

# KaliTut</>

Home » Tutorials » Wifi Hacking » How to decrypt WiFi traffic in Wireshark

## How to decrypt WiFi traffic in Wireshark

*How to decrypt Wi-Fi traffic in Wireshark with kali linux*



Walid Salame  7:48 PM

 0

Share it:

 Facebook

 Twitter

 G+

 P

 in

 t

## Decrypt WPA traffic in Wireshark

Let's start with the theory to understand why the process of decrypting WiFi traffic in Wireshark requires some effort and why one cannot simply decrypt any captured WiFi traffic even if there is a password from the Access Point.



When transmitting over WiFi, the traffic is encrypted using PTK (the Pairwise transient key can be translated as a Pair of Transition Key). At the same time, PTK is dynamic, that is, it is created anew for each new connection. Thus, it turns out that WiFi traffic for each connection in the same Access Point is encrypted with different PTK, and even for one Client after reconnection, PTK changes. To calculate PTK, you need data from a four-stage handshake, as well as a password from a WiFi network (in fact, you also need other information, such as the network name (SSID), but obtaining this data is not a problem).

#### Contents

1. Capturing WiFi traffic in Airodump-ng
2. Decryption of WiFi traffic in Wireshark
3. Capture WiFi in Wireshark

The main thing you need to understand: to decrypt WiFi traffic, you need a four-landmark handshake. And not any, but exactly the one that happened to transmit the traffic that needs to be decrypted. But to use the captured handshake you need a password from the WiFi network.

So, to **decrypt WiFi traffic** is needed:

1. a handshake that occurred between the Client and the Access Point immediately prior to the exchange of decrypted information
  1. for this we need Monitor Mode WiFi adapter
2. password to connect to the Access Point

Next will be shown two examples of capturing WiFi traffic and its decryption. The first data capture is performed using Airodump-ng , and then the wireless traffic will be decrypted in Wireshark. In the second example, the data will be captured and decrypted using only Wireshark .

# Capturing WiFi traffic in Airodump-ng

In order for the data to be suitable for decryption, it is necessary that the WiFi card does not switch channels, but to capture information on one channel on which the target Access Point operates. Therefore, we start by collecting information about the target access point.

We look at the names of wireless interfaces:

```
1 | iw dev
```

We translate the INTERFACE into the monitor mode with commands like this:

```
1 | sudo ip link set INTERFACE down
2 | sudo iw INTERFACE set monitor control
3 | sudo ip link set INTERFACE up
```

Change **INTERFACE** with your WiFi adapter name

Run airodump-ng with a command like:

```
1 | sudo airodump-ng wlan0mon
```

For example, I want to capture and decrypt traffic for the Kali Access Point, which operates on channel 5.



Then I need to restart airodump-ng with a command like this:

```
1 | sudo airodump-ng wlan0mon --channel CHANNEL --write FILE NAME
```

The **WPA handshake** inscription says that a four-stage handshake was captured. It means that:

- Now we can decrypt the WiFi data (**if we have the key to the WiFi network**)
- we can only decrypt data for a specific client (with which a handshake was made)
- we will be able to decrypt the data that was sent only after this captured handshake

## Decryption of WiFi traffic in Wireshark

Open the capture file in Wireshark. In its original form, traffic looks like this:





That is, without decryption, we see only the MAC addresses of the data transfer participants, some types of packets, as well as data packets — in which the payload is encrypted.

Before decoding, make sure that there is a handshake, otherwise there is no point in continuing:

```
1 | eap01
```



Before decoding, we need to make some changes in the IEEE 802.11 protocol settings.

Go to **Edit** → **Preferences** , expand the **protocol** section and select **IEEE 802.11** . The settings should be:

make sure you have the same settings as in the previous screenshot, click on the Edit button next to Decryption Keys (to add a WEP / WPA key):



Click the **Create** button . In the window that opens, in the **Key type** field, select **wpa-pwd** , enter the password for the WiFi network, and after the colon, enter the network name (SSID) and click OK.

For example, in my case, the password is qivxy17988, and the network name is Kali, then I enter:

1 | qivxy17988:Kali

Click Apply :

Traffic will be decrypted:





Now there are visible DNS, HTTP requests and responses, as well as other network packets.

If traffic is captured not only for this network, but also for other networks operating on the same channel, or for this network but other clients for which no handshakes are taken, then this traffic will not be decrypted.

## Capture WiFi in Wireshark

**WiFi traffic can be captured directly in Wireshark.**

But we first need to switch the WiFi card to the same channel as the target Access Point. This is done by commands like:

```
1 sudo ip link set INTERFACE down
2 sudo iw INTERFACE set monitor control
3 sudo ip link set INTERFACE up
4 sudo iw dev INTERFACE set channel
```







## WANNA GET OUR AWESOME NEWS?

Sign up and get the best stories straight into your inbox!

Enter your email address...

Subscribe Now

\* we won't spam you



Next

Intercept Passwords With Wireshark

Previous

How to increase WiFi TXPower



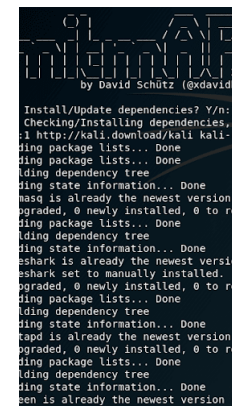
## Tutorials

Statistics   Telephony   Wireless   Tools		
	Destination	Protocol
80	Netgear_88:ac:82	EAP
82	Netgear_7e:40:80	EAP
80	Netgear_88:ac:82	EAP
82	Netgear_7e:40:80	EAP

```
1 00:00:00:00:00:00 Unknown
2 00:15:60:9A:26:C0 Anan Apartment WPA (0 handshake)
3 00:15:60:9C:28:84 Anan Apartment WPA (0 handshake)
4 00:27:22:02:0C:00 Anan Apartment WPA (0 handshake)
5 00:AA:77:00:50:AA No data - WEP or WPA
6 04:4F:76:07:BC:05 Porsee_2G No data - WEP or WPA
7 0C:5A:5A:5A:AA:11 Tonyhooza No data - WEP or WPA
8 10:87:13:0F:C7:58 Anan Apartment No data - WEP or WPA
9 10:87:13:0F:C7:59 wllwllboon2 No data - WEP or WPA
10 10:87:13:0F:C7:60 NETGEAR_ORB_2B No data - WEP or WPA
11 10:87:13:0F:C7:61 NETGEAR_ORB_1_hidden57 No data - WEP or WPA
12 10:87:13:0F:C7:62 No data - WEP or WPA
13 10:87:13:0F:C7:63 07206 No data - WEP or WPA
14 10:87:13:0F:C7:64 AndroidAP WPA (0 handshake)
15 10:87:13:0F:C7:67 true_home2_442 No data - WEP or WPA
16 10:87:13:0F:C7:68 true_home2_106 No data - WEP or WPA
17 10:87:13:0F:C7:69 058728282 No data - WEP or WPA
18 10:87:13:0F:C7:6A PURE_FONETUNE No data - WEP or WPA
19 10:87:13:0F:C7:6B Boochu2 No data - WEP or WPA
20 14:07:0F:7B:07:0A 334_2G No data - WEP or WPA
21 18:A6:9F:7A:50:00 naskingofny_3_40Hz No data - WEP or WPA
22 18:0A:C7:48:32:80 WPA-PSK 2_40Hz No data - WEP or WPA
23 20:89:6F:FF:8E:9A:92 Kabilza No data - WEP or WPA
24 2C:08:8C:1A:48:62 Boochu2 WPA (0 handshake, with PWEID)
25 2C:08:8C:1A:48:62 Boochu2 No data - WEP or WPA
26 2C:08:8C:1A:48:62 alilithon2 No data - WEP or WPA
27 2C:08:8C:1A:48:62 naupaya_20 No data - WEP or WPA
28 2C:08:8C:1A:48:62 casper No data - WEP or WPA
29 38:4C:4F:08:46:08 Sunday No data - WEP or WPA
30 3C:71:4F:C5:0A:0C Cody No data - WEP or WPA
31 40:30:8C:18:52:10 true_home2_442 WPA (0 handshake, with PWEID)
32 40:30:8C:1A:48:62 Pangchai WPA (0 handshake, with PWEID)
33 40:30:8C:18:52:10 The Local Barz_2G_TEST No data - WEP or WPA
34 40:30:8C:1A:48:62 true_home2_606 No data - WEP or WPA
35 40:30:8C:18:52:10 true_home2_106 WPA (0 handshake, with PWEID)
36 40:30:8C:1A:48:62 Paangoon_20 WPA (0 handshake, with PWEID)
37 40:30:8C:1A:48:62 paishopos No data - WEP or WPA
38 48:55:5F:0C:63:88 Wateen_2_40 No data - WEP or WPA
39 38:05:68:65:71:8A AccountTop Room No data - WEP or WPA
40 38:07:59:18:03:9C Private745 No data - WEP or WPA
41 40:30:8C:1A:48:62 true_home2_106 No data - WEP or WPA
42 40:2E:20:0A:44:8C Sneavillao No data - WEP or WPA
43 40:2E:20:0A:44:8C anile home No data - WEP or WPA
44 70:4F:15:71:3C:80 PARD No data - WEP or WPA
45 70:4F:15:71:3C:80 Andrew Tiew No data - WEP or WPA
```



LECTIVE JAMMING  
OF  
WIFI NETWORKS  
AND CLIENTS



## WPA2 Half Handshake attack

🕒 Jun 08 2019

## Hacking Wifi using PMKID and Aircrack-ng

🕒 Jun 08 2019

## Hacking WiFi without users using PMKID attack

🕒 Jun 07 2019

## Selective jamming of WiFi networks and clients

🕒 Jun 07 2019

## mitmAP WiFi access point intercept passwords

🕒 May 31 2019

### Post A Comment:



0 comments:

Enter your comment...



Comment as:

Google Account ▼

Publish

Preview

### Social Widget



6.7K



22k



4.1K



3.9K

### Popular Posts

---

## Fix Kali Linux sources.list Repositories

Fix default repository First after installing a clean Kali Linux the sources.list contains only tow repository and they are ## Regul...

## Useful Commands for Kali Linux

New to Kali Linux ? or to Linux world at all ... welcome to this new experience i'm sure you will enjoy once you start to try ... an...

## Password dictionary

hi Guys how are you ? Looking for wordlist password ? password list ? ? they are all the same and you are on the right place :) ...

## how to update Kali Linux and Fix update error

Kali Linux's the great Penetration testing system is like any other system in the world it need to be updated, Most of the update is not ...

## infernall twin Automated Evil Twin Attack

Automated Evil Twin Attack: infernall-twin Evil twin is a term for a fake WiFi access point, it appears to be a legitimate one offered on t...

---

## Labels

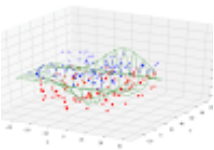
▶ Android	(5)
▶ Books	(11)
▶ Cyber Security	(4)
▶ Kali Linux	(17)
▶ Linux	(6)

▶ Linux Commands	(14)
▶ MITM	(1)
▶ Network Administrator	(3)
▶ Penetration Testing Tools	(12)
▶ Raspberry Pi	(132)
▶ Tutorials	(11)
▶ Video Tutorials	(29)
▶ WiFi Adapter	(7)
▶ Wifi Hacking	(40)

 Recent

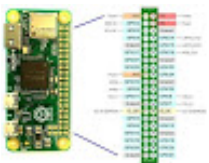
 Random

 Comment



### What is data science

🕒 Sep 15 2019



### Raspberry Pi Zero W Review

🕒 Sep 11 2019





## Raspberry Pi Camera Board V2 Overview

🕒 Sep 10 2019



## Raspberry pi zero w camera

🕒 Sep 10 2019



## best laptop for Kali Linux

🕒 Aug 07 2019

A blog dedicated to Penetration Testing, Tutorials on hacking and security

KaliTut © 2016-2017. All Rights Reserved.