

Training: Software Defined Radio

Dates of the training: March 12-13, 2018 in Heidelberg, Germany

Book Now using the voucher code: **TR18HMTSEB** and save an additional 5% of the current valid rate of any package!

Overview

The two-day Software Defined Radio (SDR) course is an introduction to digital signal processing, software radio, and the powerful tools that enable the growing array of SDR projects within the hacker community. This course takes a unique “software radio for hackers” approach, building on the participants’ knowledge of computer programming and introducing them to the forefront of digital radio technology. Participants will learn how to transmit, receive, and analyze radio signals and will be prepared to use this knowledge in the research of wireless communication security.

Course Content

INTRODUCTION TO SOFTWARE DEFINED RADIO

- Overview of SDR
- What people have done with software radio in the hacker community
- GNU Radio architecture and what it includes
- What you can do in GNU Radio Companion vs. python vs. C++
- Capabilities of HackRF and other SDR hardware platforms

Don't hesitate to call us. We are fluent in English and German.

TROOPERS
Need assistance?
+49 6022 508200

<https://www.troopers.de>
 +49 6221 480390
info@troopers.de

HM Training Solution www.hmtrainingsolutions.com
Need assistance? 

info@hmtrainingsolutions.com

EXERCISE: FINDING A SIGNAL

- Using HackRF and GNU Radio to locate and receive a radio signal
- Signal analysis with Baudline

COMPLEX VS. REAL SIGNALS

- How to think in the complex plane
- Why we use complex signals for software radio

EXERCISE: WORKING WITH COMPLEX SIGNALS (PART 1)

- A software challenge

EXERCISE: WORKING WITH COMPLEX SIGNALS (PART 2)

- Exploring real and complex signals in GNU Radio Companion

ALIASING AND SAMPLING THEORY

- Introduction to sampling and aliasing
- Negative frequencies: what they mean in real vs. complex signals
- Importance of anti-aliasing filters
- The Nyquist criterion

EXERCISE: TRANSMISSION AND SIMULATION

- Transmit a signal with HackRF
- Simulate both transmission and reception on a single computer

EXERCISE: DIGITAL FILTERS

- Explore different types of filters in GNU Radio Companion

BANDWIDTH

- The term “bandwidth” and what it means in the context of radio communications
- Familiarity with the bandwidth of different wireless technologies
- Uses of filters

Don't hesitate to call us. We are fluent in English and German.

- EXERCISE: REPLAY
- Attack an active RFID security device by capturing and replaying a signal

MODULATION

- amplitude modulation
- frequency modulation
- phase modulation
- analog vs. digital modulations

EXERCISE: MODULATION IDENTIFICATION

- Try to identify the type of modulation used in some sample transmissions

REVERSE ENGINEERING

- Using online resources
- Finding a signal with HackRF
- Signal analysis
- Determining signal characteristics (frequency, bandwidth, modulation, symbol rate)

EXERCISE: REVERSE ENGINEERING

- Investigate a device experimentally and/or online

DECODING DIGITAL SIGNALS

- Digital Modulations
- Synchronization
- Correlation

EXERCISE: DECODING

- Decode a digital radio transmission

Don't hesitate to call us. We are fluent in English and German.

TROOPERS
Need assistance?
+49 6022 508200

<https://www.troopers.de>
 +49 6221 480390
info@troopers.de

HM Training Solution www.hmtrainingsolutions.com
Need assistance? 

info@hmtrainingsolutions.com

THE DISCRETE FOURIER TRANSFORM

- Demystification of the most useful algorithm in signal processing
- The Fast Fourier Transform (FFT)

What Would the Attendees Gain?

A prototype HackRF software defined radio peripheral from Great Scott Gadgets will be provided to each student for use during the class. The HackRF will be available for purchase at the end of the class.

What should Attendees Bring?

LAPTOP

- There are no minimum processing power or memory requirements but signal processing is an intensive application, so more of both is always useful. Native Linux operation (not in a virtual machine) is strongly recommended. High-Speed USB 2.0 is required.


SYSTEM REQUIREMENTS:

- A Pentoo Linux bootable USB flash drive supporting all class activities will be provided. If you choose to bring your own software environment, be prepared to boot to the Pentoo drive just in case.
- We'll be working primarily with GNU Radio, an open-source signal processing framework. We will also use libhackrf, hackrf-tools, and gr-osmosdr. Additionally, you should install Baudline, a visual signal analysis tool.

Don't hesitate to call us. We are fluent in English and German.

TROOPERS
Need assistance?
+49 6022 508200

<https://www.troopers.de>
 +49 6221 480390
info@troopers.de

HM Training Solution www.hmtrainingsolutions.com
Need assistance? 

info@hmtrainingsolutions.com

WIRELESS DEVICES

Anything with a radio that you think might be fun to work with or show off.

Examples that people have brought in the past:

- Garage door remote controls
- Remote keyless entry devices
- Remote control toys
- Mobile phone jammers
- Amateur radio SDR equipment

About Your Trainer: Mike Ossmann

Michael Ossmann is a wireless security researcher who makes hardware for hackers. Best known for the open source HackRF, Ubertooth, and Daisho projects, he founded Great Scott Gadgets in an effort to put exciting, new tools into the hands of innovative people.

Twitter: [@michaelossmann](https://twitter.com/michaelossmann)

Don't hesitate to call us. We are fluent in English and German.

TROOPERS
Need assistance?
+49 6022 508200

<https://www.troopers.de>
 +49 6221 480390
info@troopers.de

HM Training Solution www.hmtrainingsolutions.com
Need assistance? 

info@hmtrainingsolutions.com

Booking

Sign-Up Form <https://www.troopers.de>

Voucher code: **TR18HMTSEB**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2018 or until seats have run out.

Contact

TROOPERS ORGANIZATION TEAM

Need assistance?



+49 6221 480390

info@troopers.de

Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Booking is also possible offline through your trusted partner from:



HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany



+49 6022 508200 info@hmtrainingsolutions.com



+49 6022 5089999 www.hmtrainingsolutions.com

Don't hesitate to call us. We are fluent in English and German.

TROOPERS
Need assistance?
+49 6022 508200

<https://www.troopers.de>



+49 6221 480390

info@troopers.de

HM Training Solution www.hmtrainingsolutions.com
Need assistance?



info@hmtrainingsolutions.com