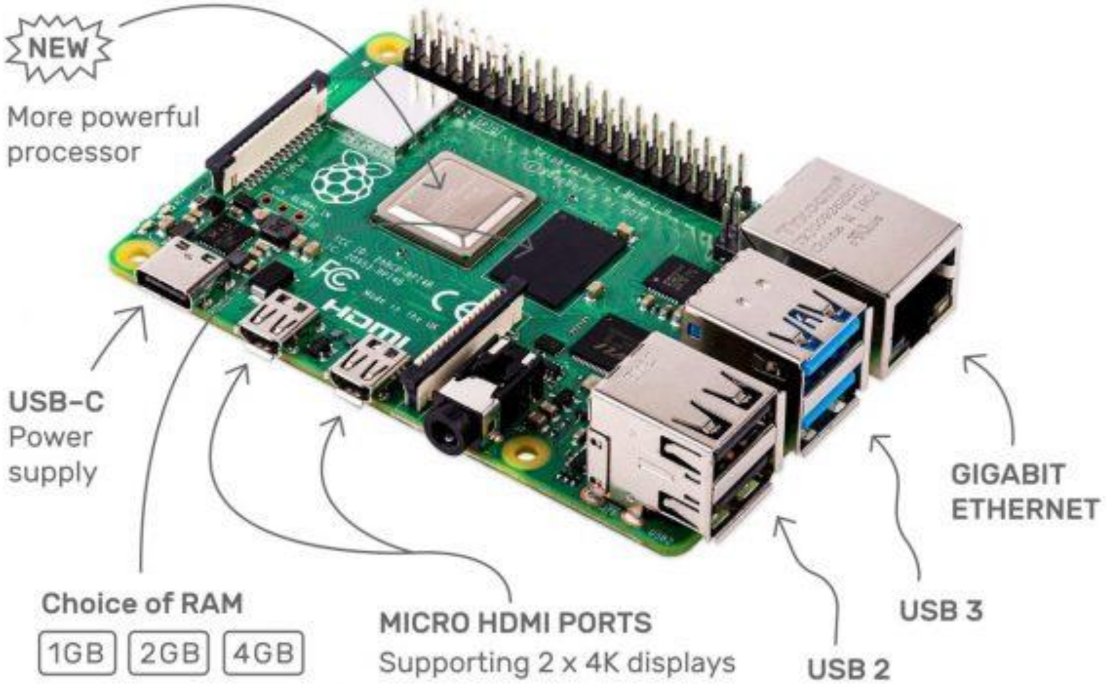
Cybersecurity Hardware Tools:

Cybersecurity consists of various types of pentesting, like website pentesting, mobile app pentesting, wireless pentesting etc. The tools in question are mainly pieces of hardware designed for security research or projects. Make sure, the use of these devices is not banned in your country.

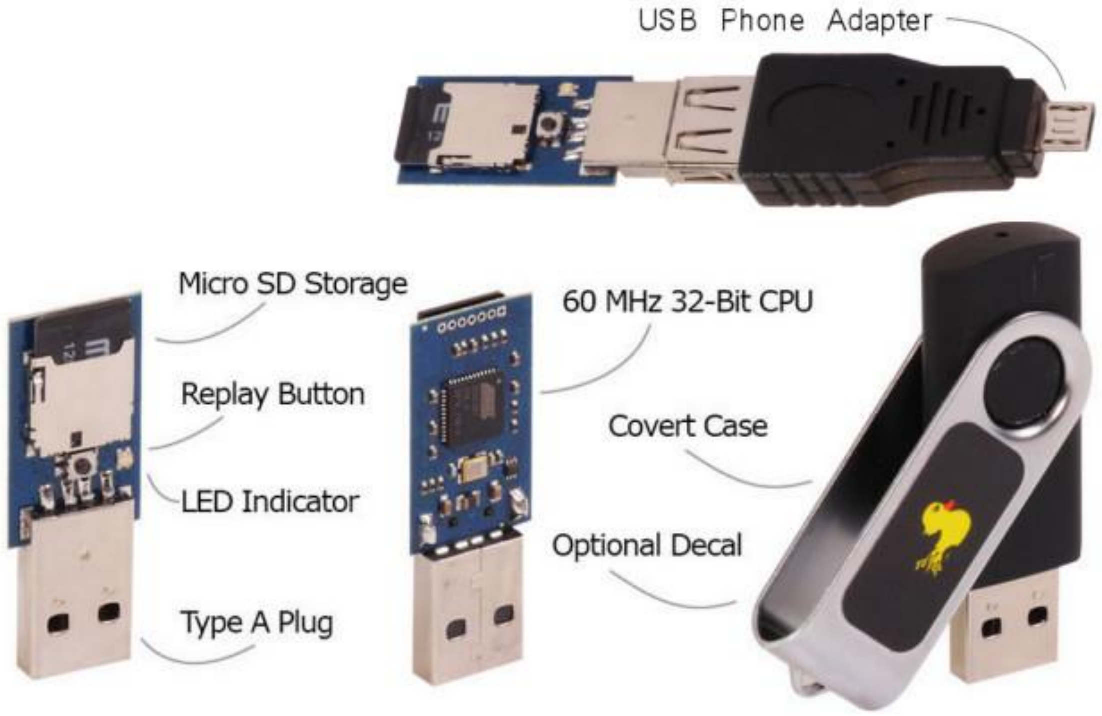
Raspberry Pi:

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. We are now on the third generation of these low-budget computers, which can be used in multiple ways. A classic example in security audits is to use a Raspberry Pi with its appropriate battery pack, a distribution platform like Kali Linux, and applications like FruityWifi, which together act like the Swiss army knife of pen testing. Raspberry Pi is not particularly made for hacking purposes but you can install Kali Linux on it and turn it into a portable Wi-Fi hacking device.



The USB Rubber Ducky:

The USB Rubber Ducky is Hak5's USB keystroke injection tool capable of executing payloads at over 1,000 words per minute. It can be used to hack a macOS device in less than 5 seconds, disable antivirus software, or social engineer someone into plugging it into their computer. USB Rubber ducky is an HID device that looks similar to a USB Pen drive. It may be used to inject keystroke into a system, used to hack a system, steal victims essential and credential data can inject payload to the victim's computers. Theoretically, this tool is for penetration testing. Security experts can use rubber duckies to test the resiliency of their computers systems. But hackers can also use the rubber ducky for keystroke injection attacks, and there are all kinds of tips and instructions online to help them.



Alfa Wireless USB Adaptor:

A USB wireless adapter is a device that we connect to our computer via a USB port and allows us to communicate with other devices via Wi-Fi, allowing us to connect to wireless networks and talk with other computers that use Wi-Fi. We need specific USB Wi-Fi adapters to play with wireless networks or Wi-Fi. Which include features like monitor mode and packet injection, which will aid in Wi-Fi penetration testing. It is plug-and-play compatible, so connect it to Kali Linux PC and begin experimenting with Wi-Fi security. It supports monitor mode and packet injection on Kali Linux and Parrot Security on.

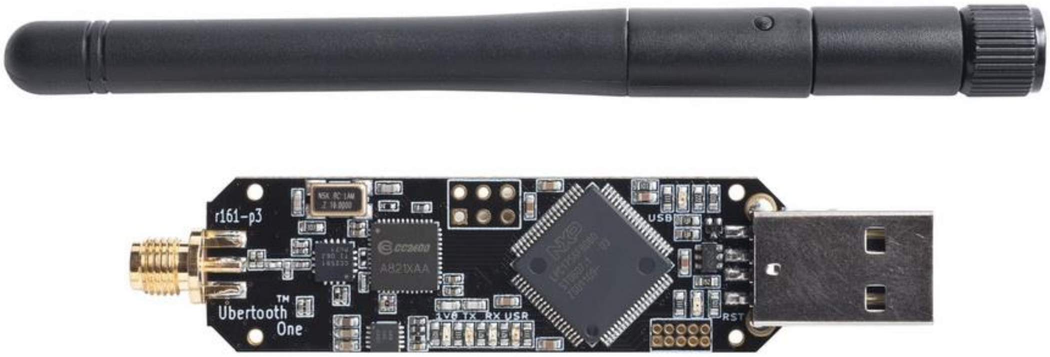
HackRF One:

HackRF One is an open-source hardware platform from Great Scott Gadgets. This software-defined radio is designed to test, develop and modify contemporary RF (Radio Frequency) systems. The unit is capable of transmitting and receiving radio signals from 1 MHz to 6 GHz. It works as a USB peripheral and can be even programmed as a stand-alone device.

The HackRF One can interact with a broad range of wireless systems which includes: Broadcasting Stations. Wi-Fi, Bluetooth, Smartphones and GPS. If you plan to pentest Radio Frequencies, then this is a must-have tool in your wireless hacking hardware toolkit.

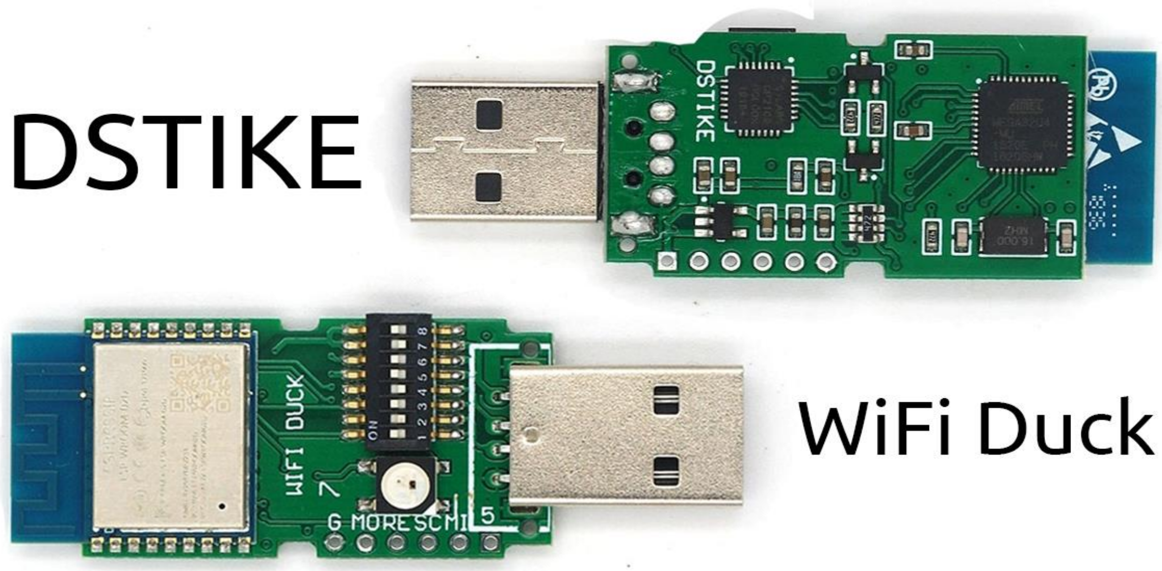
Ubertooth One:

The Ubertooth One is an open-source Bluetooth pentest tool. It is bundled with an ARM Cortex M3 microcontroller and an antenna. It has an operating frequency of 2.4 GHz. You can plug this tool into a computer using the USB and use it with various wireless monitoring tools like Kismet. The best part of Ubertooth One is both the software and hardware of this device is open-source, therefore you can even build one yourself.



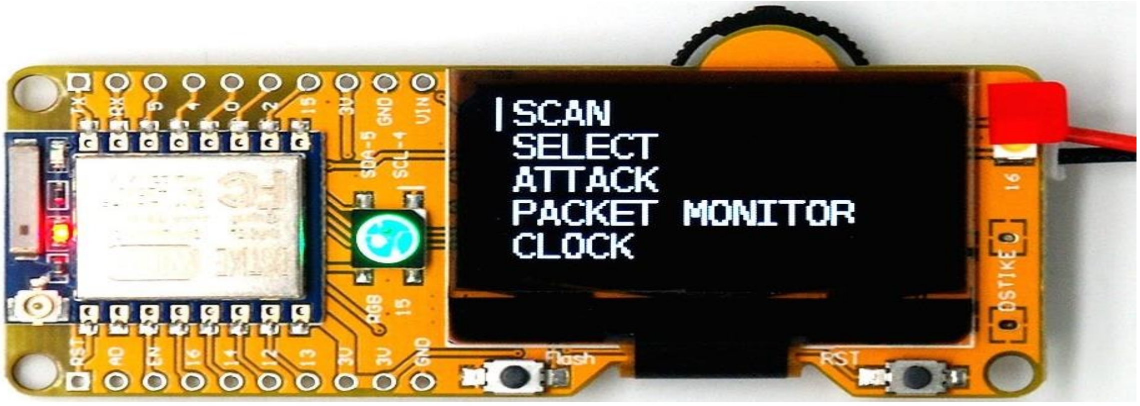
DSTIKE WIFI Duck:

This is where DSTIKE WIFI Duck comes into play. Wi-Fi Duck does the same thing as USB Rubber ducky but has Wi-Fi access and has a web interface. This means you can control it remotely over Wi-Fi from a distance. Now, an attacker can easily send payloads and commands over the Wi-Fi to the target machine as long as the Wi-Fi Duck is connected. An attacker can also use this device to inject backdoors into the target machine, so even if Wi-Fi Duck is disconnected the target machine will still be under the control of the attacker.



Wi-Fi Deauther:

De-authentication is necessary for hacking Wi-Fi networks. Once you de-authenticate a client from a wireless network, the client is forced to re-authenticate with the network. During re-authentication, an attacker can steal the WPA handshake and use it to brute-force the password for the network. Also, de-authentication is useful in “Evil Twin” attacks, where the attacker disconnects the client from the wireless network and force the client to authenticate to a “Rouge Access Point”. DSTIKE Wi-Fi Deauther Board is a small and cheap de-authentication tool that is bundled with an ESP8266 Deauther software. With this tiny development board, you can perform different attacks to test Wi-Fi networks.



RTL-SDR Device:

RTL-SDR (RealTek) is a low-cost USB device that can be used as a computer-based radio for receiving live radio signals. Depending on the RTL-SDR it could receive frequencies from 500 kHz up to 1.75 GHz. Most of the software for the RTL-SDR is also community developed, open-source and most of the time free of charge.

Other:

Wi-Fi Pineapple, Proxmark3, Crazyradio PA, Comidox Zigbee CC2531 Sniffer, USB Live Persistence Kali Linux Drive and more.