

CSEC 464 Computer System Forensics
Professor Yin Pan

Proposers

Zachary Mangiaracina
Grant Foti
Christian Luca
Alex Sutay

Proposal Title

Coalescence Toolkit

Abstract

The Coalescence Toolkit will be a combination of several different tools that has the ability to read a directory of files and generate a report detailing anything with forensics significance. The report will explain what tool was used, what information was extracted and what its significance is from a forensics perspective. The tool should be able to determine what kind of file is being run against it to then run the proper subsequent tools. The toolkit will also make use of origami for pdfs with the main goal to be attempting to detect information from normal pdfs, encrypted pdfs, and malicious pdfs.

Included Tools

- Exiftool (<https://exiftool.org/>)
- Jhead (<https://www.sentex.ca/~mwandel/jhead/>)
- Pdftinfo (<https://www.xpdfreader.com/pdftinfo-man.html>)
- Origami (<https://github.com/gdelugre/origami>)