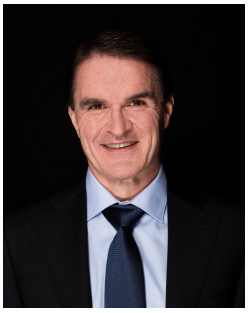
Möglichkeiten und Grenzen in der Auswertung von Smartphones am Beispiel von WhatsApp



Beat Grossenbacher

Dipl. Informatik Ing. ETH
Executive MBA HSG
MAS Economic Crime Investigation Hochschule Luzern (MAS ECI 12)

Nach einer 25-jährigen Tätigkeit in der Informationstechnologie hat er anfangs 2016 die Firma FORINCO AG in Zug mitgegründet. Die Firma ist spezialisiert in der Aufklärung von Wirtschaftsdelikten. Mit Methoden aus der digitalen Forensik wie auch mittels Informationsbeschaffung wird nach Spuren der Täterschaft gesucht. Das Unternehmen arbeitet sowohl für staatliche Behörden wie auch für private Auftraggeber und ist bestens vernetzt. Beat Grossenbacher hat das MAS ECI 12 absolviert und ist Mitglied bei der Schweizerischen Expertenvereinigung «Bekämpfung der Wirtschaftskriminalität».

„In this modern age, it is hard to imagine a crime that does not have a digital dimension" (Eoghan Casey, Digital Evidence and Computer Crime). In einer vernetzten Gesellschaft soll es also in einem Verbrechen immer eine digitale Spur geben. Dieser Frage bin ich in meiner Arbeit nachgegangen. Der Frage, wie gut man Spuren auf Smartphones finden und mit welchen Werkzeugen und Methoden man sie auswerten und gewinnbringend in einem Ermittlungsverfahren nutzen kann. Im Fokus meiner Untersuchung lag WhatsApp, eine der meistgenutzten Chat-Anwendungen. Die Untersuchung der Verkaufszahlen von Smartphones im Jahr 2014 in der Schweiz hat verdeutlicht, dass ich mich weiter auf die Vertreter von iOS- und Android-Smartphones konzentrieren konnte.

Das Angebot an Werkzeugen zur forensischen Analyse von Smartphones ist vielfältig. In meiner Arbeit habe ich sowohl kommerziell forensische als auch Open Source und nicht-forensische Werkzeuge auf verschiedene Fragestellungen angewendet und ihre Resultate bewertet und beurteilt.

Mit vier Smartphones und sechs Werkzeugen ging ich den Fragen nach,

- wie gut sich die Werkzeuge für bestimmte Fragestellungen eignen,
- ob teurere kommerzielle Werkzeuge besser als Open Source bzw. nicht-forensische Werkzeuge sind,
- ob Smartphones seit ihrem „Dasein" (ab 2010) vermehrt in WK-Delikten eingesetzt werden,
- wo die Schwierigkeiten und Grenzen im Prozess der Datenextraktion von Smartphones liegen.

Aus Sicht eines Ermittlers habe ich dazu acht Fragestellungen inszeniert und mit dem Versand von WhatsApp-Nachrichten auf den Smartphones nachgestellt. Die Untersuchungen haben gezeigt, dass es i. d. R. nicht ein einziges Werkzeug gibt, das eine Fragestellung optimal beantwortet. Um ein bestes Resultat zu erhalten, drängt sich u. U. der Einsatz mehrerer Werkzeuge auf. Die kommerziell forensischen Werkzeuge konnten zu den meisten Fragestellungen die besten Erkenntnisse und Antworten liefern. Nur zu einer der Fragestellungen lieferten Open Source und nicht-forensische Werkzeuge aussagekräftigere Resultate.

Die Strafverfolgung sieht sich dabei mit verschiedenen Problemen konfrontiert. Zu nennen sind die wachsende Speicherkapazität der Smartphones und der Trend der Smartphone-Hersteller zum Datenschutz. Mit der zunehmenden Speicherkapazität wächst zugleich der Zeitaufwand, den eine Datenauslesung beansprucht und verdeutlicht, dass auch eine „rasche" Datenauslesung zeitlich sehr aufwendig ist. Die Smartphone-Hersteller erhöhen den Datenschutz und setzen vermehrt eine Standardverschlüsselung ein, die die Möglichkeiten in der Datenauslesung zunehmend einschränken. Bzgl. der Relevanz von Smartphones in WK-Delikten habe ich das Forensische Asservate Tracking System der Kantonspolizei Zürich ausgewertet. Das Ergebnis zeigt, dass Smartphones trotz ihrer Beliebtheit nicht vermehrt in WK-Delikten eingesetzt werden.

Das Smartphone mag eine Quelle für digitale Spuren sein, doch aus Sicht der Ermittlung muss man vermehrt auch andere Quellen miteinbeziehen. Quellen, die eine Person nutzt und die unbewusst Datenkopien enthalten können. Die Cloud, der lokale Backup oder eine Speicherkarte ist bestens geeignet, um im Rahmen einer Ermittlung willkommene Erkenntnisse zu liefern.

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Grafenauweg 10
Postfach 7344
CH-6302 Zug
+41 41 757 67 67
ifz@hslu.ch