

# **WIRELESS PENETRATION TESTING**



## SSID Discovery

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>inSSIDer .....</b>	<b>4</b>
<b>Wireless NetView .....</b>	<b>6</b>
<b>Microsoft Network Monitor .....</b>	<b>6</b>
<b>NetSurveyor .....</b>	<b>7</b>
<b>Kismet.....</b>	<b>8</b>
<b>Airodump-ng .....</b>	<b>10</b>
<b>Wash.....</b>	<b>11</b>
<b>Wireshark .....</b>	<b>12</b>

## Introduction

SSID acronym is used for **Service Set Identifier** also known as the network identification which is the name of the wireless network. This may be viewed by anybody with a wireless device within reach of your network. It could be set up to 32 characters long and are case-sensitive of your choice.

Wireless Settings

2.4GHz | 5GHz

?

☒ Enable Wireless Radio

Network Name (SSID):

aarti

☐ Hide SSID

Security:

WEP

Type:

☒ Auto

☐ Open System

☐ Shared Key

WEP Key Format:

☐ ASCII

☒ Hexadecimal

Key Type:

☒ 64-bit

☐ 128-bit

Key Value:

12345678ac

Mode:

802.11b/g/n mixed

Channel Width:

Auto

Channel:

Auto

Transmit Power:

☐ Low

☐ Middle

☒ High

Save

After the network manager has set up the SSID, the router or another Wi-Fi base station broadcasts it to the surrounding region. Then when a device scans the neighboring networks, its SSIDs are displayed—the user only has to pick the one and connect to the device.



In Wi-Fi Pentesting, we need to discover SSID, Security, Channels, and connected client for further exploitation. Through this post, I divulge some tool names that may help you to discover the following:

- Wi-Fi Network Name
- MAC Address
- Channel
- Wifi Mode
- Client
- Security

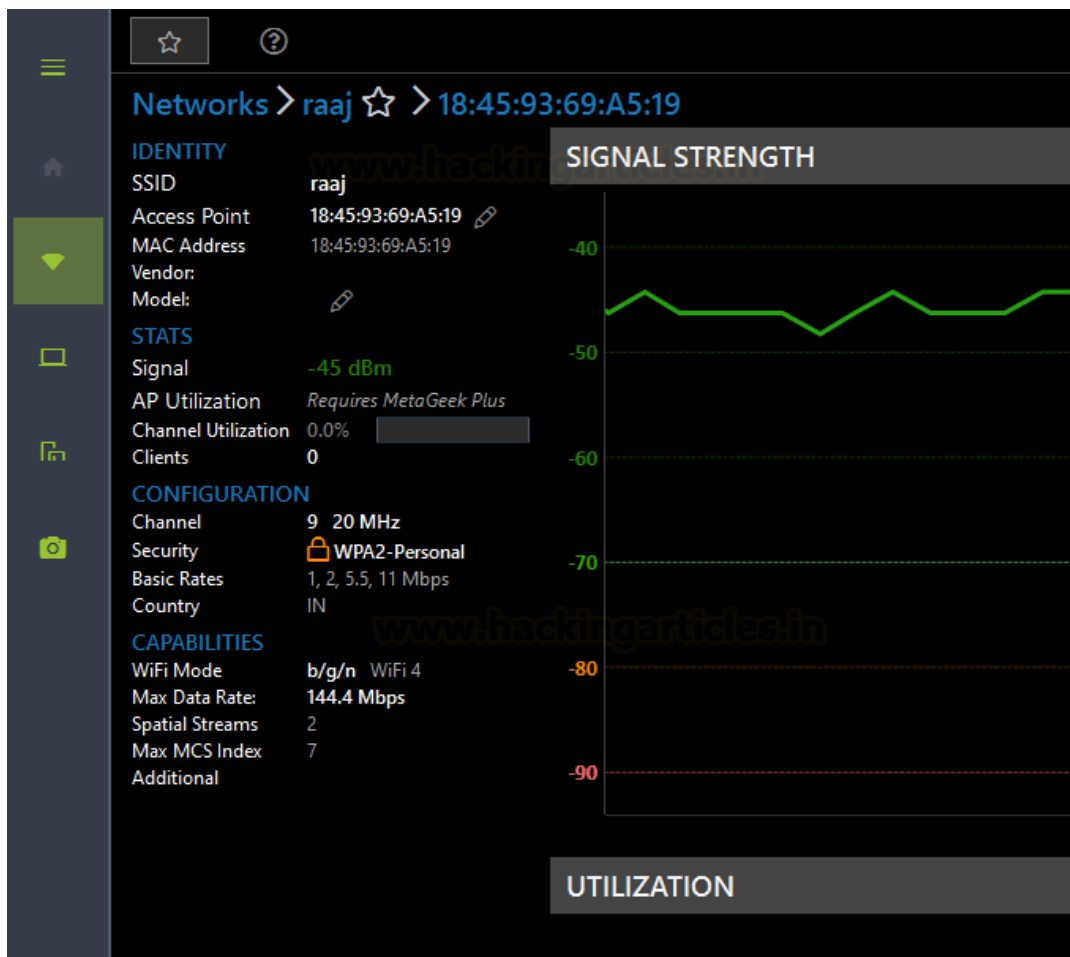
## inSSIDer

inSSIDer analyzes the configuration of your WiFi including channel settings, security, signal strength, and the impact of neighboring WiFi networks. It is easy to install and use for enumeration neighboring WiFi networks.

Download it from [here](#)

SSID	Signal	Radios	Clients	Channels	Security	Mode	Max Rate	Last Seen
aarti	-39 dBm	1	-	11	🔒	b/g	54.0	now
raaj	-45 dBm	1	-	9	🔒	b/g/n	144.4	now
Amit 2.4G	-81 dBm	1	-	1	🔒	b/g/n	216.7	now
[HIDDEN] on AG_93	-83 dBm	1	-	11	🔒	n	144.4	< 30 sec ago
Mehak jain_4G	-85 dBm	1	-	11	🔒	n	144.4	now
AG_93	-85 dBm	1	-	11	🔒	n	144.4	now
Sachin 2.4	-85 dBm	1	1	1	🔒	b/g/n	216.7	now
703 jio_4G	-87 dBm	1	-	11	🔒	n	144.4	now
[HIDDEN] on Mehak jain_4G	-87 dBm	1	-	11	🔒	n	144.4	now
Vikas	-87 dBm	1	-	5	🔒	b/g/n	130.0	now
[HIDDEN] on AA:DA:0C:58:3	-87 dBm	1	-	10	🔒	n	144.4	1 min ago
[HIDDEN] on 703 jio_4G	-89 dBm	1	-	11	🔒	n	144.4	< 1 min ago
601 2.4G	-89 dBm	1	1	1	🔒	b/g/n	216.7	1 min ago
snowie/glowie5g	-91 dBm	1	1	5	🔒	b/g/n	144.4	< 30 sec ago
Kavz	-91 dBm	1	-	7	🔒	b/g/n	144.4	< 30 sec ago

After execution, it will list all SSIDs and select an SSID in which you are interested.

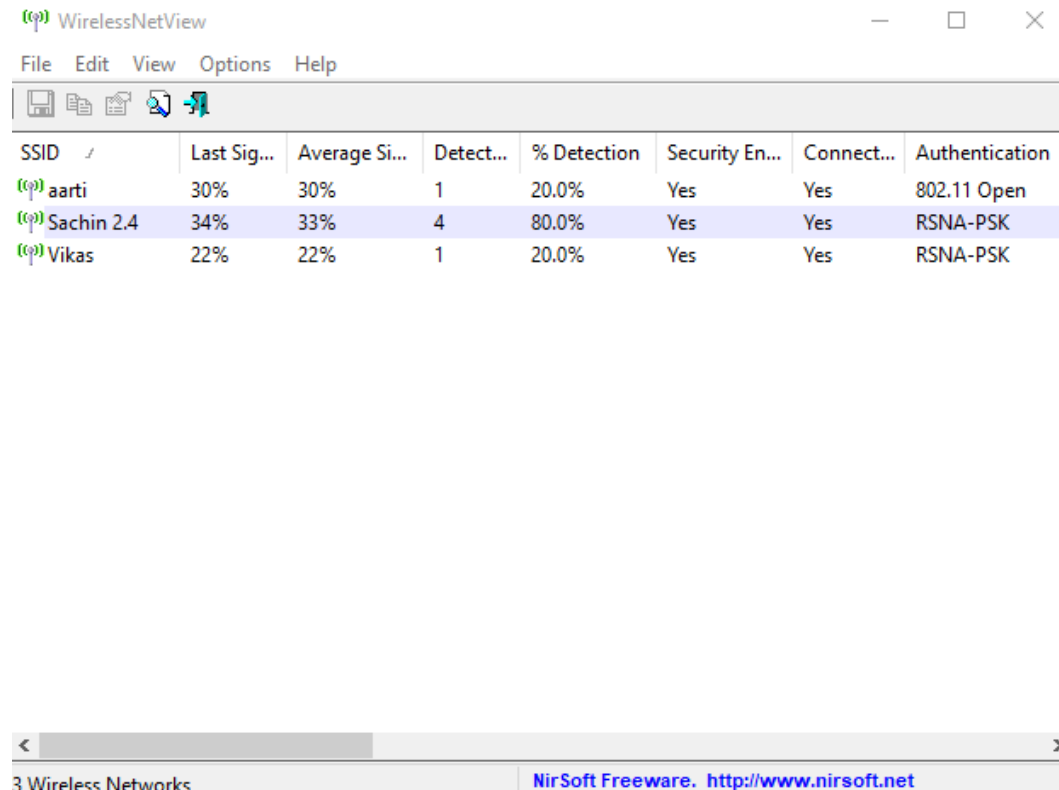


## Wireless NetView

Wireless NetView is a small utility that runs in the background and monitors the activity of wireless networks around you. For each detected network, it displays the following information: SSID, Last Signal Quality, Average Signal Quality, Detection Counter, Authentication Algorithm, Cipher Algorithm, MAC Address, RSSI, Channel Frequency, Channel Number, and more.

Download it from [here](#)

This tool is very easy to use, unzip the folder and run the executable file which will start SSID scanning and will list neighboring Wi-Fi networks.



## Microsoft Network Monitor

Microsoft Network Monitor is a tool for viewing the contents of network packets that are being sent and received over a live network connection or from a previously captured data file. It provides filtering options for the complex analysis of network data.

**Note: To use this tool you may need an external wi-fi adapter.**

You can download it from [here](#):

Microsoft Network Monitor 3.4

File Edit View Frames Capture Filter Experts Tools Help

New Capture Open Capture Save As Capture Settings Start Pause Stop

Capture1 Start Page Parsers

Frame Summary

Find Autoscroll

Fr...	Description	Time Offset	Source
1	NetmonFilter:Updated Capture Filter: None	0.0130384	
2	NetworkInfoEx:Network info for , Network Adapter Count = 1	0.0130384	
3	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.0130384	[D84732 E93F33]
4	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.0160101	[94FBA7 5A06AF]
5	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.0193294	[96FBA7 5A06AF]
6	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.0737218	[A8DA0C 36DD82]
7	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.1154529	[D84732 E93F33]
8	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.1184536	[94FBA7 5A06AF]
9	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.1217658	[96FBA7 5A06AF]
10	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.1761015	[A8DA0C 36DD82]
11	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.1820669	[AADA0C 16DD82]
12	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.2145176	[C28F20 19C5B2]
13	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.2178508	[D84732 E93F33]
14	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.2208729	[94FBA7 5A06AF]
15	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.2246620	[96FBA7 5A06AF]
16	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.2786083	[A8DA0C 36DD82]
17	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.3232530	[94FBA7 5A06AF]
18	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.3265792	[96FBA7 5A06AF]
19	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.3808941	[A8DA0C 36DD82]
20	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.4175165	[C28F20 19C5B2]
21	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.4226624	[D84732 E93F33]
22	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.4289757	[96FBA7 5A06AF]
23	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.4833103	[A8DA0C 36DD82]
24	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.4870996	[AADA0C 16DD82]
25	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.5251336	[D84732 E93F33]
26	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.5313752	[96FBA7 5A06AF]
27	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.5857259	[A8DA0C 36DD82]
28	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.5913118	[AADA0C 16DD82]
29	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.6274706	[D84732 E93F33]
30	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.6339520	[96FBA7 5A06AF]
31	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.6880990	[A8DA0C 36DD82]
32	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = 703 jio_4G, Channel = 11	0.7206670	[C08F20 39C5B2]
33	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.7247053	[C28F20 19C5B2]
34	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.7362070	[96FBA7 5A06AF]
35	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.7906865	[A8DA0C 36DD82]
36	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.7967137	[AADA0C 16DD82]
37	WiFi:[ManagementBeacon] ..... RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.8322627	[D84732 E93F33]

## NetSurveyor

NetSurveyor is a diagnostic tool that falls under the category of WiFi Scanners or 802.11 Network Discovery Tools. The best known in this category is NetStumbler. A discovery tool reports the Service Set Identifier (SSID) for each wireless network it detects, along with the channel used by the access point (AP) servicing that network.

You can download it from [here](#):

	SSID	BSSID (MAC)	Cha...	Bea...	Beaco...	Signal Quality	Radio Type	Encryption	Active
▶	UNKNOWN_SSID_...	96:fb:a7:5a:06:af	11	-100	2	No Signal	Unknown	YES	NO
	aarti	d8:47:32:e9:3f:33	11	-39	77	Excellent	OFDM24	YES	YES
	raaj	18:45:93:69:a5:19	9	-45	70	Excellent	Unknown	YES	YES
	UNKNOWN_SSID_...	aa:da:0c:16:dd:82	11	-100	2	No Signal	Unknown	YES	NO
	Amit 2.4G	68:14:01:5a:0e:9c	1	-100	2	No Signal	Unknown	YES	NO
	UNKNOWN_SSID_...	c2:8f:20:19:c5:b2	11	-100	2	No Signal	Unknown	YES	NO
	Sachin 2.4	40:49:0f:3c:49:88	1	-77	30	Low	Unknown	YES	YES
	AG_93	94:fb:a7:6a:06:af	11	-100	2	No Signal	Unknown	YES	NO
	A602_4G	a8:da:0c:78:34:fe	10	-100	2	No Signal	Unknown	YES	NO
	ajoy	70:c7:f2:ed:6a:44	4	-100	2	No Signal	Unknown	YES	NO
	Vikas	30:cc:21:e3:47:88	8	-85	20	Very Low	Unknown	YES	YES
	Mehak jain_4G	a8:da:0c:36:dd:82	11	-100	2	No Signal	Unknown	YES	NO
	703 jio_4G	c0:8f:20:39:c5:b2	11	-100	2	No Signal	Unknown	YES	NO
	snowie/glowie5g	6c:eb:b6:2f:83:34	5	-100	2	No Signal	Unknown	YES	NO
	UNKNOWN_SSID_...	aa:da:0c:1c:fc:a3	1	-89	16	Very Low	Unknown	YES	YES
	Kavz	74:5a:aa:76:66:44	7	-100	2	No Signal	Unknown	YES	NO
	Tan_4	a8:da:0c:1c:fc:a3	1	-100	2	No Signal	Unknown	YES	NO
	UNKNOWN_SSID_...	aa:da:0c:58:34:fe	10	-100	2	No Signal	Unknown	YES	NO

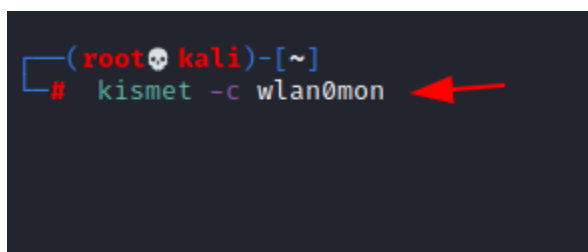
## Kismet

Kismet is an 802.11 layer-2 wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework. Kismet works with Wi-Fi interfaces, Bluetooth interfaces, some SDR (software-defined radio) hardware like the RTLSDR, and other specialized capture hardware. Kismet works on Linux, OSX, and, to a degree, Windows 10 under the WSL framework.

Start the Kismet server, using the wireless interface as the capture source (-c wlan0mon)

**Note: To use this tool you may need an external wi-fi adapter.**

```
kismet -c wlan0mon
```



The service will be running at localhost on port 2501 which is accessible through web browser **<http://localhost:2501>**

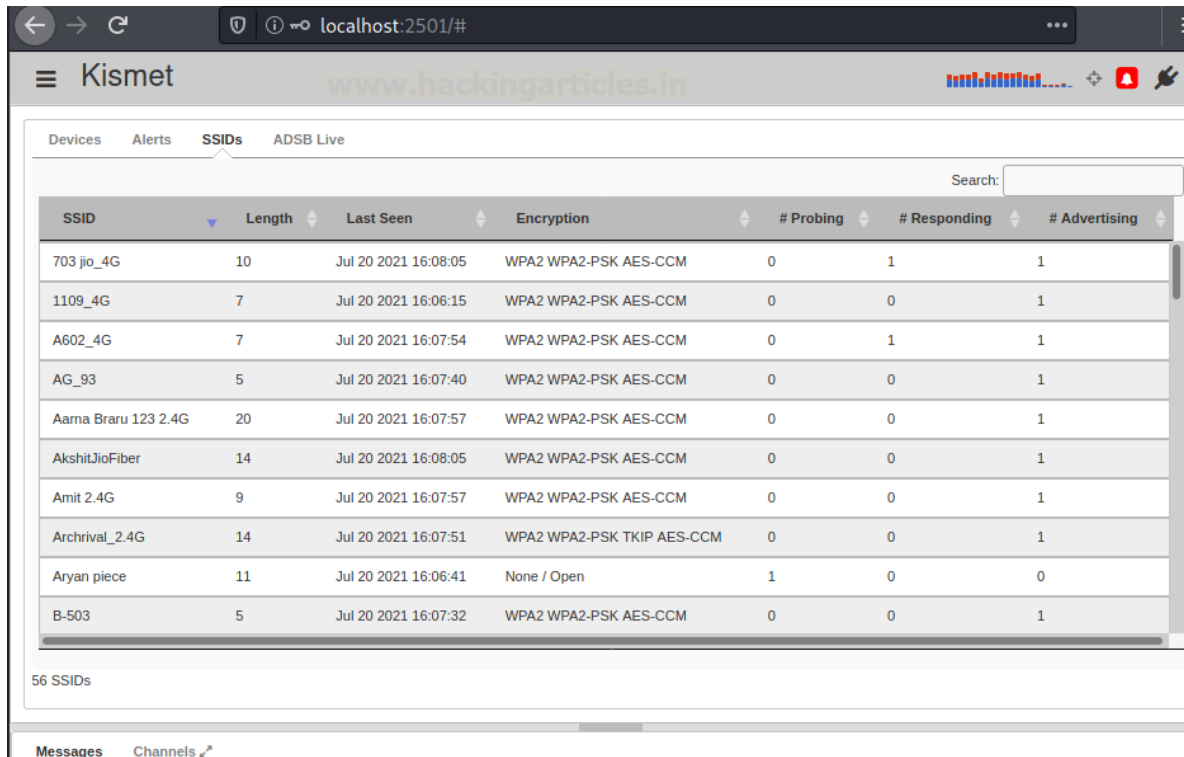


```

KISMET - Point your browser to http://localhost:2501 (or the address of this system) for
INFO: Registered PHY handler 'BTLE' as ID 6
INFO: Registered PHY handler 'RTLAMR' as ID 7
INFO: Indexing ADSB ICAO db
INFO: Completed indexing ADSB ICAO db, 322495 lines 6450 indexes
INFO: Registered PHY handler 'RTLADSB' as ID 8
INFO: Registered PHY handler '802.15.4' as ID 9
INFO: Could not open system plugin directory (/usr/lib/x86_64-linux-gnu/kismet/), skipping: No such file or directory
INFO: Did not find a user plugin directory (/root/.kismet/plugins/).

```

Kismet will enumerate neighboring WiFi networks along with their MAC address and Encryption type.



The screenshot shows the Kismet web interface in a browser window. The address bar shows 'localhost:2501/#'. The interface has a navigation bar with 'Devices', 'Alerts', 'SSIDs', and 'ADSB Live'. The 'SSIDs' tab is active, displaying a table of detected networks. A search bar is located at the top right of the table. The table has columns: SSID, Length, Last Seen, Encryption, # Probing, # Responding, and # Advertising. Below the table, it says '56 SSIDs'.

SSID	Length	Last Seen	Encryption	# Probing	# Responding	# Advertising
703 jio_4G	10	Jul 20 2021 16:08:05	WPA2 WPA2-PSK AES-CCM	0	1	1
1109_4G	7	Jul 20 2021 16:06:15	WPA2 WPA2-PSK AES-CCM	0	0	1
A602_4G	7	Jul 20 2021 16:07:54	WPA2 WPA2-PSK AES-CCM	0	1	1
AG_93	5	Jul 20 2021 16:07:40	WPA2 WPA2-PSK AES-CCM	0	0	1
Aarna Braru 123 2.4G	20	Jul 20 2021 16:07:57	WPA2 WPA2-PSK AES-CCM	0	0	1
AkshitJioFiber	14	Jul 20 2021 16:08:05	WPA2 WPA2-PSK AES-CCM	0	0	1
Amit 2.4G	9	Jul 20 2021 16:07:57	WPA2 WPA2-PSK AES-CCM	0	0	1
Archival_2.4G	14	Jul 20 2021 16:07:51	WPA2 WPA2-PSK TKIP AES-CCM	0	0	1
Aryan piece	11	Jul 20 2021 16:06:41	None / Open	1	0	0
B-503	5	Jul 20 2021 16:07:32	WPA2 WPA2-PSK AES-CCM	0	0	1

If you choose any Network ID it will depict the Wi-Fi configuration details. As you can see, we are interested in “SSID: AARTI” that has WEP encryptions (less secure and highly exploitable).

SSID: AARTI

✕

▼ Wi-Fi (802.11) SSIDs

SSID ⓘ

aarti (5 characters)

First Seen

Jul 20 2021 16:06:06

Last Seen

Jul 20 2021 16:09:59

Encryption ⓘ

WEP

Advertising APs ⓘ

▼ aarti - D8:47:32:E9:3F:33 - WEP

Advertising Device

View Device Details

MAC

D8:47:32:E9:3F:33 (TP-Link Technologies Ltd)

Name

aarti

Type

Wi-Fi AP

Advertised encryption ⓘ

WEP

First advertised

Jul 20 2021 16:06:06

Last advertised

Jul 20 2021 16:09:55

Last advertised SSID

aarti

Responding APs ⓘ

▼ aarti - D8:47:32:E9:3F:33 - WEP

Responding Device

View Device Details

MAC

D8:47:32:E9:3F:33 (TP-Link Technologies Ltd)

Name

aarti

Type

Wi-Fi AP

Advertised encryption ⓘ

WEP

First responded

Jul 20 2021 16:08:09

Last responded

Jul 20 2021 16:09:59

Last advertised SSID

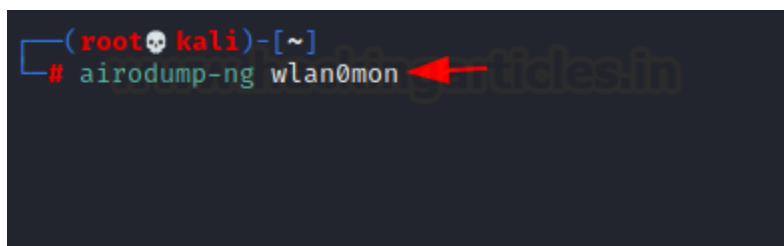
aarti

## Airodump-ng

Airodump-ng is included in the aircrack-ng package and is used for packet capturing of raw 802.11 frames. It is ideal for collecting WEP IVs for use with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng can log the coordinates of the discovered access points.

**Note:** To use this tool you may need an external wi-fi adapter.

```
airodump-ng wlan0mon
```



The following command monitors all wireless networks, frequency hopping between all wireless channels.

CH 11 ][ Elapsed: 6 s ][ 2021-07-20 16:13

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
F4:79:60:3B:55:58	-66	2	0 0	5	270	WPA2 CCMP	PSK	K 307
30:CC:21:E8:8E:EA	-73	2	0 0	5	130	WPA2 CCMP	PSK	Abhiraj
AA:DA:0C:58:34:FE	-67	3	0 0	10	130	WPA2 CCMP	PSK	<length: 0>
98:35:ED:D9:A1:B8	-1	0	0 0	7	-1			<length: 0>
18:45:93:69:A5:19	-21	1	2 0	9	130	WPA2 CCMP	PSK	raaj
68:14:01:5A:0E:9C	-61	2	0 0	1	195	WPA2 CCMP	PSK	Amit 2.4G
70:C7:F2:ED:6A:44	-65	2	0 0	4	130	WPA2 CCMP	PSK	ajoy
1A:59:C0:33:EB:8A	-67	1	4 0	13	360	WPA2 CCMP	PSK	riddikenator@orbi
E8:D0:B9:A3:12:F9	-67	2	0 0	7	270	WPA2 CCMP	PSK	Jasmeen_2G
AC:37:28:64:D5:C9	-70	0	0 0	9	130	WPA2 CCMP	PSK	Abhiaka
04:95:E6:63:6F:D8	-71	2	0 0	8	130	WPA2 CCMP	PSK	B-503
B0:08:75:19:83:50	-73	2	0 0	4	130	WPA2 CCMP	PSK	Mayank-A

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
98:35:ED:D9:A1:B8	52:83:23:F2:A8:94	-76	0 - 1	0	2		
(not associated)	38:A4:ED:CF:8E:8D	-48	0 - 1	0	2		
(not associated)	CA:7B:54:EE:02:1D	-70	0 - 1	10	4		Kavz_5G
(not associated)	96:D9:7A:8D:95:18	-74	0 - 1	0	1		
(not associated)	F8:E4:E3:9E:24:9C	-76	0 - 1	0	1		MetNet
18:45:93:69:A5:19	2A:84:98:9F:E5:5E	-20	1e- 1e	126	8		

## Wash

Wash is a tool for discovering WPS-enabled access points. It may either survey from a live interface or scan a list of pcap files. Wash is included in the Reaver package. It comes preinstalled in Kali Linux and you can execute the following command for SSID discovery.

```
wash -i wlan0mon
```

**Note:** To use this tool you may need an external wi-fi adapter.

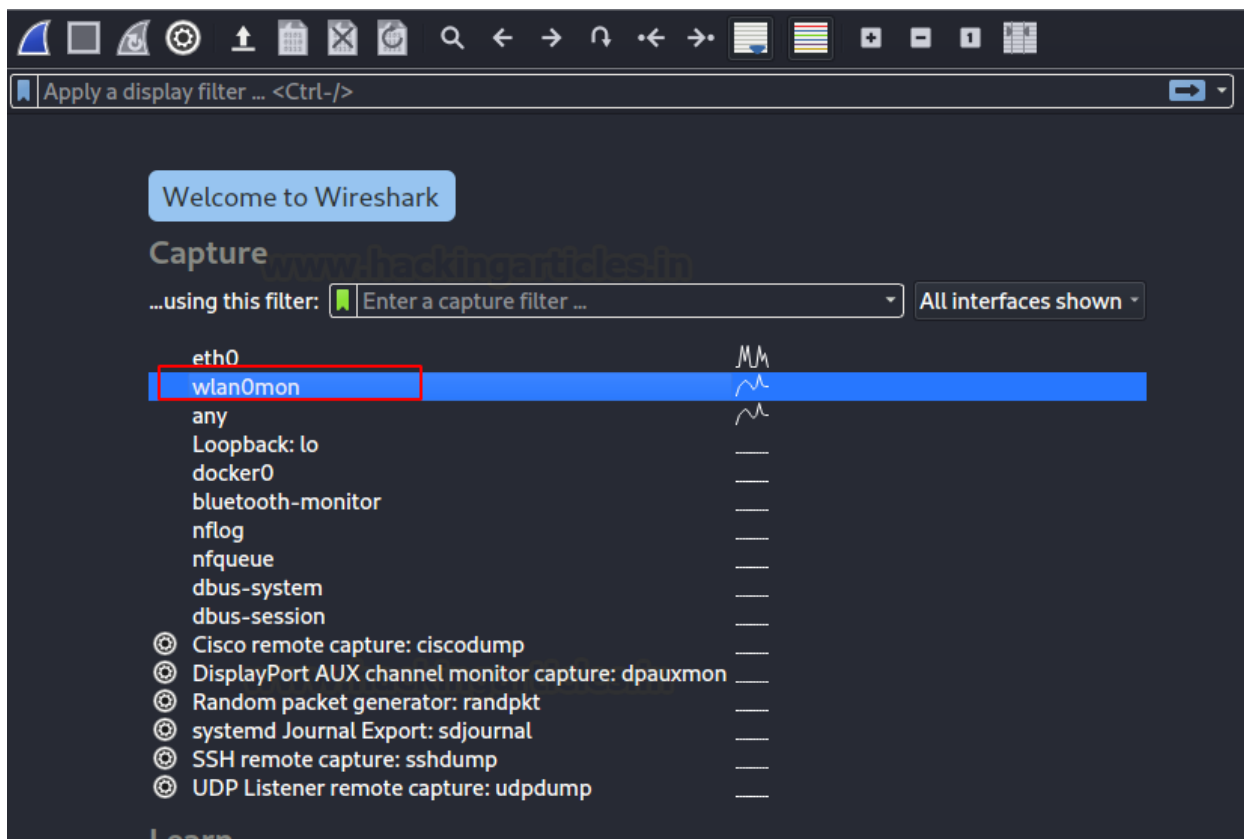
```
(root@kali)-[~]
# wash -i wlan0mon
```

BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
68:14:01:5A:0E:9C	1	-65	2.0	No	Broadcom	Amit 2.4G
68:14:01:0B:BB:B5	1	-71	2.0	No	Broadcom	Aarna Braru 123 2.4G
96:FB:A7:54:C1:F4	1	-73	1.0	No	RalinkTe	(null)
68:14:01:34:B9:E3	1	-71	2.0	No	Broadcom	JioFiber-QwXYk
40:49:0F:3C:49:88	1	-57	2.0	No	Broadcom	Sachin 2.4
68:14:01:6A:F1:57	1	-69	2.0	No	Broadcom	Jas303 2.4G
18:82:8C:F2:5C:C8	1	-75	2.0	No	Broadcom	Vikash jio_4G
68:14:01:35:45:96	1	-79	2.0	No	Broadcom	Mohsinhind 2.4 G
40:49:0F:0A:AB:D6	1	-75	2.0	No	Broadcom	203 Jio 2.4 G
A8:DA:0C:B3:65:99	1	-75	2.0	No	Broadcom	1109_4G
18:82:8C:ED:86:CA	1	-79	2.0	No	Broadcom	Marvel
68:14:01:3A:AF:3A	1	-75	2.0	No	Broadcom	Durgesh 2.4G
96:FB:A7:54:F1:26	2	-75	1.0	No	RalinkTe	(null)
94:FB:A7:64:F1:26	2	-75	1.0	No	RalinkTe	Ankush 4G
30:CC:21:E3:47:88	3	-49	2.0	No		Vikas

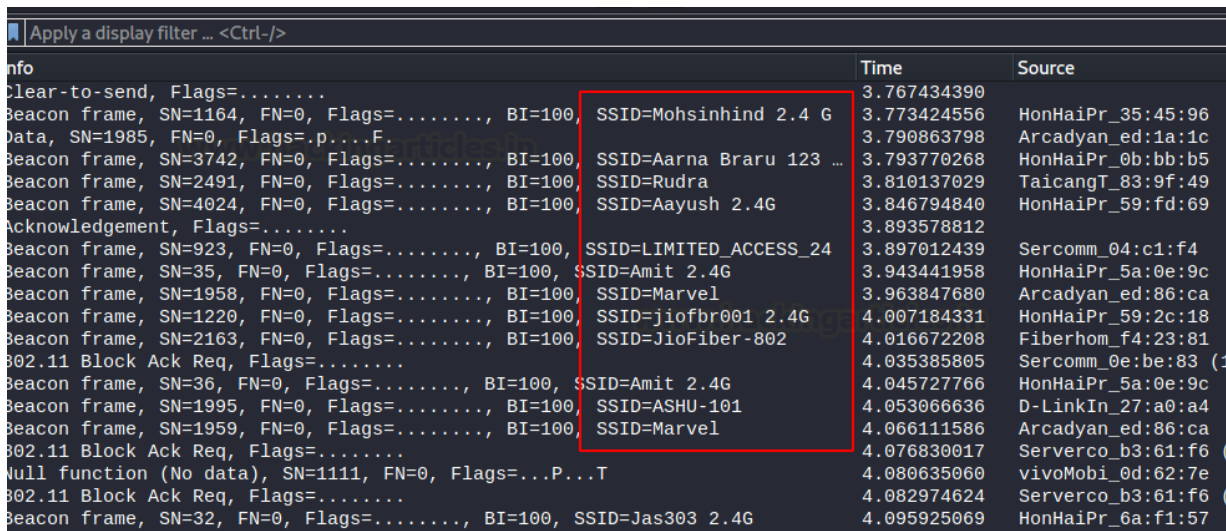
## Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is also WAN/LAN Analyzer and Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

**Note: To use this tool you may need an external wi-fi adapter for SSID discovery.**



Start Wireshark and choose the interface for the Wi-Fi adapter and it will list all network ID available in the surroundings.



# JOIN OUR TRAINING PROGRAMS

