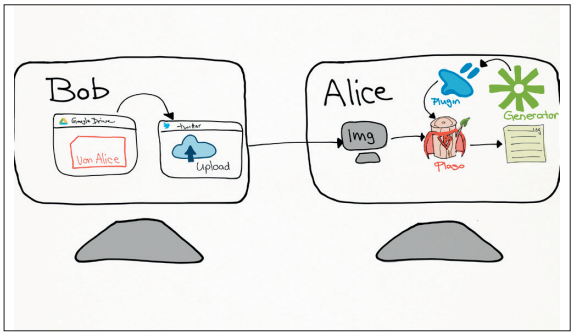
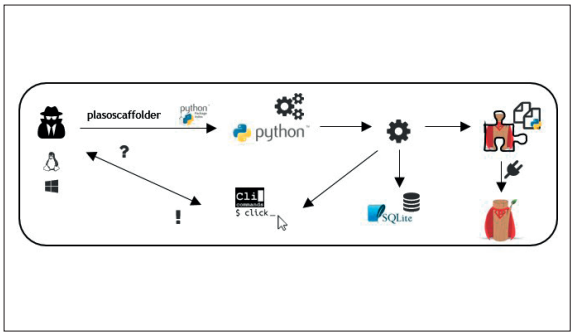
Claudia
Saxer

Diplomandin	Claudia Saxer
Examinator	Jürg Jucker
Experte	Maurin Egler, Synpulse Schweiz AG, Zürich, ZH
Themengebiet	Software
Projektpartner	Google Switzerland GmbH, Zürich, ZH

Plaso SQLite Plugin Scaffolder

Command Line Interface in Python





Ausgangslage: Plaso ist die Backend-Engine für das Tool Log2timeline, das Google für die forensische Datenanalyse verwendet. Log2timeline ist ein Tool, das aus einem Image alle Informationen sammelt, um eine Super Timeline zu erstellen, das ein riesiges Logfile darstellt. Plaso ist zu einem grossen Opensource Framework gewachsen, das von vielen Security Engineers verwendet wird und beinhaltet eine Ansammlung von Plugins. Plugins werden von Log2timeline verwendet, um Informationen von einem File zu extrahieren. Ein Grossteil der Plugins wurden für verschiedene SQLite Datenbanken entwickelt, und die Nachfrage für neue Plugins für SQLite-Datenbanken steigt. Im Moment involviert das Hinzufügen eines Plugins das manuelle Verändern von mehreren Files in vorgegebener Reihenfolge.

Vorgehen/Technologien: In einer ersten Phase soll deshalb das Erstellen von SQLite Plugins mit einem Gerüst vereinfacht und teilweise automatisiert werden. Somit sollen auch Security Engineers, die nicht viel Erfahrung mit der Entwicklung haben, schnell und einfach ein Plugin zu Plaso hinzufügen können. Dies verringert den manuellen Aufwand für das Schreiben der Plugins, sowie für die Codereviews. Das Tool soll ein ähnliches Konzept verwenden, das in anderen Frameworks als «scaffolding» bekannt ist. Das Tool soll vom Benutzer Eingaben entgegennehmen und daraus Files generieren sowie bestehende editieren, um schnell ein neues SQLite Plugin zu erstellen.

Ergebnis: Im Rahmen dieses Projektes wurde ein Command Line Interface Tool erstellt, das interaktiv Daten des Benutzers entgegennimmt und validiert sowie Daten einer SQLite-Datenbank auswertet. Die Applikation erlaubt durch ihren Aufbau das einfache Hinzufügen von weiteren Plugin Scaffolders. Der SQLite Scaffolder besitzt einerseits einen interaktiven Vorgang und erlaubt auch das Parametrisieren von einigen Eingaben. Die Kommunikation zwischen User und Applikation läuft mit dem Command Line Interface Tool Click, das auf optparse aufbaut. Die Files Templates wurden mit Jinja2 erstellt und sind einfach anpassbar. Das Tool beinhaltet das Editieren, Erstellen sowie Kopieren von Files. Die generierten Files sowie das Programm sind mit Pylint validiert.