSD is running on. This can be localhost OR remote!

gpshost=localhost:2947

Отладка листинга каналов WIFI:

```
# Default channel lists
# These channel lists MUST BE PRESENT for Kismet to work properly. While it is
# possible to change these, it is not recommended. These are used when the
supported
# channel list can not be found for the source; to force using these instead of
# the detected supported channels, override with channellist= in the source defintion
#
# IN GENERAL, if you think you want to modify these, what you REALLY want to
do is
# copy them and use channellist= in the packet source.
```

```
channellist=IEEE80211b:1:3,6:3,11:3,2,7,3,8,4,9,5,10
```

```
channellist=IEEE80211a:36,40,44,48,52,56,60,64,149,153,157,161,165
```

```
channellist=IEEE80211ab:1:3,6:3,11:3,2,7,3,8,4,9,5,10,36,40,44,48,52,56,60,64,149,153,157,161,165
```