# RE Preprocessor

Capstone Assessment

The RE Proprocessor (REPr) is a tool designed to help software reverse engineers and capture-the-flag competitors. Inspired by tools like CyberChef and Binwalk, REPr is a tool designed to identify files and process them for further human analysis. The project seeks to blend aspects of high-level programming, like a friendly interface and highly modular design with lower-level systems which will be used for identifying files. While not new, this mix of high and low will create many interesting challenges to overcome.

The curriculum at UC has set this project up for success. By teaching a combination of high- and low-level languages the knowledge necessary to build this tool has already been taught. This project is an application of these technologies to build something useful. This project goes beyond what is taught in the classroom however, student orgs like Cyber@UC have also shown me the gap where this project could uniquely fit in.

The CO-OP program was the reason I picked UC, and I was very fortunate to complete all five of my CO-OPs with Northrop Grumman as a Cyber Software intern. Like UC’s curriculum, I was exposed to a lot of different technologies and was given the opportunity to see them in real world use. I plan to take a lot of lessons I learned from working at Northrop, like building modularly, designing ahead, and anticipating use cases and applying them to this project.

While competing on Cyber@UC’s capture-the-flag (hacking competitions) team I often found myself frustrated by challenges which involved identifying obscure file types. A few tools exist which can attempt to identify more esoteric files, but they often struggle with files which are too far off the beaten path.

I plan to build this project in several steps, starting with the bare minimum and working up to a more complete ‘product’. At first, the project will only be a command line utility and will have limited modules for file identification (based off existing tools like Binwalk). As the project matures, I will work to integrate it with existing pieces of reverse engineering software like Ghidra, IDA, and Binary Ninja. As a final stretch goal, I plan to add more bespoke file identifiers in an attempt to surpass existing tools.

Because I am working on this project alone, I plan to rely on my own sense of progress and that of my advisor to know the project’s health. I plan to take this project seriously and treat it as a real product which I’d like others and myself to use. In doing this, I hope to build a useful, extensible tool.