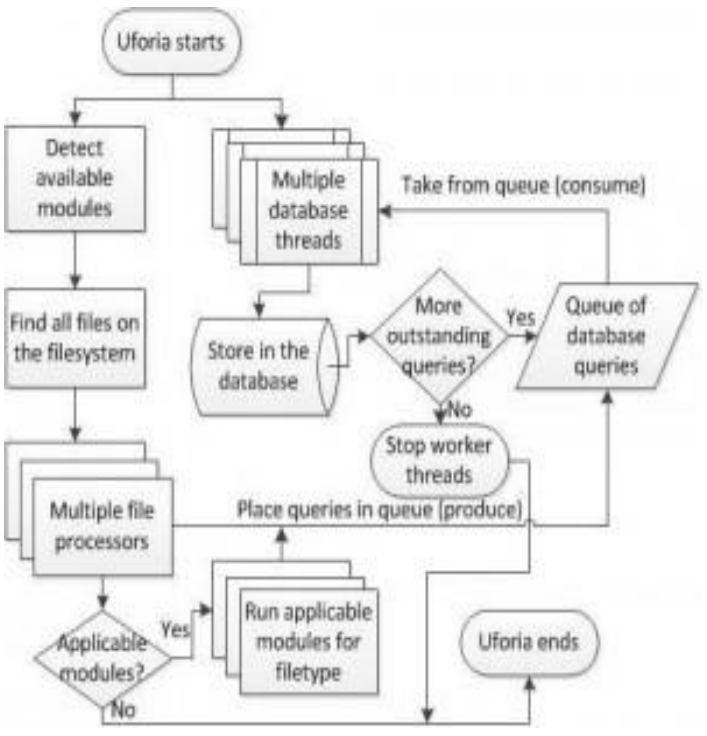
Uforia

The research initiative Uforia (Universal Forensic Indexer and Analyzer) is a simple, flexible and extensible framework for metadata collection and processing. Uforia is different from conventional forensic tooling by being completely modularized. Not only can the source and method of the evidence item collection, database type and database handler be changed, but for every 'evidence item' a dynamic number (from zero to unlimited) of parsers can be run.



Since publication in the Springer Journal of Virology, recent developments have been support for SQLite3 databases, a MacOSX-compatible branch, full document parsing with Apache Tika, overall performance improvements and support for many more filetypes.

We are currently exploring the options for the first front-end interface for viewing the parsed metadata, likely to be based on the Apache Lucene/ ElasticSearch frameworks. Uforia is licensed under the GPLv2 and is written in Python.

Source code is available as a Github repository at:

http://uforia.dhcp.net/.

The Uforia development-team can be reached via E-mail:

uforia@dhcp.net