Universal Radio Hacker

> The Universal Radio Hacker (URH) is a complete suite for wireless protocol investigation with native support for many common Software Defined Radios. URH allows easy demodulation of signals combined with an automatic detection of modulation parameters making it a breeze to identify the bits and bytes that fly over the air. As data often gets encoded before transmission, URH offers customizable decodings to crack even sophisticated encodings like CC1101 data whitening. When it comes to protocol reverse-engineering, URH is helpful in two ways. You can either manually assign protocol fields and message types or let URH automatically infer protocol fields with a rule-based intelligence. Finally, URH entails a fuzzing component aimed at stateless protocols and a simulation environment for stateful attacks.

https://github.com/jopohl/urh