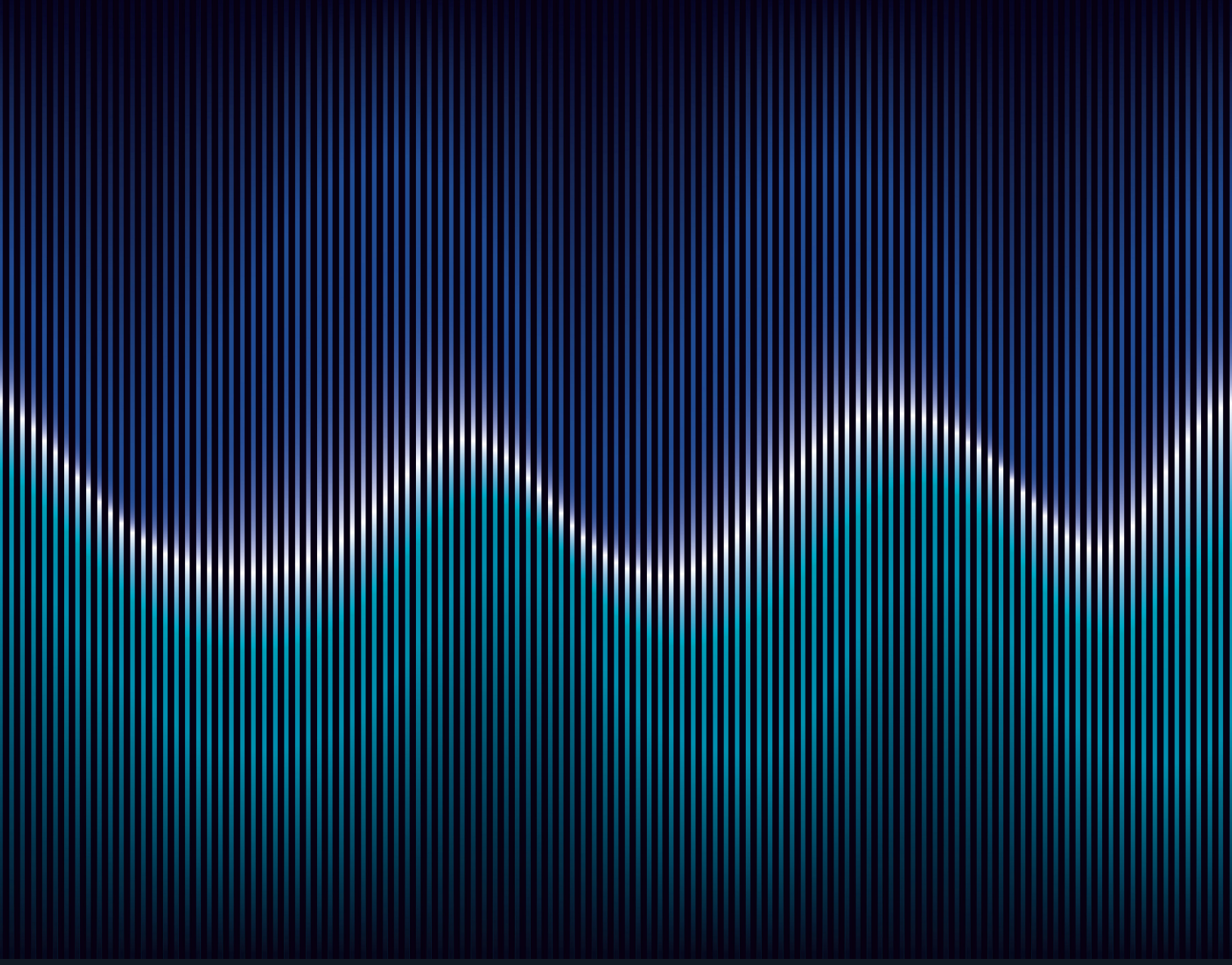

FISSURE

Frequency Independent SDR-Based Signal Understanding and Reverse Engineering

Assured Information Security · 315.336.3306 · **WWW.AINFOSEC.COM**

ais

FISSURE

FISSURE is an open-source RF and reverse engineering framework designed for all skill levels.

FISSURE has hooks for signal detection and classification, protocol discovery, attack execution, IQ manipulation, vulnerability analysis, automation, and AI/ML. The framework was built to promote the rapid integration of software modules, radios, protocols, signal data, scripts, flow graphs, reference material, and third-party tools. FISSURE is a workflow enabler that keeps software in one location and allows teams to effortlessly get up to speed while sharing the same proven baseline configuration for specific Linux distributions.

The RF Framework for Everyone

The friendly Python codebase and user interface allows beginners to quickly learn about popular tools and techniques involving RF and reverse engineering. Educators in cybersecurity and engineering can take advantage of the built-in material or utilize the framework to demonstrate their own real-world applications. Developers and researchers can use FISSURE for their daily tasks or to expose their cutting-edge solutions to a wider audience. As awareness and usage of FISSURE grows in the community, so will the extent of its capabilities and the breadth of the technology it encompasses.

FEATURES

The framework and tools included with FISSURE are designed to detect the presence of RF energy, understand the characteristics of a signal, collect and analyze samples, develop transmit and/or injection techniques, and craft custom payloads or messages. FISSURE contains a growing library of protocol and signal information to assist in identification, packet crafting, and fuzzing. Online archive capabilities exist to download signal files and build playlists to simulate traffic and test systems.

FISSURE supports multiple types of RF hardware and reuses existing analysis tools developed by the Cyber community to give operators more flexibility and an instant sense of familiarity. The framework was designed to be easily modified and allow for the integration of already established standalone components with minimum rework. Helpful guides and reference material are included in the software to make it easier to modify the code and integrate your own solutions.

How to Contribute

FISSURE gets its power from the contributions of programmers in the open-source, cybersecurity, and engineering communities. Leave a comment in the GitHub Discussions tab to contribute to the growth of FISSURE:

- Suggest RF and cybersecurity tools frequently used by the community
- Provide installation scripts for new software
- Supply attacks, scripts, and exploits
- Propose more types of hardware and SDRs to be integrated
- Offer new GUI features and improvements
- Generate feedback and material for lessons and help items
- Produce library material for RF protocols of interest
- Share your favorite IQ analysis scripts for Python
- Collaborate with AIS to include your software as a module

Contact AIS to integrate FISSURE into other platforms/applications or to include your software as a new module.

github.com/ainfosec/fissure

bd@ainfosec.com

Assured Information Security
315.336.3306
WWW.AINFOSEC.COM

About Assured Information Security

AIS is a cyber and information technology company that plays a leading role in supporting critical cyber operations for the United States Department of Defense and Intelligence Community. AIS employs expert engineers and research scientists across the United States.