RF Frequency Analysis Hardware Kit

CONTENTS

RF Frequency Analysis Hardware Kit - Medium Grade

Executive Summary

This document outlines a comprehensive roadmap for building a medium-grade radio frequency (RF) analysis hardware kit using off-the-shelf components. The kit is designed for users transitioning from beginner to intermediate level, providing professional-grade capabilities at reasonable cost.

Hardware Tier Comparison

Tier 1: Entry Level (Beginner)

Device	Frequency Range	Bandwidth	Sample Rate	Price	Best For
RTL-SDR Blog V3	24-1766 MHz	2.4 MHz	2.4 MSPS	$35	Learning, FM radio, ADS-B
RTL-SDR Blog V4	500 kHz-1.7 GHz	2.4 MHz	2.4 MSPS	$45	Improved HF, all V3 features
Nooelec NESDR SMArTee	24-1766 MHz	2.4 MHz	2.4 MSPS	$40	Low noise, bias-tee built-in

Pros: Very affordable, great learning tool, wide software support **Cons:** RX only, limited bandwidth, no TX capability

Tier 2: Medium Grade (Intermediate) - RECOMMENDED

Device	Frequency Range	Bandwidth	Sample Rate	TX Power	Price
HackRF One	1-6000 MHz	20 MHz	20 MSPS	0-15 dBm	$300
LimeSDR	100 kHz-3.8 GHz	61.44 MHz	61.44 MSPS	Up to 10 dBm	$300
LimeSDR Mini	10 MHz-3.5 GHz	30.72 MHz	30.72 MSPS	Up to 10 dBm	$150
BladeRF x40	300 MHz-3.8 GHz	28 MHz	40 MSPS	Up to 6 dBm	$400

Pros: Full duplex (TX+RX), wider bandwidth, more capable **Cons:** Higher cost, steeper learning curve

Tier 3: Professional Grade (Advanced)

Device	Frequency Range	Bandwidth	Sample Rate	Price
Ettus USRP B210	70 MHz-6 GHz	56 MHz	61.44 MSPS	$1,100
BladeRF 2.0 micro	47 MHz-6 GHz	56 MHz	61 MSPS	$540
PlutoSDR	70 MHz-6 GHz	56 MHz	61 MSPS	$230

Recommended Kit Configuration

Core SDR Hardware

Primary Device: HackRF One ($300)

Specification	Value
Frequency Range	1 MHz - 6 GHz
Operating Modes	Half-duplex (TX or RX)
RF Bandwidth	Up to 20 MHz
Sample Rate	20 MSPS (8-bit I/Q)
TX Power	0 to +15 dBm typical
RX Sensitivity	-80 dBm typical
Interface	USB 2.0
Antenna Connector	SMA female
Power	USB bus-powered

Why HackRF One: - Widest frequency range (1 MHz - 6 GHz) - Transmit AND receive capability - Massive community support - Open source hardware - Excellent documentation and tutorials

Supporting Equipment

Antennas ($100-150)

Antenna	Frequency	Use Case	Price
Dipole antenna kit	70-1000 MHz	General purpose	Included
Telescopic whip	VHF/UHF	Portable scanning	$20
Discone antenna	25-1300 MHz	Wideband RX	$80
Log Periodic	400-1000 MHz	Directional	$60

Cables and Adapters ($50)

Item	Quantity	Price
SMA male to SMA male cable	2	$15
SMA male to BNC adapter	2	$10
SMA male to N adapter	1	$8
SMA attenuator set (3, 6, 10, 20 dB)	1 set	$20

Accessories ($80-150)

Item	Purpose	Price
USB 3.0 powered hub	Stable power, reduced interference	$25
Aluminum case	Protection, EMI shielding	$30
LNA (Low Noise Amplifier)	Weak signal reception	$40
Bias-tee power injector	Power remote LNAs	$25
TCXO oscillator upgrade	Improved frequency stability	$30

Computing Platform ($200-500)

Option	Specs	Price
Laptop (recommended)	i5+, 8GB RAM, USB 3.0	$300-500
Raspberry Pi 4	4GB+ RAM, USB 3.0	$55
Desktop PC	PCIe slot for future upgrades	$400+

Phased Implementation Plan

Phase 1: Foundation (Weeks 1-4) - $100

Equipment: - RTL-SDR Blog V4 dongle ($45) - Basic dipole antenna kit ($25) - USB cable, SMA adapters ($30)

Skills Developed: - Software installation (SDR#, GQRX, SDR-Radio) - Frequency scanning and waterfall interpretation - Signal identification (FM, AM, digital modes) - Basic spectrum analysis - Recording and playback

Deliverables: - Working SDR setup - Frequency database for local signals - First signal recordings

Phase 2: Enhancement (Weeks 5-8) - $400

Equipment: - HackRF One ($300) - Discone antenna ($80) - USB 3.0 hub ($25)

Skills Developed: - Transmitting signals - Digital signal processing - GNU Radio basics - Signal modulation analysis - Protocol reverse engineering basics

Deliverables: - First TX transmissions (legal bands) - Custom GNU Radio flowgraphs - Signal classification capability

Phase 3: Analysis (Weeks 9-12) - $200

Equipment: - LNA with bias-tee ($60) - Better cables and adapters ($50) - Directional antenna ($60) - TCXO upgrade ($30)

Skills Developed: - Weak signal reception - Direction finding basics - Signal attribution - Frequency coordination - Regulatory compliance (FCC Part 97, Part 15)

Deliverables: - Enhanced signal database - Direction finding capability - Compliance documentation

Phase 4: Advanced (Weeks 13-16) - $300

Equipment: - Second SDR (diversity reception) ($45) - Shielded enclosure ($50) - GPSDO for timing ($200 optional)

Skills Developed: - Coherent reception - Time-aligned measurements - Advanced GNU Radio - Custom protocol implementation - Security testing basics

Deliverables: - Multi-SDR setup - Custom analysis tools - Research documentation

---

Software Stack

Core Analysis Software

Software	Platform	Purpose	License
GQRX	Linux/Mac	General receiver	GPL
SDR++	Windows/Linux/Mac	Wideband receiver	GPL
SDR-Angel	Windows/Linux	Multi-mode receiver	GPL
CubicSDR	Cross-platform	Visual spectrum	BSD
GNU Radio	Cross-platform	DSP framework	GPL

Specialized Tools

Software	Purpose
URH (Universal Radio Hacker)	Protocol analysis
SigDigger	Signal analysis
** baudline**	Spectral analysis
Fosphor	GPU-accelerated waterfall
QSpectrumAnalyzer	Python spectrum analyzer

Digital Mode Decoders

Software	Modes Decoded
MultiPSK	PSK31, RTTY, Packet, etc.
Fldigi	CW, PSK, RTTY, MFSK
DSD+	Digital voice (DMR, P25, D-STAR)
AIS Decoder	Maritime AIS
rtl_adsb	ADS-B aircraft tracking
ACARS Decoder	Aircraft messaging

Frequency Analysis Workflow

Signal Detection

```
1. Configure SDR software (gain, sample rate)
2. Set frequency range to scan
3. Monitor waterfall display for energy
4. Record signal characteristics:
   - Center frequency
   - Bandwidth
   - Signal strength (dBm)
   - Time of day
   - Duration
```

Signal Identification

```
1. Measure bandwidth
2. Identify modulation type:
   - AM (envelope varies)
   - FM (constant envelope)
   - Digital (discrete levels)
```

```
3. Check against known signal database
4. Use demodulator to decode content
5. Compare with reference recordings
```

Signal Recording

```
1. Set appropriate sample rate (2x signal BW minimum)
2. Record I/Q data (not just audio)
3. Include metadata:
   - Frequency
   - Time
   - Location
   - Equipment used
   - Gain settings
```

Budget Summary

Phase	Equipment	Cost
Phase 1	RTL-SDR kit	$100
Phase 2	HackRF One + antenna	$400
Phase 3	LNA, adapters, directional	$200
Phase 4	Second SDR, shielding	$300
Total		**$1,000**

Minimum Viable Kit ($450)

- RTL-SDR V4 ($45)
- HackRF One ($300)
- Basic antennas ($50)
- Cables and adapters ($55)

Optimal Medium-Grade Kit ($1,000)

All four phases combined with recommended accessories.

Learning Resources

Free Resources

Resource	URL	Focus
RTL-SDR.com	rtl-sdr.com	Beginner tutorials
Great Scott Gadgets	greatscottgadgets.com/sdr	Video series
GNU Radio Tutorials	tutorials.gnuradio.org	DSP fundamentals
Signal Identification Wiki	sigidwiki.com	Signal database
RadioReference	radioreference.com	Frequency database

Recommended Books

Book	Author	Price
“SDR for Engineers”	Analog Devices	Free PDF
“GNU Radio Cookbook”	Various	Free online
“Signals and Systems”	Oppenheim	$120

Online Courses

Course	Platform	Cost
Software Defined Radio	Michael Ossmann	Free
DSP for Radio	Coursera	$50
RF Engineering	edX	Free

Safety and Legal Considerations

Transmit Restrictions

Band	TX Allowed?	License Required
AM Broadcast	□ NO	N/A
FM Broadcast	□ NO	N/A
Amateur Radio	□ YES	Amateur license
ISM Bands (315/433/915 MHz)	□ YES	Part 15 compliant
Citizen’s Band	□ YES	None (Part 95)
FRS/GMRS	□ Partial	GMRS requires license

Best Practices

1. **Never transmit on restricted frequencies**
2. **Use attenuators when testing near transmitters**
3. **Obtain proper licenses before TX**
4. **Keep records of all transmissions**
5. **Respect privacy - don’t decode private communications**

Maintenance and Upgrades

Regular Maintenance

Task	Frequency
Check antenna connections	Monthly
Clean SMA connectors	Monthly
Update SDR software	Weekly
Calibrate frequency reference	Quarterly
Back up recordings	Weekly

Upgrade Path

Upgrade	Benefit	Cost
GPSDO	±0.01 ppm accuracy	$200
Shielded enclosure	Reduced noise	$50
Preselector filter	Better selectivity	$100
High-gain antenna	Weak signal RX	$150
Second SDR	Diversity/coherent	$300

Conclusion

A medium-grade RF analysis kit centered on the HackRF One provides excellent value for intermediate users. The phased approach allows gradual skill development while building capability. Total investment of $1,000 provides professional-grade analysis capability across 1 MHz to 6 GHz with both transmit and receive functionality.

Key recommendations: 1. Start with RTL-SDR for learning ($45-100) 2. Upgrade to HackRF One for TX capability ($300) 3. Add LNA and better antennas for weak signals ($100) 4. Expand to multi-SDR setups for advanced analysis ($300+)

This kit provides the foundation for: - RF spectrum analysis - Signal identification - Protocol reverse engineering - Security testing (authorized) - Amateur radio operation - Regulatory compliance verification

Appendix A: Vendor List

Vendor	Products	Website
RTL-SDR Blog	RTL-SDR V3/V4	rtl-sdr.com
Nooelec	NESDR series	nooelec.com
Great Scott Gadgets	HackRF	greatscottgadgets.com

Vendor	Products	Website
Lime Microsystems	LimeSDR	limemicro.com
Nuand	BladeRF	nuand.com
Ettus Research	USRP	ettus.com

Appendix B: Software Installation

Linux (Ubuntu/Debian)

```
# RTL-SDR
sudo apt install rtl-sdr gqrx-sdr

# HackRF
sudo apt install hackrf gqrx-sdr

# GNU Radio
sudo apt install gnuradio

# Additional tools
sudo apt install gr-gsm urh baudline
```

Windows

1. Download Zadig from zadig.akeo.ie
2. Install WinUSB driver for device
3. Download SDR++ from sdrplusplus.com
4. Download GNU Radio from gnuradio.org

macOS

```
# Homebrew
brew install gqrx
brew install gnuradio
brew install hackrf
```

Document Version: 1.0 Date: March 23, 2026 Author: STSGYM Research Division