# Software Defined Radio & Radio Hacking. Part 1

[](https://medium.com/@investigator515?source=post_page---byline--a9b5a0608d9e---------------------------------------)

[Investigator515](https://medium.com/@investigator515?source=post_page---byline--a9b5a0608d9e---------------------------------------)

Follow

10 min read

·

Aug 28, 2023

Listen

Share

More

**Understanding SDR is essential for mastering cyber security disciplines.**

**Note: The legalities behind the radio spectrum vary from country to country. While generally speaking receiving is okay, in some places this may be still prohibited so you should check your local laws before starting. Transmission of signals outside the licence free ISM band requires a license, again please check your locality for situation specific details. Direction finding can be done in seconds with the correct setup… so play nicely.**

If you were around in the early days of the internet you might recall it was a much simpler time.

We had simpler web pages, less security and the proliferation of social media and smart devices hadn’t occurred yet, meaning the art of cyber security was much easier to master. This doesn’t mean the early internet didn’t have good things. Some classic pieces of software like Snort were designed literally decades ago yet remain entirely relevant even today.

However over time as the world and how we communicate changed, we see more importance given to specialized roles that are essential in understanding just how technology works, and more importantly how it can be exploited. Then subsequent to that, how something can be protected.

As the internet slowly changed and we saw the growth of IOT devices, how these devices connect and engage with the world also changed. In the private world, we saw cloud based assets grow, and private CCTV networks explode into everyday usage

In the commercial world we saw the development of things like aircraft ADS-B and marine AIS systems bring information to the masses, allowing anyone with a Web connection and a browser to browse traffic globally in an instant. We also saw the development of things like smart electricity meters and point to point links for information sharing, allowing the growth of integrated RF systems to replace the role of many manual jobs.

Because of these changes in our world, we see that some skill sets grow and evolve right along side our technology. Everyday we see solar installers using RF systems to monitor power generation, and garage door installers using RF triggers to open garages at the push of a button. Starlink and Iridium signals fly overhead, transmitting conversations, internet and telemetry the whole way. All of these can be explored with some SDR knowledge.

When we look at all of this in context and try to understand how we analyse the world around us, we start to realize that we need to cultivate certain skill sets to effectively engage with these new forms of technology. Without a doubt one of these essential skills to master, is Software Defined Radio.

In Part 1 of today’s article, we’ll be looking further into SDR and radio hacking, attempting to understand exactly what it is and why exactly we consider this an essential skill for the cyber security professional. Let’s get started.

**What Is It:**

We’ve actually covered simple software defined radio before, in **this article,**as well as discussing the different types of emissions as well in this [**earlier piece too**](https://www.bulbapp.io/p/a7691488-8e3f-4faa-bd39-fc50b0ecf182/electronic-fingerprinting-mobiles-devices-behind-the-shadows)**.**However these were more generalized, and today we’ll be digging deeper into some of the specifics.

In the interests of providing more clarity, we can say that Software Defined Radio (SDR) is a technology that allows you to use software to control and manipulate radio signals, instead of using traditional hardware components. It provides flexibility and versatility in terms of signal processing and modulation techniques.

In a nutshell, this effectively means that rather than needing a radio to intercept and analyse radio transmissions, we can now use our computer. But more importantly, rather than simply using and relying on voice transmissions, we can now use digital signals and modes linked to our computer.

We can also record, analyse and play back or re transmit signals near instantly, whilst also keeping an eye on the spectrum at the same time.

This is a lot to take in for beginners, so let’s pause here and ask Chat GPT for a quick summary of some of the benefits of SDR compared to analogue radio.

**Input:**Please explain some of the benefits of SDR over traditional radio

**Output:**Sure! Some benefits of Software Defined Radio (SDR) over traditional radios are:

1. Flexibility: SDR allows for easy reconfiguration and adaptation to different communication standards and protocols.

2. Cost-Effectiveness: SDR reduces the need for specialized hardware components, making it more cost-effective to implement and upgrade radio systems.

3. Upgradability: SDR systems can be updated with new features and functionalities through software updates, extending their lifespan and keeping them up-to-date.

4. Spectrum Efficiency: SDR enables efficient utilization of the available spectrum by adapting to changing conditions and optimizing signal processing techniques.

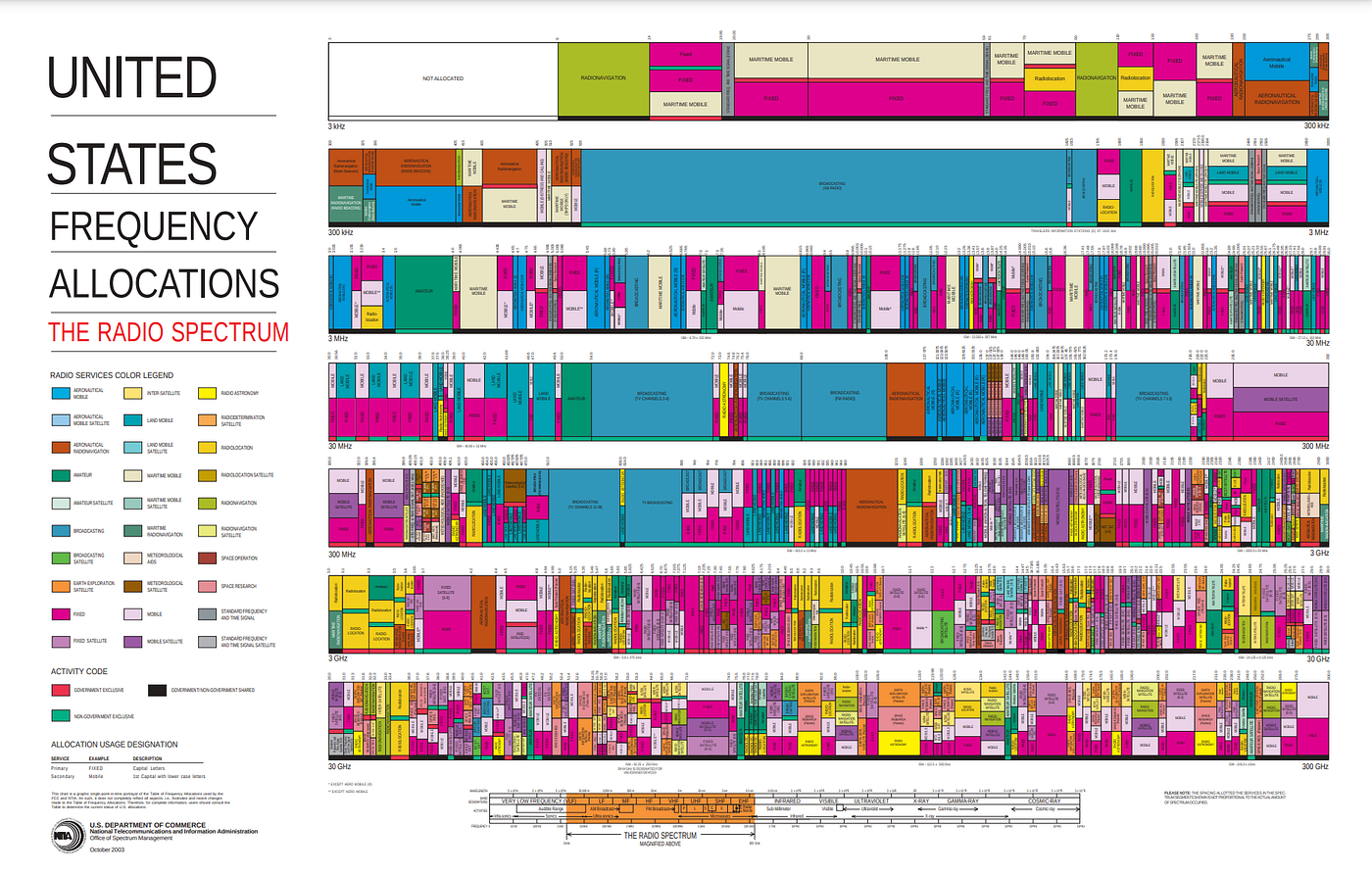
5. Interoperability: SDR can support multiple communication standards, making it easier for different systems to communicate with each other.

6. Development and Experimentation: SDR provides a platform for researchers and developers to experiment with new radio technologies and algorithms.

Overall, SDR offers increased flexibility, cost savings, and the ability toadapt to evolving communication needs.

Okay, so this seems pretty clear cut. Let’s look at how we can get started learning about SDR in a cyber security capacity.

Press enter or click to view image in full size



The Radio spectrum, from DC to Daylight. It’s a vast playground for those willing to learn to ropes. Source: FCC

**Where to Begin:**

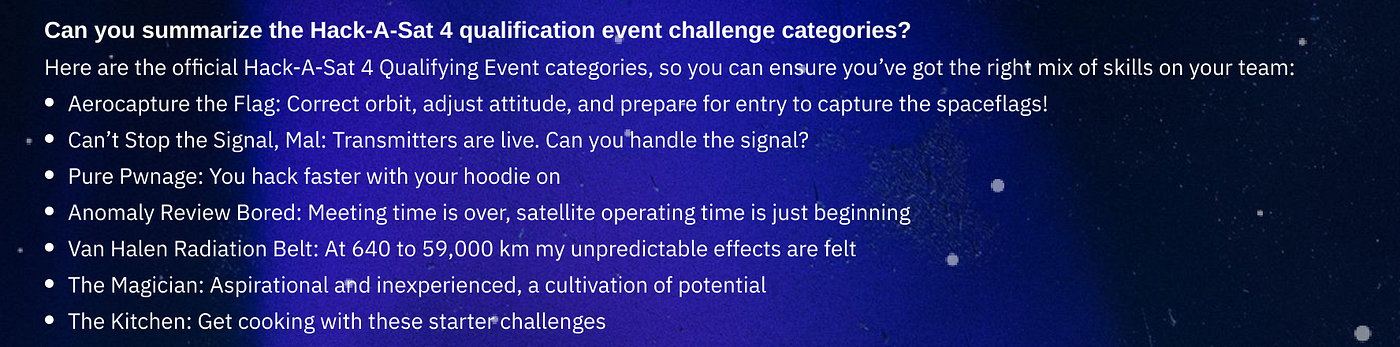
Before we begin, it’s important to understand your own limitations and learning path here.  
Do you wish to have a cursory understanding or something deeper? Do you have a hardware budget, or are there financial limitations that restrict you from from obtaining what you need?

While none of these will make your journey impossible, like anything clearly setting and understanding both goals and limitations will allow a clear learning path whilst creating a good environment for said learning.

It’s also important to understand before we start that when you pair SDR and then the concept of hacking, we start to see how vast the world is around us while taking a distinct step away from networks and traditional forms of hacking. While it’s still present and does overlap into our article today, the point is that mastering SDR gives you far more options in the tool kit and because of this, we move into some rather exciting and specific applications.

Want to hack a satellite?? You’ll need SDR experience to master uplinks and down links, as well as dealing with Doppler effect and intercepting telemetry from beacons in space. This is no joke, check out our screen cap from the latest [**Hack-A-Sat**](https://hackasat.com/)contest in the United States showing different event types.

Press enter or click to view image in full size



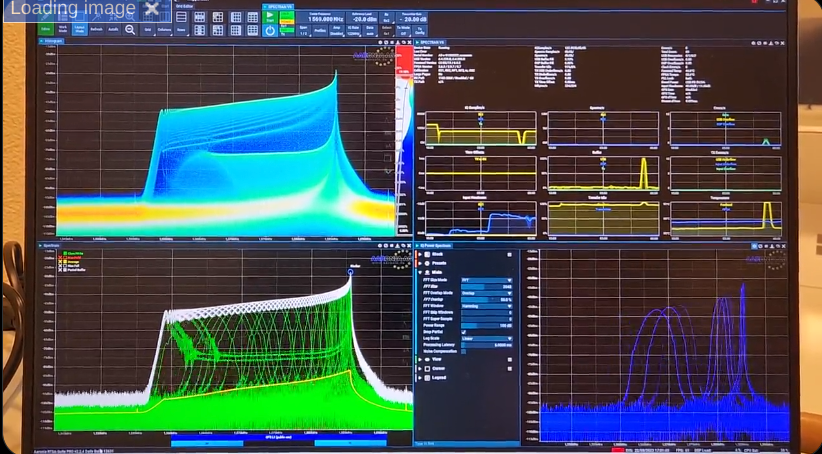
Hack a Sat 4. The dream for space enthusiast’s. Source: Hack-aSat.com

Want to fly Kismet on a drone? You’ll still use Wi-Fi for some parts of this, but you’ll need radio frequency spectrum experience to deal with channels, spacing, antennas and optimizing your setup.

Perhaps your interest is Geolocation of transmissions and devices? Understanding where to look for different transmissions and how to optimally Geolocate signals means you’ll obtain experience with more antennas, feed lines and software that can be used to assist you in your quest.

As you can see, the addition of SDR to our toolkit gives us a vast array of choices beyond traditional networking and computers. And this is before we look at things like Bluetooth devices, wireless camera and ISM band devices and beyond that, spectrum specific functions like location spoofing and other offensive applications. So if you like to push the limits of learning, there’s plenty of specialties for you to focus on should you choose.

Press enter or click to view image in full size



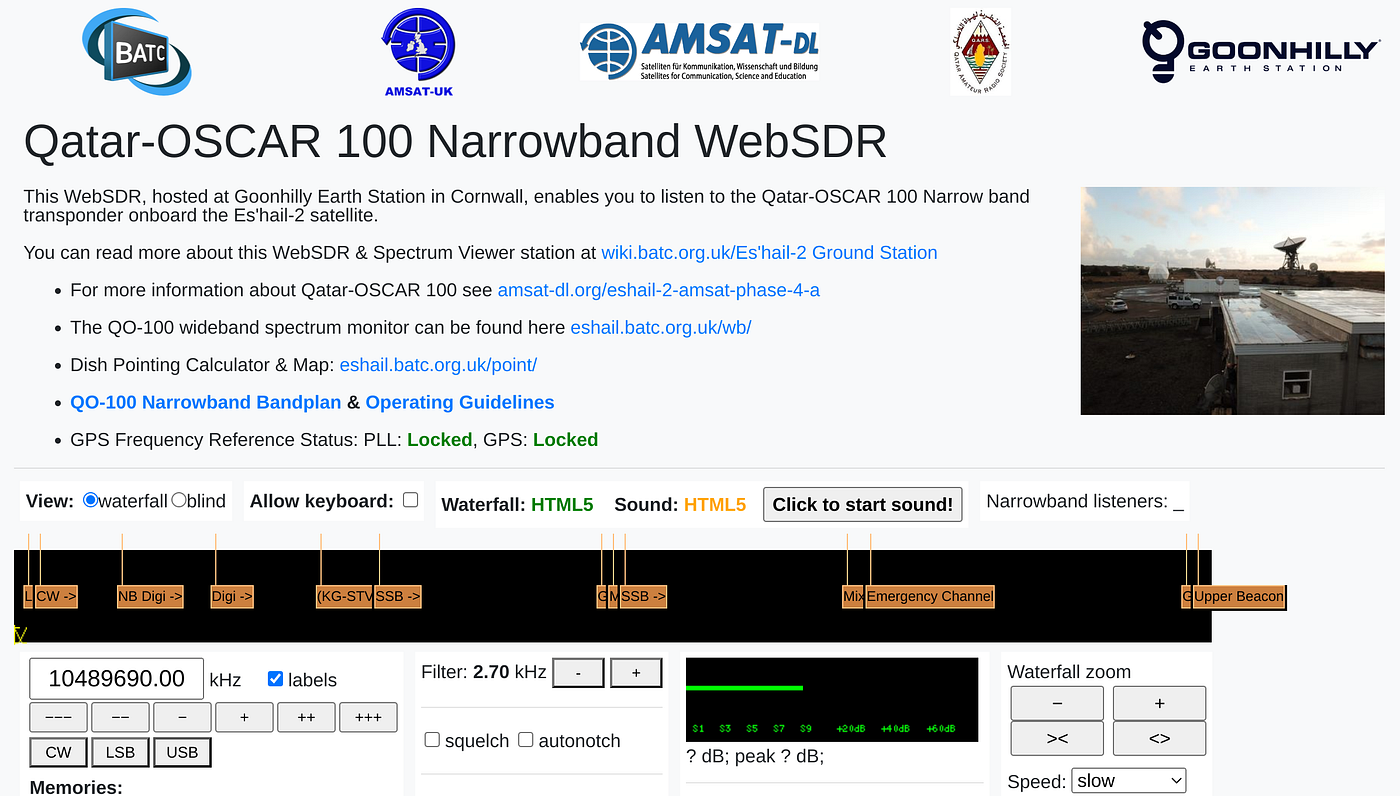
A visual look at Broadband GPS Jamming conducted in a lab environment. Source: twitter.com

Now we’ve broken that down, it’s time to see how we start our journey. Lets look at some non hardware options first as that’s the simplest way to get started.

**Online Tools: Web SDR**

Proliferating thanks to Ham Radio operators the world over, Web SDR relies on web portals streaming online to provide an open access system that basically anyone can use. While you’ll find traditional Web SDR portals have good hardware, you’ll typically find they tend to focus on amateur radio bands. While some of this can be considered to be menial “chit chat”, the amateur bands also included dedicated space communications bandwidth. This allows for the interception and transmission of both voice and data modes by anyone with an appropriate license and equipment.

Press enter or click to view image in full size



Web SDR Dashboard for the Qatari Es’hail-2 Satellite. Source: WebSDR.org

While the Ham Bands do come with limitations, they can be a great way to get started with SDR, with users able to learn how to tune frequencies, record transmissions, adjust bandwidth, IF and other essential SDR skills.

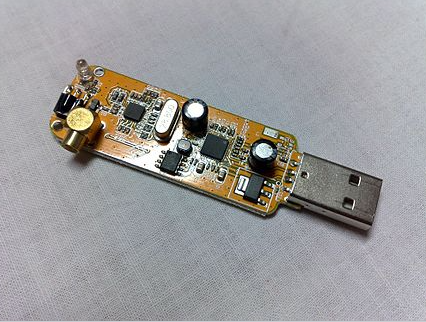
If we’ve got your attention, then you should check out [**websdr.org**](http://www.websdr.org/) to get started with the non hardware approach.

**Hardware Methods:**

When looking at our Hardware approach we see a two different options available to us. We have receive only and receive / transmit capable devices.

Receive only devices come in a number of variants, with probably the RTL-SDR being the cheapest and most prolific of these devices. Based on a modified TV tuner, these devices unlocked software defined radio to the masses due to the fact they are able to be procured extremely cheaply.

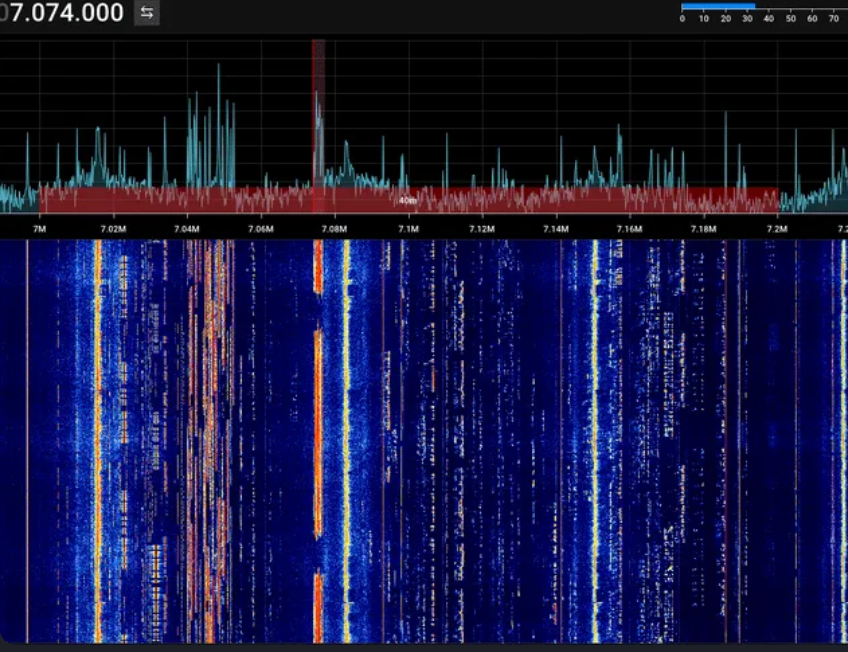
The other benefit of RTL devices is the proliferation of free, open source software to power it. This means that many digital modes are able to be decoded with a simple software patch, allowing many signals that are outside the scope of an analogue radio become trivial to intercept.



RTL-SDR powered by the R2832U Chipset. Source: Wikipedia.

The down side of these devices is that due to their cheap nature and typically plastic housing, they can be finicky, subject to interference and signal drift. While they are still a useful tool, they can be frustrating for beginners and any serious professional should be considering devices that come with a metal housing, and a crystal oscillator to provide legitimate frequency stability.

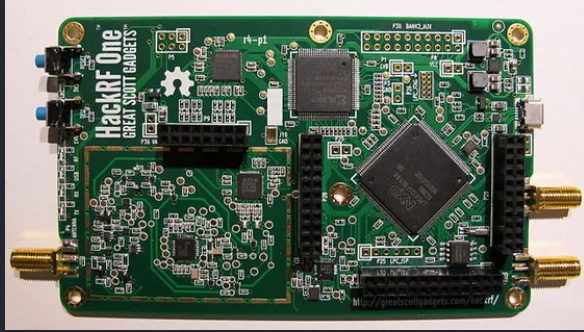
Press enter or click to view image in full size



One of the biggest SDR benefits is seeing large chunks of spectrum along with multiple signals. This is the HF amateur band showing many different types of signals. Source: RTL-SDR.com

The next step up from these devices are systems like the HackRF or Blade RF. Fully transmit and receive capable across a wide range of the spectrum these are the types of devices our radio hacker will find useful, providing both interception and re transmission capability in a rugged housing with plenty of bandwidth as well as the much needed frequency stability that many of the cheaper RTL devices lack.

Press enter or click to view image in full size

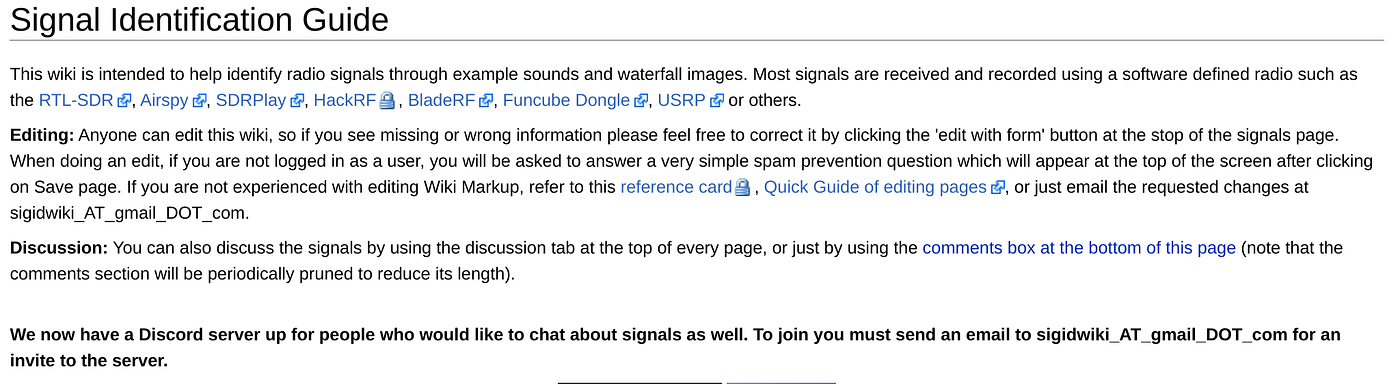


Hack RF one. A half duplex, transmit capable SDR. All will be explained by part 2. Source: Wikipedia.

While we’ll leave the utility of this device for part two of this series what we can say about these types of SDR units is that they are capable of re transmitting many different types of signals, including many well known open source types. This might include Video, Loran or a Spoofed GPS Signal. There’s also propitiatory signals like digital radio, car and garage remotes and much more.

If you’d like a look at some of the signals you might see while conducting this type of research, you should check out the [**SigID**](https://www.sigidwiki.com/wiki/Signal_Identification_Guide)wiki for both visual and audio captures of common transmission types.

Press enter or click to view image in full size

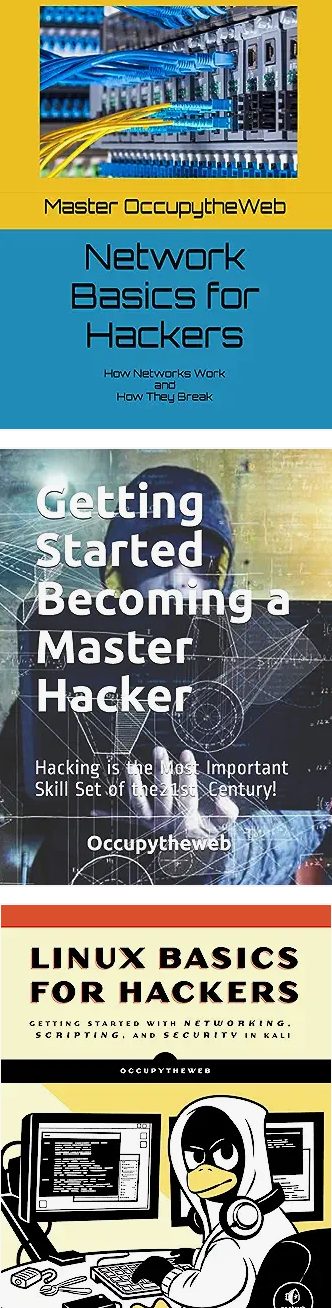


**More Resources**

So at this point in our article, you now know where to source Signal Information as well as what type of hardware to select to get your journey started. You also know where to get started with online SDR right now. In Part 2 of this article, we’ll break out our shiny new SDR and use it for some Signals Intelligence, focusing on direction finding and intercepting some basic space communications. We’ll also show you how to build some simple antennas for your new system and discuss the importance of antennas in making this whole thing work. Antenna Theory is probably worth it’s own specific article!

However if you’d like to supercharge your learning journey in between reads, we’d love to provide you with some extra reading and video resources to send you along your way.

OccupyTheWeb has a full course on SDR for Hackers that’s a brilliant learning resource for those interested in taking their learning to the next level. Check it, along with many other free resources at his website [**Hackers-Arise**](https://www.hackers-arise.com/sdr-for-hackers)



OTW should be a famiiar shadow in cybersecurity. Source: Amazon.com

[**David Bombal**](https://www.youtube.com/@davidbombal) has interviewed OccupyTheWeb, as well as providing many useful video based, SDR resources on his YouTube channel. Check it out here.

Press enter or click to view image in full size



David’s YouTube is a goldmine of useful information. Source: YouTube.com

The RTL-SDR website has a blog, new and a vast array of SDR based articles based on many different disciplines. Find them [**here**](http://rtl-sdr.com/)**.**

And of course we’ll continue releasing our own tutorials, which you can receive by following our socials and subscribing for email updates on your platform of choice. See all our relevant details below.

🌟 Enjoyed this article? Support our work and join the community! 🌟

💙 Support me on Ko-fi: [**Investigator515**](http://ko-fi.com/investigator515)

📢 Join our [**Telegram**](http://t.me/investigator515) channel for exclusive updates or.

🐦 Follow us on [**Twitter**](http://twitter.com/inv515)

🔗 Articles we think you’ll like:

1. OSINT Unleashed: 5 Essential Tools for Cyber [**Investigators**](https://medium.com/age-of-awareness/osint-unleashed-the-5-best-tools-for-cyber-investigators-8ff08fe9a4ba)
2. What the Tech?! GPS [**Technology**](https://medium.com/@investigator515/unleashing-the-hunters-a-journey-through-the-history-of-wild-weasels-35f72a98534d)

✉️ Want more content like this? Sign up for email updates [**here**](https://medium.com/subscribe/@investigator515)

[Sdr](https://medium.com/tag/sdr?source=post_page-----a9b5a0608d9e---------------------------------------)

[Radio](https://medium.com/tag/radio?source=post_page-----a9b5a0608d9e---------------------------------------)

[Technology](https://medium.com/tag/technology?source=post_page-----a9b5a0608d9e---------------------------------------)