**PICK SYSTEM INSTALLATION GUIDE**

PICK is a system that allow analysts to create a visualization that depicts a series of events

that occurred during an attack on a system. The system creates log entries by validating log files with given validation rules given by the analyst. Once a log file is validated, the system will ingest and use Splunk to parse log files into log entries that will be stored in the database as nodes within a graph along its relationships.

**Dependencies:**

* Python 3 ver. 3.8.0 - website: <https://www.python.org/downloads>
* Splunk Enterprise ver. 8.0.3- website: <https://www.splunk.com/en_us/download/splunk-enterprise.html>
* PyQT5 5.14.1 - command line: **pip install PyQt5**
* PyQt5-sip 12.7.0 – command line: **pip install PyQt5-sip**
* PyMongo 3.10.1 – command line: **pip install pymongo**
* Splunk-sdk 1.6.12 - command line: **pip install splunk-sdk**
* psutil 5.7.0 - command line: **pip install psutil**
* python-dateutil 2.8.1- command line: **pip install python-dateutil**

(Located in Requirements.txt)

**Additional Useful Software:**

* MongoDB Compass: GUI Representation & Control of Mongo Database <https://www.mongodb.com/products/compass>

**How to Run:**

* type **git clone https://github.com/CS4311-spring-2020/pick-tool-team05-static-variables**
* provide the executable path for MongoDB in the file **\_\_init\_\_.py** file to start the MongoDB Server
* provide Splunk username and password in the command line.
* run **python3 \_\_init\_\_.py**

**Trouble shooting:**

* If you are getting the error **“No connection could be made because the target machine actively refused it,** “you should reinstall splunk.

**Known Issues:**

* User must log in into splunk server in command line after running splunk.
* Main Window does not refresh when vectors are added or deleted. PICK must be restarted in order to see new vectors or remove deleted vectors.
* Event Configuration information is hardcoded into \_\_init\_\_.py
* In order to run the MongoDB server running in the background when the PICK system runs you need to provide the MongoDB executable path.