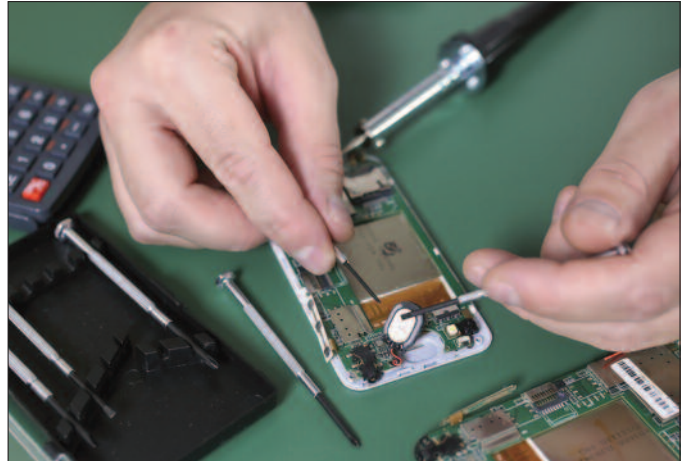




Panama City: Politiker, Sportler und Prominente sollen ihr Geld in „Offshore-Firmen“ in Panama versteckt haben.



Mobile Forensik: Die Auswertung von mobilen Geräten liefert der Polizei oft beweisrelevante Informationen.

Spuren sichern im Internet

Internationale Expertinnen und Experten tauschten Erfahrungen aus bei der digitalen Beweismittelsicherung, in der „Digital Investigation Conference“ am 13. und 14. Oktober 2016 in Wien.

Die Veröffentlichung der „Panama-Papers“ überführte im April 2016 zahlreiche Politiker und Prominente der Steuerflucht. Es handelte sich um vertrauliche Unterlagen der Firma „Mossack Fonseca“ – einem internationalen Wirtschaftsunternehmen mit Sitz in Panama-Stadt. Das Daten-Leck dokumentierte, wie Milliarden von Euro an Konten von Briefkastenfirmen weitergeleitet wurden, um Steuern oder rechtliche Sanktionen zu umgehen. 11,5 Millionen interne Dateien wurden den Mitarbeitern der „Süddeutschen Zeitung“ zugespielt. Es handelte sich unter anderem um 4,8 Millionen E-Mails, 2,1 Millionen PDF-Dokumente, 1,1 Millionen Bilder und 320.000 Textdokumente. Um die Daten verwerten zu können, mussten 1,5 Terabyte Datenmaterial analysiert werden.

Die Herausforderung bestand dabei nicht im Umfang, sondern in der Heterogenität der Daten. Deswegen wurde die Softwarefirma *Nuix* zur Hilfe gezogen. „Die Daten sind uns über einen Zeitraum von mehreren Monaten zugespielt worden. Es ist aufwendig, Tabellen, Abbildungen, PDF-Dokumente maschinell lesbar zu machen und mit anderen Textdokumenten zu vergleichen. Sie sind wie Bilddateien – man kann den Text nicht extrahieren“, sagte Carl Baron, Senior Solutions Consultant der Firma *Nuix* bei der „Digital Investigation Conference“, die auf Initiative des

Bundeskriminalamts Wien am 13. und 14. Oktober 2016 in der Marokkanerkaserne in Wien stattfand. „Wir haben die Methode der optischen Zeichenerkennung genutzt und damit die Daten in Text umgewandelt. Der Text wurde in einen Index und eine Datenbank eingepflegt.“ Durch die Stichwortsuche konnten Beziehungen zwischen den Daten erkannt werden, zum Beispiel Namen mit Firmen in Verbindung gebracht werden. Wenn in einer E-Mail ein Name aufgetaucht war, konnte man dann mithilfe der Stichwortsuche herausfinden, in welchen anderen Dokumenten dieser Name wieder vorkommt. Auf diese Art und Weise wurden zahlreiche Fälle der Steuerhinterziehung und Geldwäsche aufgedeckt.

IT-Forensik-Fachtagung. An der „Digital Investigations Conference 2016“ nahmen 60 Datenforensiker und IT-Ermittler aus dem Bundeskriminalamt und den Landeskriminalämtern teil sowie Vertreter der Zentralstelle des Bundesministeriums für Inneres (BMI) und des Bundesministeriums für Finanzen. Außerdem waren Sachverständige und Wirtschaftsprüfer vertreten. Die Programminhalte umfassten unter anderem die Bereiche E-Discovery, mobile Forensik und Cloud-Forensik sowie die effiziente und rasche Analyse von Bild- und Videodateien. In Kooperation mit der Firma *Arina AG* kamen Experten aus dem Ausland nach Wien, unter an-

derem aus Kanada und Australien. Sie brachten den Teilnehmern in Vorträgen und Workshops die aktuellen Entwicklungen aus den unterschiedlichen Bereichen und Teilgebieten der digitalen Beweismittelsicherung näher.

„Wir arbeiten täglich mit den Programmen, die bei dieser Veranstaltung präsentiert worden sind. Die Teilnehmer bekommen Informationen aus erster Hand – nämlich von jenen Menschen, die die Technologien mitentwickelt haben“, sagte Mag. Leopold Löschl, Leiter des Cybercrime-Competence-Centers (C⁴) im Bundeskriminalamt. „Die Vernetzung ist in der digitalen Beweismittelsicherung wichtig, denn Lösungen müssen auf internationaler Ebene gefunden werden.“

Ziel der Veranstaltung war die Weiterbildung der Mitarbeiter, die in diesen Fachbereichen tätig sind“, sagte Kontrollinspektor Horst Reiser, MSc vom C⁴. „Die Teilnehmer haben sich mit Vertretern von Hersteller- und Entwicklungsfirmen im Bereich der Datenforensik-Software austauschen können, deren Produkte in unterschiedlichen Ressorts und Dienststellen verwendet werden. Wir haben Probleme bei der Beweissicherung und Analyse von digitalen Beweismitteln erörtern können. Das positive Feedback der Teilnehmer und Aussteller hat uns gezeigt, dass großes Interesse an einer weiteren Veranstaltung im nächsten Jahr besteht.“ A. S.