Success Story
COMET

SBA-K1
SBA Research gGmbH
Programme: COMET – Competence Centers for Excellent Technologies
Programme line: K1-Centres
Project 3.1 – Digital Forensics, duration and type of project:
04/2017 – ongoing, multi-firm

SmartForensics: LEAP

Immer mehr kriminelle Aktivitäten werden über Smartphones koordiniert bzw. teilweise durchgeführt. Smartphones werden immer billiger, die Speicherkapazitäten immer größer. Doch vollständige forensische Analysen von Smartphones sind zeitraubend, kostenintensiv und die entsprechenden Abteilungen der Ermittlungsbehörden sind oft auf Wochen hin ausgebucht. Damit ergibt sich die Notwendigkeit, den Ermittlern vor Ort ein Werkzeug zur Verfügung zu stellen, das in der Lage ist, in kurzer Zeit eine erste aussagekräftige Einschätzung über die fallspezifischen Inhalte eines beschlagnahmten Smartphones zu liefern.

Ausgangssituation: Automatisierung notwendig

Ermittlerinnen und Ermittler in verschiedenen Sparten der Kriminalitätsbekämpfung, wie z.B. der Bekämpfung von Schlepperwesen, stehen während eines Einsatzes oft vor einer schwierigen Entscheidung: Soll ein beschlagnahmtes Smartphone für eine eingehende forensische Untersuchung an die entsprechenden Kolleginnen und Kollegen weitergeleitet werden, um einige Wochen später eine detaillierte Analyse zu erhalten, oder ist dieser Aufwand in der konkreten Situation zu hoch?

Ist es stattdessen möglich, ein Werkzeug zu entwickeln, das die Lücke zwischen dieser Fragestellung und einer vollständigen forensischen Analyse schließt, indem in extrem kurzer Zeit eine Art „Quickcheck“ des beschlagnahmten Geräts durchgeführt werden kann, bei dem vorrangig auf die fallspezifischen Charakteristika und Anforderungen der Ermittlerinnen und Ermittler Rücksicht genommen wird?

Mit dieser Fragestellung wurden die beiden Firmenpartner T3K Forensics und Kibosec von internationalen Strafverfolgungsbehörden immer öfter konfrontiert, und gemeinsam mit SBA Research wird seit April 2017 an einer entsprechenden Lösung gearbeitet.

Lösungsansatz: LEAP Law Enforcement Analytical Product

Die Partner T3K Forensics, Kibosec und SBA Research entwickelten daher in intensiver kooperativer Zusammenarbeit ein Framework, das verschiedenste Bedürfnisse von Ermittlungsbehörden erfüllen kann, gleichzeitig regulatorischen und gesetzlichen Anforderungen gerecht wird und rasch und gezielt eine erste Einschätzung in Form eines leicht verständlichen und aussagekräftigen Berichts zur Verfügung stellen kann. Dabei wird auf modernste Methoden etwa von Machine Learning, Deep Learning und Latent Space Virtualisierungen zurückgegriffen, die es ermöglichen, binnen 60 Minuten eine grundlegende und umfassende Erstanalyse fertigzustellen.

Federal Ministry for Digital, Business and Enterprise
bmvit Austrian Ministry for Transport, Innovation and Technology

Ein solches Werkzeug soll Ermittlerinnen und Ermittlern in kurzer Zeit helfen, eine Einschätzung zu treffen, ob eine vollständige forensische Untersuchung angezeigt ist und gegebenenfalls die im „Quickcheck“ bereits gesammelten Erkenntnisse der jeweiligen Forensikabteilung als Startpunkt für deren eingehende Analysen zur Verfügung zu stellen.

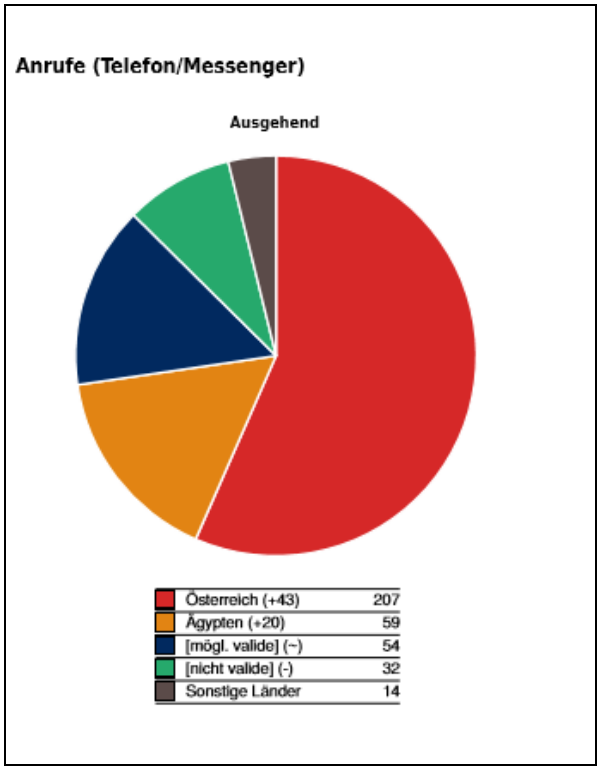

Fig. 1: Visualisierung einer fallspezifischen Berichtskomponente von LEAP

Impact and effects

Unser Partner T3K, der auf Forensikschulungen im Umfeld von Sicherheitsbehörden spezialisiert ist, konnte erste frühe Prototypen von LEAP mit ausländischen Behörden im konkreten Feldeinsatz bereits testen.

Dabei zeigt sich, dass insbesondere bei größervolumigen Ermittlungen, bei denen eine große Anzahl von Geräten in verhältnismäßig kurzer Zeit bewertet werden müssen, ein solches Werkzeug einen enormen Mehrwert für die Mitarbeiterinnen und Mitarbeitern vor Ort darstellt.
Zwar müssen noch zahlreiche technische Aspekte und Spezifika weiter analysiert, erweitert und verbessert werden, aber bereits in diesem frühen Stadium ist der Nutzen bereits deutlich sichtbar. Ein solches Toolkit, das auch weniger forensikversierten Beamtinnen und Beamten die Möglichkeit gibt, in relativ kurzer Zeit zu beurteilen, ob eine tiefergehende Analyse notwendig erscheint, ist international bislang einzigartig und schließt eine Lücke, die in Zukunft eher noch größer als kleiner werden wird.

In den kommenden Monaten und Jahren sollen einerseits die Analysemethoden laufend verfeinert und weiter verbessert werden, indem LEAP Berichte mit späteren Erkenntnissen von vollständigen forensischen Analysen abgeglichen werden, auf der anderen Seite sollen in weiteren Projekten spezifische kriminaltechnische Spezialfälle (z.B. Bekämpfung des Schlepperwesens) mit dem LEAP Framework realisiert werden. Zusätzlich soll die Analysedauer von LEAP laufend gesenkt werden.

Mittelfristig erlaubt die COMET Kooperation so zwei kleinen, hochspezialisierten österreichischen Unternehmen, im internationalen Wettbewerb in diesem Umfeld weiter Fuß zu fassen und einen erheblichen Wettbewerbsvorteil zu erarbeiten.

Contact and information
SBA-K1

SBA Research gGmbH
Favoritenstrasse 16, A-1040 Wien
T +43 (1) 505 36 88
E office@sba-research.org, www.sba-research.org

Project coordinator
DI Peter Kieseberg

Project partners

Organisation	Country
T3K Forensics	Austria
Kibosec	Austria