SRE with Ghidra
CAE Forum – 18 September 2019
Software Reverse Engineering (SRE)

• “...a process of recovering the design, requirement specifications and functions of a product from an analysis of its code.”
  – GeekforGeeks

• “What’s in Your Binary?”

• Key skill of cyber security

• Especially important for black-box software
  – Ghidra’s core use case
Ghidra

- SRE Framework
- Created and maintained by NSA Research
  - Much like the R&D branches of major corporations
  - Seek innovative solutions to mission problems
  - Less like academic research
- Released to public early March at RSA2019
- Released source on GitHub late March
- Released v9.0.4 mid May
Demo Resources

• NSA Codebreaker Challenge
  – https://codebreaker.ltsnet.net/resources
  – Windows Binary from 2014
  – (Solution in 2015 Tech talk)

• Ghidra
  – https://ghidra-sre.org
  – (Version 9.0.4)