

Buchkritiken

10.04.2024

IT-Forensik kurz & einfach: Wie Sie digitale Spuren sichern oder beseitigen, Daten verschlüsseln und Straftaten aufdecken¹ von Daniel Liersch ASIN: B07J57F98C

Es wurde die Kindle-Ausgabe gelesen. Es ist schnell zu lesen und verständlich als IT-Experte.

Erst wird ihnen erklärt wie sie ein Festplatten-Image erstellen und Dateien durchsuchen. Und dann Berichte schreiben. Dann wird erwähnt das die Datei bombenbau.txt kriminell sein. Das ist es aber nicht. Das ist eher Niveau Kreispolizei und gerichtlich null auswertbar. Wir lachen alle. Stink normales IT-Grundwissen. Grundgesetz. Es ist erstmal nur ein Text und somit Kunst und Wissenschaft.

Was eher interessant ist sind bestimmte Inhalte (aber nicht Wasserstoffperoxid) mit einer bestimmten Informationsdichte die auf eine Straftat (also an einer Sache oder Handlung) konkret hindeuten. Oder offene Daten wie Führerschein, standamtliche Daten oder richtige Belege.

Zudem muss auch hier die Umgebung versiegelt sein. Eine Datei zu kopieren ist noch schneller gemacht als draußen. Es gibt zahlreiche Zugänge. Direkt (zum Beispiel per USB-Stick oder lokales LAN) und remote (SSH, SFTP) diese müssen versiegelt sein.

HASH-Werte Vergleiche müssten vorher nachher Zustände gemacht werden und da wird es schon kritisch.

Heiko Wolf, mail@heikowolf.info, FDL 1.3, Stand: 11.04.2024, heikowolf.info, OCRID: 0000-0003-3089-3076

¹ https://www.amazon.de/Forensik-kurz-einfach-beseitigen-verschl%C3%BCsseln-ebook/dp/B07J57F98C/ref=cm_cr_srp_d_product_top?ie=UTF8, abgerufen am 10.04.2024