Omnibus Documentation

InQuest Labs

Aug 03, 2018

Contents

Omnibus is an easy to user interactive command line applications for users to perform OSINT investigation of artifacts such as IP addresses, domains, email addresses, user names, file hashes, and Bitcoin addresses.

An Omnibus is defined as a volume containing several novels or other items previously published separately and that is exactly what the InQuest Omnibus project intends to be for Open Source Intelligence collection, research, and artifact management.

The project requires both MongoDB and Redis running in order to store artifact data long term and while within a CLI session, respectively.

CHAPTER 1

User Guide

- Getting Started

1.1 Installation

Omnibus is written for Python 2.7 and has been tested on OS X 10.13.6, Ubuntu 16.04, and Ubuntu 18.04.

To get started, first clone the GitHub repository:: git clone https://github.com/InQuest/omnibus

Move into the new directory and install the required Python libraries:: cd omnibus pip install -r requirements.txt

1.2 Databases

Omnibus requires that MongoDB and Redis be running and reachable by the host that runs the omnibus-cli.

The following file holds host and port configuration details for the databases. If you have them both running on your local etc/omnibus.conf

1.3 API Keys

All of your API keys for third party service modules must be stored within etc/apikeys.json. For each named service simply paste your API key as the quoted value within the JSON file.

All services used are free to receive an API key, but if you don't enter one for a given service and attempt to run its module it will simply return no results.

1.4 Vocabulary

- Using Omnibus

1.5 Interactive CLI

1.6 Artifacts

1.7 Sessions

1.8 Modules

1.9 Machines

Machines are used to run every available module for an artifact type against a user specified artifact. This is designed to make it simple to collect all available data on an artifact with one command.

1.9.1 Usage

1.10 Reporting

1.11 Redirection

- Quick Reference

1.12 Quick Reference

CHAPTER 2

Indices and tables

- genindex
- modindex
- search