Uforia: Universal forensic indexer and analyzer

Arnim Eijkhoudt

Department of Informatics, DMCI

University of Applied Sciences

Amsterdam, Netherlands

a.eijkhoudt@hva.nl

programming, concept and design

Tristan Suerink

Department of IT

National Institute for Subatomic Physics

Amsterdam, Netherlands

tsuerink@nikhef.nl

concept

Abstract

Uforia is a simple, flexible and extensible framework for analysis and parsing of file metadata. It has been written in Python and is available under the GPLv2.

Uforia traverses a file-system and triggers a configurable set of modules for every file it encounters. Out-of-the-box, Uforia conforms to the NIST standard for forensic hashing by storing the currently most common three cryptographic hashes for each file: the MD5, SHA-1 and SHA-256 hash.

Uforia strives for optimal scaling of the metadata-analysis by offering an easily configurable threading model of both its Producers and Consumers. Additionally, the interface is written and intended to be as loosely coupled as possible. It is therefore easy to change the Producer's and Consumer's functionalities to match the specific needs of the user. Similarly, Uforia attempts to reduce database redundancy to a minimum, by only loosely coupling database tables and delegating the relevant parts to the individual modules. Each of these modules will perform its tasks asynchronously of Uforia and is automatically detected, registered and called to handle its specific filetypes.

Uforia does not yet come with a front-end interface for viewing the information stored in the database, but the database contents stored could theoretically already be applied to a wide variety of situations, such as searching for specific metadata or information during a forensic investigation, for filesystem-level deduplication or even for creating custom known file hash tables. The interface for creating new database handlers and modules has been simplified as much as possible, allowing for easy extensibility and tailoring to each use-case's specific requirements.

If you would like to participate in Uforia, please contact the development team by E-mail: uforia@dhcp.net.