Goals

Goals

Our goal during basic static analysis is to triage correctly and as quickly as possible. Now that we've learned a bit about how to perform basic static analysis and how to correlate static indicators, let's deploy another tool that can assist in this phase and hopefully speed things up.

Introducing, Capa

Capa is a program that detects malicious capabilities in suspicious programs by using a set of rules

The program's primary strength is how **it leverages rules**. Capa has a default rule set, but also has an open-source repository of rules where anyone can contribute. You can see the Capa rule repository here

It will Run on FlareVm.