HSLU Hochschule Luzern

Anforderungen an ein Open Source Smartphone Forensik Tool in der Schweiz mit Massnahmen zur Implementierung

Masterthesis im Studiengang Wirtschaftsinformatik an der
Hochschule Luzern

Es ist nur das Management Summary sowie das Inhaltsverzeichnis der Arbeit einsehbar. Bei Interesse an der Arbeit, bitte ich um Kontaktaufnahme.

Autor: *Thomas Meier*
[redacted]
Matr. Nr.: [redacted]

Erstgutachter: [redacted]

Ort, Datum: Arbedo, 08.05.2023

Management Summary

Mit der vorliegenden Masterthesis sollen die *Anforderungen an ein Open Source Smartphone Forensik Tool in der Schweiz* identifiziert und *Massnahmen zur Implementierung* aufgezeigt werden. Für die Identifizierung der Anforderungen für die Forschungsfrage 1a *welche Anforderungen werden an ein Open Source Smartphone Forensik Tool gestellt, damit die Ergebnisse in der Schweiz gerichtlich verwendet werden können* und 1b, *welche Anforderungen werden an ein Open Source Smartphone Forensik Tool gestellt, damit es auch von Personen bedient werden kann, welche nur über bescheidene IT-Anwendungskentnisse verfügen* wurde eine Literaturrecherche durchgeführt, welche nach der Theorie von Requirements Engineering kategorisiert und ausgewertet wurde. Zusätzlich wurden Interviews mit Fachpersonen der digitalen Forensik der kantonalen Polizeikorps geführt, um weitere Anforderungen zu eruieren, einen Praxisbezug zu schaffen und die Erkenntnisse aus der Literaturrecherche einzuordnen. Für die Beantwortung von Forschungsfrage 1b wurden besonderem Fokus auf das Thema Human Computer Interaction ausgewertet. Die Forschungsfrage 2 lautet *wie können diese Anforderungen im Rahmen einer Semesterarbeit durch Studierende der Hochschule Luzern in eine Software implementiert werden?* Dabei werden die weiteren Schritte vom Requirements Engineering konkret am Projekt Open Source Smartphone Forensik Software angewendet und verständlich aufgezeigt.

Mit dem gewählten Verfahren wurden insgesamt 103 Anforderungen an ein Open Source Smartphone Forensik Tool identifiziert. Diese Anforderungen wurden im Sinne von Requirements Engineering kategorisiert und tabellarisch dargestellt. Die Mehrheit der Anforderungen für die gerichtliche Verwendbarkeit von Forschungsfrage 1a, befindet sich im Bereich der funktionalen Anforderungen und betreffen Anforderungen an Produktfunktionen, Datenarten und Extraktionen. Bei den Randbedingungen sticht die Vielzahl der Anforderungen an Support und Dokumentation heraus. Wesentlich weniger Anforderungen wurden für eine einfache Bedienbarkeit von Forschungsfrage 1b identifiziert. Hier liegt der Fokus der Anforderungen bezüglich Ansicht und Erlebnis bei der Nutzung. Die Massnahmen für die Implementierung des Open Source Smartphone Forensik Tools umfassen Schritte wie das Projekt initiieren, an der Hochschule Luzern

ausschreiben, den Source Code auf einer auserwählten Plattform zugänglich machen und interessierte und sachverständige Personen zur Mitarbeit einladen.

Nach Beantworten der Forschungsfragen zeigt sich, welch umfassender Aufwand die Entwicklung eines Open Source Smartphone Forensik Tools bedeutet. Beispielsweise allein für den Support und die Dokumentation würden geschätzt hohe zeitliche und finanzielle Investitionen in das Projekt anfallen, was wohl kaum im Rahmen einer Semesterarbeit an der Hochschule Luzern umsetzbar wäre. Die in den Interviews aufgespürten Anforderungen im Bereich Datenarten und Extraktion zeigen deutlich, wie wichtig eine stetige Aktualisierung und Weiterentwicklung der Software für die Praxis ist.

Zudem hat die Literaturanalyse ergeben, dass bereits verschiedene staatliche oder vom Staat unterstützte Organisationen, wie zum Beispiel Homeland Security in den USA und FORMOBILE auf europäischer Flughöhe, an einer solchen Open Source Lösung arbeiten. Als Fazit dieser Arbeit kann gesagt werden, dass die Anforderungen an ein Open Source Smartphone Forensik Tool sehr umfassend sind und die Massnahmen zur Implementierung nur erahnen lassen, welch immenser zeitlicher und finanzieller Aufwand mit der Umsetzung verbunden wäre.

Aus diesem Grund wird empfohlen, eine Mitarbeit der Studierenden der Hochschule Luzern bei den bestehenden Projekten auf internationaler Ebene zu prüfen. Dies würde die Gelegenheit bieten, von vorhandenem Fachwissen zu profitieren, das persönliche Netzwerk zu erweitern und Einblick in die Arbeitsweise einer solchen Organisation zu erhalten.

Die Analyse hat gezeigt, dass für die Befragten kantonalen Polizeikorps der Mehrwert eines öffentlich zugänglichen Quellcodes nicht direkt ersichtlich ist. Dagegen wurde das Bedürfnis nach einer hoch automatisierten Software identifiziert, um die eingesetzten Personalressourcen minimal zu halten. Folglich könnte der Fokus für weitere Schritte auf einer Open Source KI-Lösung von extrahierten Daten gelegt werden.

Inhaltsverzeichnis