# Lab Rats: 6 Essential Tools For Your RF Hacking Lab

[](https://medium.com/@investigator515?source=post_page---byline--0165e377636d---------------------------------------)

[Investigator515](https://medium.com/@investigator515?source=post_page---byline--0165e377636d---------------------------------------)

Follow

7 min read

·

May 8, 2025

Listen

Share

More

To experiment with RF, you’ll need a proper workspace and some suitable tools.

**We strive to provide informative articles, however, it is important for users to ensure their research is both ethical and responsible. Additionally, it is your responsibility to ensure you’re compliant with all applicable laws and regulations for your region. The information provided in this article is intended for educational purposes only.**

When you’re learning about RF-based systems, you’ll typically find that while there are plenty of signals to receive, carrying out true experimentation requires you to be able to transmit as well.

Given the nature of some of this research, you’ll often find that staying legal requires that you carry out these experiments in an environment with controlled conditions so that your research isn’t interfering with real-world assets.

To optimise your lab, you’ll need to acquire some tools to help you get the most out of your resources. While it can be pretty tempting to just throw money at things, for many, budget is still the primary restrictor. But smart shopping and selective purchasing mean that you can still acquire your test gear over time without blowing the budget.

Here are a few of our favourite things to help get your RF test lab off to a flying start.

## HackRF One

A fully featured software-defined radio unit that comes with a wide range of accessories, the HackRF One is an essential piece of equipment for your lab. While it comes with a significant price penalty in comparison to something like an RTL-SDR, it’s a transmit-capable wideband transceiver.

Press enter or click to view image in full size



While the power levels aren’t ridiculously high, the transmit functionality does allow you to explore how various protocols can be spoofed or replicated. It’s also user-friendly and has good community support with plenty of ways to modify the standard board.

Look for the portapack running Mayhem firmware to get a mobile capable device that comes with broad utility.

*Pro Tip: If you’re a builder, it will be cheaper for you to buy the kit to self assemble.*

## Nano VNA

Before the explosion of cheap electronics, antenna analysers were often commercially designed devices that came with a hefty price penalty. Now, thanks to tools like the nanoVNA, we can add a broad range of analysis equipment to our test lab without blowing the budget on a single piece of equipment.



Helping you test and identify the electrical profile of RF-based systems, the nanoVNA's diminutive size hides its utility in a lab environment. Use it to identify faults, optimise antennas and ascertain loss and matching in things like patch cables and connectors.

*Pro Tip: Savvy shoppers can find them at online retailers for ridiculously cheap prices, so it’s worth shopping around.*

## Antenna Arrays

If you’re just getting started and you purchase something like an RTL-SDR you might be slightly underwhelmed at the start. While this might be dependent on your environment (cities have higher levels of RF activity over regional areas), one thing that will also influence this is the type of antenna system you decide to use.

We’ve covered this in previous articles before, as antenna theory covers a whole lot of interesting information that focuses on design. If you’re a newbie, though, you’ll probably find purchasing an off-the-shelf system to be the best return on your dollar, performance-wise.



Handheld antennas are great for portability, but if you’re looking to optimise the reception of High Frequency (HF) transmissions or track ADS-B signals out to the horizon, you’ll find an external antenna to provide much better performance.

If you’re the building type, easy formulas can be found online to help build almost any antenna you can think of.

*Pro Tip: Use 3d print templates to create insulators quickly and cheaply.*

## Raspberry Pi

It’s easy to be a believer in the Raspberry Pi and single-board computer systems. Responsible for helping to kick off the maker trend, the Pi has been endowed with ever-increasing performance specs. What was once a board with just 2 USB ports, no wi-fi and average performance specs, is now a powerhouse that, in some instances, is too much computer for some projects.



For circumstances like these, you might want to use the Pi Zero board, but there’s no denying the broad product range makes the Pi pretty attractive for makers.

From a lab perspective, the Pi brings a broad range of utility in a small package, just like the NanoVNA did. We can use it to run an instance of Kali Linux or DragonOS to help capture or analyse signals. We can take it portable to detect Wi-Fi or Bluetooth signals, or we can use the I2C bus and GPIO pins to modulate radio signals of our own choosing. Get one. Then get experimenting.

*Pro Tip: While the Pi can emit via the GPIO, it’s a pretty dirty signal despite the low power levels. Use filters to clean this up and stay legal*

## Jumper Wires

Some tools are more glamorous than others, and it’s fair to say that the good old jumper wires are most definitely part of the unglamorous list. However, these are more of an essential lab part than you might realise.

Not only will they help us to download data from an assortment of devices, but they’ll also help us to interface devices together temporarily. It’s a good idea to have a mixture of MM/MF/FF cables to ensure you can make a connection when you need to.

Don’t forget that we can also use jumper wires to download firmware or even flash new firmware in certain instances, as well as interface I2C or SPI buses.



Often, RF hacking is not dissimilar to hardware hacking, so ensuring we have a wide range of lengths and connector types gives us the most utility in our lab.

*Pro Tip: Jumpers are one of the easiest things to start building in your home-lab and can be built using recycled components.*

## Multi Meter

Saving the best till last, means the good old multimeter is the final bit of essential kit your test lab should acquire. While the nanoVNA is great for exploring RF-based systems, the multimeter will help you test electrical systems in general. This means you can analyse voltage and current, determine resistance or loss, and troubleshoot problems in various electrical systems.



If you’re looking to do hands-on learning, you’ll find that the multimeter has plenty to teach you. Not only can you test components like resistors, you can also use them to do continuity checks on things like patch cables to ensure they are electrically sound.

*Pro Tip: Order some coax and connectors and get hands on by building your own patch cables. This will teach you about connector types as well as resistance and continuity.*

## Remember

If you’re a beginner, it’s easy to find some things intimidating when you’re trying to learn. Something like a spectrum analyser can be a great learning tool, but it’s fair to say that both the price and learning curve can be daunting.

However, it’s worth looking at the market to get a feel for where things are at, as in the good old days, things like analysers could cost tens of thousands of dollars while being easily damaged if used incorrectly.

Now, we can get a NanoVNA for well under a hundred dollars, meaning that if our hardware fails or breaks, it’s easily replaceable. It also means that even at a beginner level, we can have accurate equipment that teaches us fundamental concepts at a hands-on level.

Remember though, while these are all “nice to haves”, learning is what you make of it. If your budget won’t stretch to analysis tools, you can always use things like the WebSDR project to explore the spectrum cost-free.

Medium has recently made some algorithm changes to improve the discoverability of articles like this one. These changes are designed to ensure that high-quality content reaches a wider audience, and your engagement plays a crucial role in making that happen.

If you found this article insightful, informative, or entertaining, we kindly encourage you to show your support. Clapping for this article not only lets the author know that their work is appreciated but also helps boost its visibility to others who might benefit from it.

**🟦**We’re now on **[Bluesky](https://investigator515.bsky.social/" \t "_blank)!**

🔗 Articles we think you’ll like:

1. What The Tech?! [**Space Shuttles**](https://medium.com/@investigator515/what-the-tech-space-shuttles-40aecde848ed)
2. Shodan: [**A Map of the Internet**](https://medium.com/the-first-digit/shodan-a-map-of-the-internet-fbf0ad8089f9)

✉️ Want more content like this? [**Sign up for email updates**](http://investigator515.substack.com/)

[Hacking](https://medium.com/tag/hacking?source=post_page-----0165e377636d---------------------------------------)

[Radio](https://medium.com/tag/radio?source=post_page-----0165e377636d---------------------------------------)

[Homelab](https://medium.com/tag/homelab?source=post_page-----0165e377636d---------------------------------------)