

Forum:[Hack Forums](#)

Thread: [Capturing 2.4GHz Wi-Fi Handshakes with a CYD ESP32 & Cracking with Hashcat](#)

Wake - April 3, 2026, 9:49 pm

Capture 2.4 GHz Wi-Fi Handshakes with a CYD ESP32 and Crack with Hashcat.

????????????????????????????????

Written by [Wake](#)

????????????????????????????????

Disclaimer

This thread Is for informational and educational purpose only. I will not be responsible for any action performed by any reader.

Introduction

In this tutorial I will be covering WPA and its levels, 2.4 and 5 GHz network bands, how to capture and crack insecure Wi-Fi passwords, what a CYD ESP32 Is, what an EAPOL handshake attack Is, what Hale Hound is, what hashcat is, And how to prevent this from happening to ourselves.

What will I need for this?

[+] SD card

[+] CYD ESP32

[+] SD Card reader

[+] Wireless Network you have permission to test

[+] HaleHound (CYD ESP32 Firmware)

[+] Hashcat

What is a CYD ESP32?

A CYD ESP32 or more commonly called Cheap Yellow Display is a low-cost ESP32 development board. The CYD ESP32 contains Bluetooth Wi-Fi and a built in TFT touch screen display making them great for portable projects or custom interfaces. The ESP32 chip is the brains of the board It's a micro controller that runs the display, Wi-Fi, Bluetooth, communicating with hardware through GPIO pins etc and running your code.

The ESP32 can only connect to 2.4 GHz Wi-Fi because its hardware is designed for that frequency. This keeps it cheap, low power, with better range, which is great for IoT devices. This does mean it can't communicate with 5 GHz Wi-Fi networks, though meaning that we will only be able to use this to interact with 2.4 GHz Wi-Fi networks.

2.4 GHz isn't outdated; it's still widely used. Some networks still use it alone. It's just not the safest option anymore. 2.4 GHz Wi-Fi has better range and better wall penetration, also works well with older and low power devices. The downsides are it is slower than 5 GHz and sometimes there can be more interference. Most modern routers use dual band, which will detect what is the best option for your device automatically when you join the network.

What is an SD card?

An SD card is a storage device used to save and move files between devices. We will be using this to install Hale Hound onto the CYD ESP32 and then using it later again to transfer the handshake files we capture onto our computer.

What is a SD Card reader?

An SD card reader is a device that allows your computer to read and transfer data from an SD card. While this is fairly straightforward, we need it to move files from the CYDESP32's SD card onto our computer so we can work with them.

Why do we need a Wi-Fi Network you have permission to test?

Accessing or interfering with a network without permission can be illegal in many places. In this setup, we'll be sending packets that can affect how a network behaves, so it's important to only use a network you own or have explicit permission to test.

Using your own network also means you won't disturb other people, and you can safely test and repeat steps as needed. It gives you full control over the setup, including the router, connected devices, and passwords.

What is HaleHound?

HaleHound is an open source firmware designed for the CYD ESP32. It was developed by Jesse Hale and is designed to turn an inexpensive cheap yellow display into a powerful handheld penetration testing and auditing tool. These devices with this firmware and similar firmware often get nicknamed as "Budget Flipper Zero's" due to their portability and range of features. I highly encourage you to go check out HaleHound; it can be found [here](#). It includes many more features than are covered in this tutorial, and the full GitHub page is worth reading if you want to explore everything it can do.

What is Hashcat?

Hashcat is a password recovery tool used to crack hashed data. Hashcat runs on Windows, Linux, and macOS. Instead of targeting systems directly, it works by taking a hash (an encrypted version of data) and trying to find the original value. Hashcat is commonly used to recover passwords from captured data using methods such as

[+] brute-force attacks

[+] dictionary attacks

[+] rule-based attacks

Hashcat Is considered one of the fastest and most advanced password cracking utility in the world, especially when using a GPU, making It one of the most efficient tools for password recovery.

What Is WPA?

WPA stands for Wi-Fi Protected Access a security protocol designed to secure wireless networks. WPA uses encryption to prevent unauthorised access with variants like, WPA2 and WPA3 that are now standard.

[+] WPA officially released in 2003 was introduced to address critical security vulnerabilities with WEP (Wired Equivalent Privacy).

[+] WPA2 was introduced in 2004 and introduced a stronger encryption system. Becoming the standard for many years.

[+] WPA3 Is the most secure standard and was released in 2018 with security improvements again this time forcing attackers to interact directly with the router for each password guess and making password guessing significantly slower using SAE (Simultaneous Authentication of Equals) This prevents traditional offline dictionary attacks. For this tutorial we will be focusing on a network with WPA/WPA2 encryption.

What is a EAPOL attack?

An EAPOL handshake attack Is best explained as imagining your Wi-Fi network as a locked door when something wants to connect It isn't going to shout the password out loud instead they perform a handshake to prove to the router that your device knows the password so the attack would go something like this.

[+] A device connects to Wi-Fi

[+] It does the secret handshake

[+] We listen and record that handshake

[+] Later we use hashcat and password lists to try find a match.

Normally when listening for a handshake we have to wait for a device to connect to the network to capture that handshake now we could be waiting minutes or hours it just depends when and If something connects. We are going to deauth the network to speed this up so the process Is the same as before but now when we are listening and deauth when that device tries to reconnect automatically we capture the handshake instantly. This only works on WPA/WPA2 which is the networks encryption we will be focusing on. Newer WPA3 networks are designed to prevent this type of offline attack.

How do I do this?

The first step to doing this Is flashing Hale Hound to your CYD ESP32 SD card (I won't be covering how to flash it to the SD card on this thread feel free to message me If you need help)

[+] Once we power on our CYD ESP32 you'll be greeted with a warning screen. Press to continue

past the warning screen.

[+] Inside the main menu, you'll see all the sub menus and options that we have. Remember to check out the GitHub for more information on all of these. Today we will be focusing on SIGINT. Click that menu to access it.Spoiler [\(Click to View\)](#)

[+] Inside the SIGINT menu we now have a few options EAPOL Capture, Karma Attack, Wardriving, Saved Captures, IoT Recon and Loot we are going to come back to these options later but for now we can go ahead and press EAPOL Capture.Spoiler [\(Click to View\)](#)

[+] The device will now scan for Wi-Fi networks around us we need to select our network we have setup for testing for this example my test network is "EpsonColorSwap" Select your test network. Spoiler [\(Click to View\)](#)

[+] Once we select our network we will be taken to a next screen with the option to deauth, go ahead and press deauth. This will send deauthentication packets while listening for a handshake, forcing the client to reconnect and speeding up capture.

[+] Once the handshake has been captured we are greeted with a flashing bar saying "Handshake captured!" and some text in a box just above the deauth button we pressed earlier. Press stop to stop deauthing the network.Spoiler [\(Click to View\)](#)

[+] Press save to save this hand shake, Hale Hound will attempt to save it as a hashcat .hc22000 file for us for convenience.

[+] Now we can back out and we will be greeted with the options where we chose EAPOL capture before this time press "Loot" and we can see we have two files under EAPOL go ahead and press EAPOL and enter that section.Spoiler [\(Click to View\)](#)

[+] Inside that section we can see the name of the files which will be the SSID of the network and on the right hand side we can see the file type. One PCAP and one HC22000.Spoiler [\(Click to View\)](#)

[+] Now back out of everything completely to main menu and power down your CYD ESP32 its time to remove the SD card and move over to our machine.Spoiler [\(Click to View\)](#)

[+] Once the SD card is removed plug it into the SD card reader and plug that into your machine. Spoiler [\(Click to View\)](#)

[+] Back on our machine we need to make sure we have Hashcat installed for this example I am on macOS for this example so I will install it using the command "brew install hashcat" and wait for it to install.Spoiler [\(Click to View\)](#)

[+] To test hashcat is working we can enter Hashcat --help and enter this will show us most of the Hashcat commands.

[+] I'm going to go ahead and clear that and change directory to where my wordlist is. My word list is in my Downloads folder so I will use cd Downloads (cd=change directory and Downloads is the directory we would like to change to)

[+] Inside the Downloads folder we can type ls to show the contents of the folder. For this test I will be using a very well known wordlist called rockyou.txt.

[+] Now before I mentioned Hale Hound will try to save the PCAP file as a .HC22000 for you but I have found It Isn't always that reliable so we are going to convert this file ourselves. To do this I will

start by copying the PCAP file from our SD card to our Downloads file so its in the same directory as our wordlist. Than we need to head over to this [website](#) put your PCAP file In and It will convert it to a .HC22000 for you.

[+] Now with our PCAP converted to a .HC22000 replace the PCAP file in your Downloads with this newly converted file. I am going to rename it to something easier also.Spoiler ([Click to View](#))

[+] Now we can head back to Terminal and enter hashcat -m 22000 Test.hc22000 rockyou.txt (Enter your .HC22000 file name and wordlist where I have entered mine)

Lets break down that command. hashcat starts and runs the hashcat program, 22000 specifies the hash type 22000 = WPA/WPA2, Test.HC22000 is our input hash file which contains our captured handshake and rockyou is our wordlist we are using and hashcat will try each password in this file. Press Enter on that command.Spoiler ([Click to View](#))

[+] While we let this run we can enter "s" at any time to see the status and this will update us on our progress and how far through our password list hashcat has got.

[+] When hashcat has finished we can scroll up to see our cracked handshake. If the password to the handshake isn't in your wordlist hashcat won't find it, it may take more than one wordlist.Spoiler ([Click to View](#))

[+] When we now go to our Wi-Fi network list and find EpsonColorSwap we can enter that password and connect.

[+] We have successfully connected and are now on the network and If you followed the steps in this tutorial you will have too.

????????????????????????????????

How can I protect myself from this?

Your Wi-Fi password Is a key Hackers are going to try lots of keys until one works, the best way to counter this Is to use a long strong password with capitals and random numbers/symbols. Some people use random phrases some people use abbreviated phrases, what ever you use make it strong with capitals numbers and symbols If possible.

Set your router to WPA3 If possible most modern routers use It as standard If your router doesn't make sure Its updated.

The attack I showed only works If some one captures your handshake and If the password Is weak, If your password Is strong enough they can try for ever and still fail.

[Thank you for taking the time to read this thread. If you enjoyed this please check out the rest of my tutorials and write-ups](#)

CL1B - April 4, 2026, 11:22 am

What a good read. I'm now tempted to buy a board, I've never gotten into that side of hacking.

Thank you for posting! Tagging a few members who might like this read as well: [HerrWinston](#) [Immortal itcorp](#)

Wake - April 4, 2026, 11:45 am

(Apr 4, 2026 11:22 AM)MarlboroMan Wrote: [\[CITE\]](#) What a good read. I'm now tempted to buy a board, I've never gotten into that side of hacking.

Thank you for posting! Tagging a few members who might like this read as well: [HerrWinston](#)
[Immortal itcorp](#)

Thank you for taking the time to read this, Very appreciative of you tagging people who may be interested also.

I've really been enjoying working with IoT devices and this side of things. I've already made a few more tutorials like this, and I've got plenty more planned.

If you're thinking of picking up a board, just a quick tip—don't get caught out by Amazon prices. You can usually find them much cheaper on AliExpress. Just make sure to buy from a reputable seller, as quality can vary quite a bit.

C00Lssh - April 9, 2026, 11:54 pm

Oh the fun of Wi-fi Handshake capturing.

Brings me to the days when i had my Wi-fi Pineapple with my deauth tool that i would use to send deauth packets with to capture the psk handshakes.

I might have to dig up the ole flipper and de-auther :P.

Thanks for the memories! Solid read/post!

Wake - April 10, 2026, 7:06 am

(Apr 9, 2026 11:54 PM)C00Lssh Wrote: [\[CITE\]](#) Oh the fun of Wi-fi Handshake capturing.

Brings me to the days when i had my Wi-fi Pineapple with my deauth tool that i would use to send deauth packets with to capture the psk handshakes.

I might have to dig up the ole flipper and de-auther :P.

Thanks for the memories! Solid read/post!

Your very welcome thanks for reading! Does Wi-Fi Pineapple have Wi-Fi 6? I would be interested into looking into them.

C00Lssh - April 10, 2026, 8:06 am

i believe they have 5GHz addon, but have not gotten 6GHz yet.

<https://shop.hak5.org/products/wifi-pineapple>.

i have/had a few of their devices. pretty neat fun little gadgets.

Wake - April 10, 2026, 8:36 am

(Apr 10, 2026 08:06 AM)C00Lssh Wrote: [\[CITE\]](#) i believe they have 5GHz addon, but have not gotten 6GHz yet.

<https://shop.hak5.org/products/wifi-pineapple>.

i have/had a few of their devices. pretty neat fun little gadgets.

Looks like a fun bit of tech it even has its own web console, which is pretty cool. A bit pricey though.

Keep an eye on my threads, I've got something coming up that's very similar to a Pineapple, around 90% cheaper also!

C00Lssh - April 10, 2026, 8:37 am

(Apr 10, 2026 08:36 AM)Wake Wrote: [\[CITE\]](#) Looks like a fun bit of tech it even has its own web console, which is pretty cool. A bit pricey though. Keep an eye on my threads, I've got something coming up that's very similar to a Pineapple, around 90% cheaper also!

Yea, it is very pricey. I bought it at DEFCON24 when Hak5 was there so it was a lot cheaper.

Wake - April 10, 2026, 8:39 am

(Apr 10, 2026 08:37 AM)C00Lssh Wrote: [\[CITE\]](#) Yea, it is very pricey. I bought it at DEFCON24 when Hak5 was there so it was a lot cheaper.

Love a good discount going to have to try attend one of those events one day.

d3athgiver - April 10, 2026, 10:19 pm

(Apr 10, 2026 07:06 AM)Wake Wrote: [\[CITE\]](#) Your very welcome thanks for reading! Does Wi-Fi Pineapple have Wi-Fi 6? I would be interested into looking into them.

Pineapple only have 2.4 . You must buy the mk7 adaptor to add 5ghz support so I don't think it support wifi6 currently. It's pricy but handle everything, allow you to make a cnc with 9 other pineapple and more. You can build one for really cheap too.

Wake - April 11, 2026, 9:00 am

(Apr 10, 2026 10:19 PM)d3athgiver Wrote: [\[CITE\]](#) Pineapple only have 2.4 . You must buy the mk7 adaptor to add 5ghz support so I don't think it support wifi6 currently. It's pricy but handle everything, allow you to make a cnc with 9 other pineapple and more. You can build one for really cheap too.

Now you got me looking into DIY pineapple builds lol, have you built your own before?

DeathPenalty666 - April 11, 2026, 10:02 am

(Apr 11, 2026 09:00 AM)Wake Wrote: [\[CITE\]](#) Now you got me looking into DIY pineapple builds lol, have you built your own before?

Let me answer for my friend. Yeah he did but this setup is FAR from the quality of the original pineapple. There is a list of compatible router with the firmware ready to work on somewhere and if you are skilled you can even compile it for device not listed. With enough storage, enough usb port to handle a usb stick and a couple wifi adaptor this is not bad at all!! If you like those things maybe the liligo devices are for you!! The T-Dongle S3 with wifi and bluetooth cost around \$12, can do hwid injection attack with different option like detect the system os (linux windows android) and run the selected hwid attack, can be used via bt or wifi to send command to the machine, badusb attack, run a vnc and much more. Very cheap device but interesting hehe.

<https://github.com/0x29aNull/WiFi-Pineapple>

Wake - April 11, 2026, 10:43 am

(Apr 11, 2026 10:02 AM)DeathPenalty666 Wrote: [\[CITE\]](#) Let me answer for my friend. Yeah he did but this setup is FAR from the quality of the original pineapple. There is a list of compatible router with the firmware ready to work on somewhere and if you are skilled you can even compile it for device not listed. With enough storage, enough usb port to handle a usb stick and a couple wifi adaptor this is not bad at all!! If you like those things maybe the liligo devices are for you!! The T-Dongle S3 with wifi and bluetooth cost around \$12, can do hwid injection attack with different option like detect the system os (linux windows android) and run the selected hwid attack, can be used via bt or wifi to send command to the machine, badusb attack, run a vnc and much more. Very cheap device but interesting hehe.

<https://github.com/0x29aNull/WiFi-Pineapple>

The DIY Pineapple sounds interesting something I will probably end up building, what are you running on your Liligo? They have got quite expensive from what I have seen.

Cooligan - April 26, 2026, 1:18 am

Great guide [Wake](#) - very informative and easy to understand.

I didn't know about HaleHound before this thread but am glad I do now. Looks like a very interesting and useful tool. Sort of reminds me of a Flipper Zero and/or other physical hacking devices such as ones from Hak5 for example.

Hashcat however, everyone should know about Hashcat by now. Incredibly useful tool.

As for WPA - I think you might be shocked to find out how many devices are still using outdated WPA protocols. Scenario: If I walk around in my city (major city/tons of people & residences), if I pull out my phone and go to my Bluetooth settings, almost every single time I'll see 20-40+ WiFi devices that I can connect to and have full control of. This can range anywhere from TV's to smart fridges. Most of the time when someone buys a new TV, or a new device that has WiFi capabilities, they don't think about adding security to it, or a custom WiFi/WPA password. Very often they're still using default passwords given by the company that are 100% meant to be changed upon service-start.

It turned from messing around at a friends house and controlling the TV in the living room to make everyone think the house is haunted, to now, where seemingly anywhere I go in a populated area, there's loads of very weak security devices.

Wake - April 26, 2026, 3:58 am

(Apr 26, 2026 01:18 AM)Cooligan Wrote: [CITEI](#) Great guide [Wake](#) - very informative and easy to understand.

I didn't know about HaleHound before this thread but am glad I do now. Looks like a very interesting and useful tool. Sort of reminds me of a Flipper Zero and/or other physical hacking devices such as ones from Hak5 for example.

Hashcat however, everyone should know about Hashcat by now. Incredibly useful tool.

As for WPA - I think you might be shocked to find out how many devices are still using outdated WPA protocols. Scenario: If I walk around in my city (major city/tons of people & residences), if I pull out my phone and go to my Bluetooth settings, almost every single time I'll see 20-40+ WiFi devices that I can connect to and have full control of. This can range anywhere from TV's to smart fridges. Most of the time when someone buys a new TV, or a new device that has WiFi capabilities, they don't think about adding security to it, or a custom WiFi/WPA password. Very often they're still using default passwords given by the company that are 100% meant to be changed upon service-start.

It turned from messing around at a friends house and controlling the TV in the living room to make everyone think the house is haunted, to now, where seemingly anywhere I go in a populated area, there's loads of very weak security devices.

Thank you for reading and your kind words, 100% agree with you about this being similar to a Flipper Zero only bonus is this has Wi-Fi built in.

On the Flipper Zero you need an external wireless board even for 2.4 GHz and even then it becomes quite cumbersome and easy to spot.

Used to love messing with my Parents network and connected devices when I lived at home lol you're not wrong at all I live near lots of hotels and most of these have networks called things like "Hotel Smart Devices" I love IoT devices they have been a focus of mine for some years but purely for ease of access of the customer and making them "easier" to connect to they are left exposed and vulnerable.

