AHA – Digitale Forensik

In der digitalen Forensik werden – wie der Name besagt – digitale Spuren und Beweise gesammelt und analysiert, um eine Straftat nachzuvollziehen. Theoretisch kann jede Straftat digitale Spuren hinterlassen. Hatte der Einbrecher auf seinem Smartphone sein Ziel auf Google Maps gesucht? Hatte der Mörder seinem Opfer vorher über E-Mail gedroht? Oder fand gar die Straftat selbst online statt z.B. bei einem Finanzbetrug? Verschickte und erhaltene Nachrichten werden auf Clouds gespeichert, hochgeladene Fotos können Ortsdaten enthalten, wenn das GPS eingeschaltet war, und der Weg eines Smartphones könnte anhand der kontaktierten Funkzellen nachvollziehbar sein.

Damit digitale Beweise vor Gericht standhalten, muss – wie in anderen Bereichen der Forensik – der gesamte Prozess der Sicherung und Analyse der Beweismittel lückenlos dokumentiert werden.

Wie geht man vor?

Geräte sicherstellen: Am Tatort werden alle digitalen Geräte wie Festplatten, Memory Sticks, Mobiltelefone, Scanner, Überwachungskameras etc. sichergestellt und soweit möglich die Passwörter von den involvierten Personen geholt. Denn, anders als häufig im Kino gezeigt, kann das Knacken von Passwörtern sehr langwierig sein. Mobiltelefone werden sofort ausgeschaltet, in eine Faraday-Tasche gesteckt oder auf Flugmodus gestellt, damit keine Verbindung zum Netzwerk aufgebaut wird, über das die vorhandenen Daten verändert werden könnten. Computermonitore werden fotografiert, um den aktuellen Stand zu sichern. Eine wichtige Entscheidung, die sofort gefällt werden muss, ist, ob der Computer eingeschaltet bleibt oder nicht. Bleibt er an, kann man aktuell laufende kriminelle Aktivität verfolgen. So gefährdet man auch nicht den späteren Zugriff auf die Daten wegen einer Festplattenverschlüsselung. Schaltet man den Computer aus, kann man unterbinden, dass Daten gelöscht werden.

Daten analysieren: Die digitalen Daten werden auf einen neuen Datenträger übertragen, damit das Original nicht aus Versehen beschädigt wird und damit keine «Datenkontamination» stattfindet. Ein so genannter Write Blocker kann sicherstellen, dass dabei die Daten nicht verändert werden können. Mit Spezialsoftware kann auch auf versteckte und teilweise gelöschte Daten zugegriffen werden. Ausserdem werden Informationen aus dem Internet gesammelt, z. B. Chats, besuchte Websites oder E-Mails, sodass die kriminellen Aktivitäten nachvollzogen werden. Möglicherweise müssen externe Spezialisten die Analyse durchführen, da sie detailliertes Wissen und Programmierkenntnisse erfordert. Nach der Sicherung der Daten werden die Geräte auf DNA, Fingerabdrücke und weitere Spuren untersucht.

Impressum
Schweizerische Akademie der Technischen Wissenschaften
www.satw.ch
Januar 2019