LAYER 8

Ihre Schnittstelle zwischen IT und Recht.

LAYER 8 GmbH
Zentralstrasse 20
Postfach 1343
CH-6031 Ebikon/Luzern

+41 41 511 5008
contact[at]layer-8.law
https://layer-8.law

Forensic Readiness Grundlagen (Teil 1)

Vorbereitung auf forensische Untersuchungen – Grundlagen

> *"Forensic Readiness" has two objectives:*
>
> 1. *Maximizing an environment's ability to collect credible digital evidence, and;*
> 2. *Minimizing the cost of forensics in an incident response.*
>
> *John Tan, Forensic Readiness, 2001*

Rechtsanwalt Roman Kost, MLaw, CAS Informationssicherheit

Digitale Forensik bezweckt die rechtsgenügliche Gewinnung von Beweisen; Forensic Readiness bedeutet, diese Beweisgewinnung auch praktisch durchführen zu können. In diesem ersten Teil des Beitrags werden die Grundlagen gelegt: Es werden die Standards ISO 27037:2012 und ISO 27043:2015, die bislang wenig Erwähnung in der einschlägigen Literatur gefunden haben. Sodann wird die Bedeutung der Schweizer Strafprozessordnung bei der Beweisgewinnung und die Anschliessende Verwertung in einem Zivilprozess beleuchtet, die zentralen computerforensischen Prinzipien (Akzeptanz der Methoden, Wahrung der Integrität, Dokumentation) und das SAP Modell (Secure, Analye, Present) dargelegt. Der separate zweite Teil des Beitrags (organisatorische und technische Massnahmen) baut auf diese Grundlagen auf.

Digital Forensics, Forensic Readiness, Informationssicherheit, Strafprozess, Zivilprozess

[v. 2023-02-02]

Inhaltsverzeichnis

1. Abstract

[1] Digitale Forensik bezweckt die rechtsgenügliche Gewinnung von Beweisen. Hält man die Vorgaben der Strafprozessordnung ein, genügen derart gewonnene Beweis auch in zivilrechtlichen Verfahren. In diesem ersten Teil des Beitrags werden die Grundlagen gelegt:

[2] Mit ISO 27037:2012 und ISO 27043:2015 existieren Standards, die organisatorische Vorgaben machen. Sie enthalten die Grundprinzipien, denen digital-forensische Beweissicherung entsprechen sollte. Beides Standards finden bislang wenig Erwähnung in der einschlägigen Literatur.

[3] Die schweizerische Strafprozessordnung verpflichtet mit Art. 139 Abs. 1 StPO zur Einhaltung des Stands von Wissenschaft und Erfahrung. Was Stand von Wissenschaft und Erfahrung ist, definieren Expertinnen und Experten der Computerforensik, auf die sich die Gerichte abstützen. Einheitliche Standards, die technische Methoden vorgeben, existieren bis dato nicht. Diese Aufgabe der Forensik bleibt weiterhin offen.

[4] Die Forensik hat zentrale Prinzipien aufgestellt: Die *Akzeptanz* der angewandten Methoden bei der digital-forensischen Beweissicherung; die Wahrung der *Integrität* des originalen Beweismittels und der davon erstellten Sicherungen während sämtlicher Stadien eines Prozesses sowie die *Dokumentation* sämtlicher Beweisgewinnungshandlungen inkl. Zugriffskontrolle, Lagerung und Vernichtung. Die Forensikexpertin oder der Forensikexperte folgen dabei grundsätzlich dem SAP-Modell: Secure – Analye – Present.

[5] Um die digital-forensische Beweisgewinnung zu unterstützen, werden im Rahmen der Forensic Readiness-Massnahmen organisatorischer und technischer Natur ergriffen. Auf diese Massnahmen geht der zweite Teil dieses Beitrags ein (Forensic Readiness - Teil II).

[6] Die technischen Massnahmen unterliegen einem stetigen Wandel, weshalb konkrete Produktvorschläge nicht sinnvoll sind. Zur grundlegenden Funktionalität der technischen Massnahmen gehört aber in jedem Fall das Dokumentieren von Vorgängen, was häufig durch die Implementation von Netzwerk und/oder Host Based Intrusion Detection Systemen erfolgt, mit denen eine Vielzahl von Daten und Metadaten erfasst werden.

2. Grundlagen

[7] "Forensic Readiness" bezeichnet den Einsatzzustand einer Organisationseinheit[1] in Bezug auf die Sicherung von digitalen Beweisen bei einem Vorfall. TAN, dem man die Erfindung dieses Begriffs zuschreibt, fügt noch eine finanzielle Komponente hinzu: Forensic Readiness soll die Kosten bei einem Ereignis (Incidence Response) minimieren und zugleich die Fähigkeit steigern, verwertbare Beweise zu sichern.[2] Das effektive Sichern von digitalen Beweisen fällt dagegen unter den Begriff "Digital Forensic".

[8] Der **Begriff Forensik** für sich alleine genommen umfasst Handlungen, die im Hinblick auf ein Gerichtsverfahren vorgenommen werden. Wer forensisch tätig ist, tritt in irgendeiner Form vor einem Forum auf

[1] Bei den Organisationseinheiten kann es sich zum Beispiel um eine Verwaltungseinheit wie ein Departement oder ein Korps handeln, wie auch um ein Unternehmen (von der Einzelunternehmung bis zur Aktiengesellschaft).

[2] TAN, Abstract, S.1.

(lat. forensis = „zum Forum, Marktplatz gehörig“).[3] Forensik im Kontext der Informationssicherheit und des Risikomanagements bedeutet das gerichtlich verwertbare Sammeln von digitalen Beweisen, um damit einen Vorfall oder eine Täterschaft belegen zu können.

[9] Seit dem Jahr 2012 gibt es den **ISO-Standard 27037:2012**[4], mit dem spezifische Richtlinien für die Behandlung von potentiellem digitalem Beweismaterial aufgestellt wurden. Der Standard unterteilt diese Behandlung von digitalem Beweismaterial in vier Schritte[5]: Identifikation (identification), Sammlung (collection), Akquise (acquisition) und Sicherung (preservation). Zu jedem dieser Schritte bietet ISO 27037:2012 im Sinne des aktuellen Stands der Technik Handlungsanweisungen an. Seit dem Jahr 2015 besteht mit **ISO-Standard 27043:2015** ausserdem eine Norm, die sich explizit mit Forensic Readiness auseinandersetzt. Behandelt werden darin sämtliche organisatorischen Abläufe zur Implementation eines angemessenen Forensic Readiness-Niveaus. Seit dem Jahr 2002 gibt es ein beachtliches RFC ("Request for Comments") unter der Nummer RFC 3227, worin sich die "Internet Best Current Practices" finden mit wertvollen Anweisungen zur Beweisgewinnung und -archivierung.

[10] Es erstaunt, dass in der beigezogenen Literatur die ISO-Standards 27037:2012 und 27043:2015 gänzlich fehlen.[6]

[11] Zwar enthält ISO 27037:2012 keine direkten Vorgaben zur Umsetzung resp. zum Erreichen von Forensic Readiness. Korrektes digital-forensisches Vorgehen ist im Unterschied zur Readiness nicht ein proaktiver, sondern ein reaktiver Prozess. Wer aber versteht, wie im Ernstfall vorzugehen wäre, kann die notwendigen Vorbereitungen treffen, um ein adäquates Mass an forensischer Bereitschaft oder eben Forensic Readiness zu erzielen.

[12] ISO 27037:2012 äussert sich nicht zu den zusätzlichen Schritten Schutz (protect) und Analyse (analyze) des digitalen Beweismaterials, wie sie bei der Forensic Readiness vorkommen. Diese beiden Schritte werden in ISO 27043:2015[7] als Phasen der Schritte Acquisitive Processes (Kap. 9) und Investigative Processes (Kap. 10) dargestellt.

[13] Der Schutz der digitalen Beweise ('Protect') für sich genommen ist **ein ständiger, sich aktualisierender Prozess**, da sich die Bedrohungslage ständig ändert. Hierfür ist ein auf die Bedürfnisse zugeschnittenes Risikomanagement resp. Informationssicherheitsmanagement notwendig. Ähnliches gilt für den Schritt 'Analyse': Die Analyse richtet sich nach dem einschlägigen gesetzlichen Rahmen und dem Zielpublikum. Auch hier wären konkrete technische Vorgaben in einem Standard wenig sinnvoll, schliesslich lässt sich nicht per se eine Analysesoftware empfehlen und genau so wenig

[3] http://www.duden.de/rechtschreibung/forensisch

[4] ISO 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

[5] Definitionen aus ISO 27037:2012 (Ziffernangabe in Klammern): **identification** (3.12 und 5.4.2): process involving the search for, recognition and documentation of potential digital evidence; **collection** (3.3 und 5.4.3): process of gathering the physical items that contain potential digital evidence; **acquisition** (3.1 und 5.4.4): process of creating a copy of data within a defined set; **preservation** (3.15 und 5.4.5): process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.

[6] Es wurde zugegebener Massen nicht völlig erschöpfend recherchiert und jeder Artikel im Bereich der Forensik konsultiert. Die zentralen Quellen aber wurden erfasst. Auch eine einschlägige Dissertation Ende 2017, siehe KONSTANTIN SACK. hat weder ISO 27037:2012 noch ISO 27043:2015 erfasst. In der hiesigen Forensikszene scheinen diese ISO-Standards ebenfalls nicht breite Bekanntheit zu geniessen.

[7] Das grobe Zusammenspiel der verschiedenen Standards ISO 27037 (sowie 27038, 27040, 27041 und 27042) mit ISO 27043 wird in 27043:2015, Introduction – Relationship to other standards, ab Seite VI beschrieben.

sagen, welche Bestandteile der digitalen Beweise denn nun notwendigerweise analysiert und aufbereitet werden müssen.

[14] Exakte Handlungsanweisungen darf man von den beiden Standards ISO 27037:2012 und 27043:2015 deshalb nicht erwarten. Dafür sind diese Standards nicht da.

3. Der gesetzliche Kontext des digitalen Beweises in der Schweiz

[15] Spricht man von **Beweisen**, so wird implizit ein rechtlicher Kontext mitgedacht, in dem diese Beweise ihre Wirkung entfalten sollen. ISO 27037:2012 hält dementsprechend fest, dass die Implementation dieses Standards sich nach den jeweiligen gesetzlichen Gegebenheiten zu richten hat.[8]

[16] In der Schweiz handelt es sich bei diesem rechtlichen Kontext im Wesentlichen um zwei Prozessordnungen: die Zivilprozessordnung (ZPO) und die Strafprozessordnung (StPO); beides sind Bundesgesetze und gelten schweizweit. Diese Gesetze regeln die Tätigkeit von Privaten, Gerichten und Strafverfolgungsbehörden innerhalb eines hängigen Prozesses.[9]

[17] Die **Beweisvorschriften** der Strafprozessordnung sind „schärfer“ als jene der Zivilprozessordnung. Das Zivilverfahren ist grundsätzlich von den Behauptungen der streitenden Parteien geprägt, wohingegen im Strafverfahren in erster Linie die beschuldigte Person[10] beurteilt wird. Diese Beurteilung resp. die Sammlung von Beweisen auf dem Weg zu Beurteilung erfolgt hoheitlich durch die Polizeien, Staatsanwaltschaften und Gerichte.

[18] Die Strafprozessordnung soll für einen fairen und korrekten Prozess, letztlich also für einen gewissen Machtausgleich zwischen dem übermächtigen Staat und einer einzelnen beschuldigten Person sorgen. Faire Verfahren sind zentral dafür, dass der Strafanspruch und die Autorität des Staats von den Rechtsunterworfenen, also dem Volk, akzeptiert wird. Faire Verfahren sorgen für Rechtssicherheit.

[19] Stellt man also für die digitale Forensik oder die Forensic Readiness auf die Voraussetzungen der Strafprozessordnung ab, genügt man automatisch auch den zivilprozessualen Anforderungen.[11] Gilt die Täterschaft unter der Herrschaft des Strafprozessrechts als überführt, dann ha das entsprechende Beweisergebnis grundsätzlich auch bei zivilrechtlichen Konflikten Bestand.

---

[8] Ziff. ISO 27037:2012, S. IV, Introduction, 6. Absatz und entsprechende Hinweise verteilt im ganzen Standard; Explizit in ISO 27043:2015, Ziff. 5.2. Legal principles.

[9] Die Unterscheidung, ob man sich in einem Prozess befindet oder nicht, ist zentral. Unter Prozess versteht man ein Verfahren, das am Ende zu einem hoheitlichen Entscheid führt. Befindet man sich in einem Prozess, dann sind die entsprechenden prozessualen Regeln strikte einzuhalten. Befindet man sich *nicht* in einem Prozess, z.B. bei Vertragsverhandlungen unter privaten Subjekten, die sich rechtlich auf Augenhöhe befinden, gibt es keine zwingenden Vorschriften, die vorgeben, was man zu tun oder zu lassen hat. Vorbehalten natürlich, man überschreitet nicht die Grenzen des Strafrechts.

[10] Und nicht etwa das Opfer. Strafprozessrecht ist nicht Opferrecht (dafür existiert das Opferhilfegesetz). Im Strafprozess geht es einzig um die Verfolgung einer mutmasslichen Täterschaft; Opferinteressen wie Genugtuung und Schadenersatz fliessen „nur“ adhäsionsweise, als quasi ans Verfahren angehängt, mit ein.

[11] Nun könnte man annehmen, man würde dadurch mehr als das Notwendig tun. Dem ist nicht so. Der versierte Gegner in einem Zivilprozess kann dieselben Argumente wie in einem Strafprozess vortragen (z.B. Unverwertbarkeit wegen technischer Fehler oder zerstörter Beweiskette). Er muss diese Argumente aber aus eigenen Stücken vortragen (Dispositionsmaxime), da die Zivilgerichte regelmässig keinen Untersuchungs-maximen unterliegen. Zivilgerichte untersuchen den Sachverhalt also nicht selber, sondern beurteilen nur, was die Parteien vorbringen und ob das erwiesen ist. Gerichte klären in Zivilprozessen grundsätzlich nichts selber ab.

[20] Für die digitale Forensik oder die Forensic Readiness gilt dem Gesagten nach die **Strafprozessordnung als Grundlage** für die Sicherung von Beweisen.

[21] Gelegentlich findet man Hinweise auf andere Gesetze wie z.B. das Datenschutzgesetz (DSG). Blickt man auf die Schutzrichtung und den Zweck des Datenschutzgesetzes, so wird klar, dass das Datenschutzgesetz nur am Rande mitspielt.

[22] Das Datenschutzgesetz bezweckt *„den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden“* (Art. 1 DSG). Das Datenschutzgesetz selber schränkt seinen Anwendungsbereich ein und deklariert sich mit Art. 2 Abs. 2 lit. c DSG als nicht anwendbar auf *hängige* Zivil- und Strafverfahren. Läuft also ein Verfahren, so kommt das Datenschutzgesetz nicht zur Anwendung und die Persönlichkeit der betroffenen Personen wird ausschliesslich durch das entsprechende Prozessrecht geschützt.

[23] Was aber, wenn noch keine Anzeige erstattet oder ein Prozess angehoben wurde? Dann ist das Datenschutzgesetz anwendbar. In dieser Situation muss unterschieden werden, ob die Beweiserhebungsmethoden sich ausschliesslich gegen die Täterschaft richten oder auch unbeteiligte Dritte betroffen sind.

[24] Nach Art. 4 DSG dürfen Personendaten nur rechtmässig und verhältnismässig (Abs. 1), nach Treu und Glauben (Abs. 2), nach angegebenem, ersichtlichem gesetzlich vorgegebenem oder erkennbarem Zweck bearbeitet (Abs. 3 und 4) werden. Bei Persönlichkeitsprofilen muss gar ausdrücklich eingewilligt werden (Abs. 5).

[25] Datenschutz ist aber nicht Täterschutz, wie häufig vorgebracht wird. Art. 4 Abs. 2 DSG enthält eine Verhältnismässigkeitsprüfung, was für das Schweizer Privatrecht an sich äusserst ungewöhnlich ist. In Fällen, wo durch digitale Forensik oder Forensic Readiness Personendaten von Tätern bearbeitet werden, hat sich die Täterschaft im Rahmen der Verhältnismässigkeitsprüfung starke Abstriche anrechnen zu lassen. Wer gegen Verbotsnormen oder vertragliche Verpflichtungen verstösst, hat sich grössere Eingriffe in die eigene Persönlichkeit gefallen zu lassen. Die Täterschaft kann sich nur in sehr beschränktem Ausmass auf den Schutz der Persönlichkeit berufen; sie hat in diesem Sinne selber durch ihr Tun über ihre Persönlichkeit disponiert. Ohnehin dürfte in aller Regel ein überwiegendes Interesse der überwachenden Organisationseinheit vorliegen, womit der Eingriff in die Persönlichkeit im Sinne von Art. 13 Abs. 2 DSG gerechtfertigt ist.

[26] Um aber datenschutzrechtliche Fallstricke zu entschärfen, empfiehlt es sich, bei den Benutzern der IT-Infrastruktur das Einverständnis zu holen. Das geschieht am besten schriftlich und unter vollständiger Aufklärung darüber, in welchem Ausmass die Benutzung der IT-Infrastruktur überwacht wird (Art. 13 Abs. 1 DSG).

[27] Zurück zur Strafprozessordnung: Enthält die Strafprozessordnung konkrete Vorgaben zur Computerforensik? Nein. Und das ist richtig so. Hätte der Gesetzgeber starre Vorgaben erlassen, wären ständige Gesetzesrevisionen die Folge und man würde stets der Technik hinterherhinken.

[28] Die Strafprozessordnung sieht in **Art. 139 Abs. 1 StPO** wörtlich vor, dass die Strafbehörden zur Wahrheitsfindung alle **nach dem Stand von Wissenschaft und Erfahrung** geeigneten Beweismittel, die rechtlich zulässig sind, einsetzen. Die Computerforensik und die

Arbeit aller Beteiligten hat sich also am Stand der Wissenschaft zu orientieren und diesen einzuhalten.[12]

[29] Der Umstand, dass das Gesetz selber keine Antwort darüber enthält, was im Rahmen der Computerforensik als korrekt gilt und was nicht, führt dazu, dass Expertenwissen notwendig wird.[13] Wie HEINSON festhält, "*existiert [bislang] keine anerkannte einheitliche Methode für die Beweissicherung und Beweisverwertung mit IT-Forensik*"[14]; dabei handelt es sich um eine offene Aufgabe der Fachwelt.[15]

[30] Die Expertinnen und Experten müssen wissen, was dem Stand von Wissenschaft und Erfahrung im Zeitpunkt der Beurteilung der digitalen Beweise entspricht. Die Gerichte werden darauf abstellen.

4. Grundprinzipien der Digital Forensic

[31] Die Computerforensik wird eingesetzt, um die kriminalistischen „W"-Fragen zu klären: Wer? Was? Wo? Wann? Warum? Womit? Wie?[16]

[32] Die einschlägige Literatur hebt folgende drei Grundsätze hervor, damit der erhobene Beweis als authentisch gilt[17]:

1. Akzeptanz[18]:
   Sämtliche Methoden, die bei einer digital-forensischen Untersuchung zum Einsatz kommen, müssen "*in der Fachwelt beschrieben und allgemein akzeptiert sein*"[19]. Sie haben also dem Stand der Wissenschaft zu entsprechen. Abweichungen von dieser Methodik sollten vermieden werden. Sind Abweichungen unumgänglich, müssen sie eingehend begründet und die Abweichungen im Einzelnen aufgezeigt werden. Die Wiederholbarkeit muss in jedem Fall gewährleistet sein. Sind die angewandten Methoden akzeptiert, sind sie auch glaubwürdig: Deren Benutzung hat sich bewährt und der kritischen Prüfung durch die Fachgemeinde standgehalten. Akzeptanz in der computerforensischen Fachwelt bedeutet damit Akzeptanz bei den Gerichten.

2. Integrität[20]:
   Die digitalen Spuren (insbesondere die originalen Datenträger) dürfen durch die Untersuchung nicht verändert werden. Sind Veränderungen nicht vermeidbar, was sehr selten je der Fall ist, muss die Vorgehensweise exakt dokumentiert werden. In solchen Fällen bedarf es zwingend einer Begründung, weshalb die Untersuchung nicht ohne Veränderung des Datenträgers möglich war. Die Integrität der gesicherten Datenträger muss jederzeit belegt werden können.

[12] Bei Abweichungen von diesem Stand der Wissenschaft bedeutet das noch nicht gleich, dass der Beweis keine Beweiskraft mehr hätte oder unverwertbar wird. In solchen Fällen steigt der Aufwand, das Abweichen vom Stand der Wissenschaft zu rechtfertigen, aber enorm. In der Schweizer Strafrechtspflege kommt dann häufig eine Interessenabwägung zum Zug, bei der die Verletzung von Vorgaben gegen die Interessen der beschuldigten Person abgewogen werden.

[13] Das ist nicht nur in der Computerforensik so, vielmehr in allen Lebensgebieten. Gutachten sind in der Medizin, dem Bauwesen, im Patentwesen etc. gang und gäbe.

[14] HEINSON, S. 407.

[15] HEINSON, S. 409 f.

[16] So wörtlich BANGERTER, S. 267, der sich auf das BSI, S. 22 und 23. RYSER, S. 556; GESCHONNECK, S. 65. Solche W-Fragen findet man in sehr vielen Gebieten, so auch bei den Juristen in Bezug auf Vertragsverhältnisse.

[17] Vgl. BANGERTER, S. 266; vgl. BSI, S. 23.

[18] DEWALD, Diss., S. 14 f; GESCHONNECK, S. 63 nennt die Prinzipien von Glaubwürdigkeit und Akzeptanz getrennt. Bangerter stützt sich direkt auf GESCHONNECK ab.

[19] GESCHONNECK, a.a.O.

[20] GESCHONNECK, S. 64, der als weiteres separates Prinzip die Wiederholbarkeit anführt, was am Ende jedoch Teilgehalt der Integrität ist; ebenso DOLLE, S. 184, der mit 5 Grundprinzipien hier seinem Berufskollegen GESCHONNECK, a.a.O., folgt; RYSER, S. 581.

Werden die digitalforensischen Ermittlungsergebnisse angezweifelt, so muss die Beweisführung von Dritten jederzeit wiederholt und bestätigt werden können. Vorausgesetzt für diese Wiederholung ist die Integrität des Ausgangsmaterials.

3. Dokumentation[21]:
   Jeder Schritt des Ermittlungsprozesses, also der digitalforensischen Arbeit, ist angemessen zu dokumentieren[22]. Die Aufbereitung- und Dokumentationsmethoden sind so zu wählen, dass nachvollziehbar Schlussfolgerungen vom Beweis auf zu prüfende Tatsachen möglich sind. Ebenso gehört zur Dokumentation, dass nachweisbar ist, wann die digitalen Beweise sich wo unter welcher Herrschaft befunden haben und namentlich, wer wann darauf zugegriffen hat.

[33] Auf der Basis dieser drei Grundsätze – Akzeptanz, Integrität und Dokumentation – ergibt sich wie erwähnt die Authentizität eines digitalforensischen Beweises. Authentizität wiederum verspricht eine lückenlose Chain of Evidence sowie eine lückenlose Chain of Custody. Beides ist wesentlich, um in einem Prozess als Beweis überhaupt erst Wirkung entfalten zu können; das kann über Sieg oder Niederlage, über Verurteilung oder Freispruch entscheiden.

[34] Die **Chain of Evidence**[23] ist zu Deutsch die Beweiskette. Der erhobene Beweis hat vorab ganz grundsätzlich dazu geeignet zu sein, das zu beweisen, was überhaupt zu beweisen ist. Sodann muss ein Beweis, der zwei bereits erwiesene Elemente in Zusammenhang bringt, sie also verknüpft, ebenfalls geeignet und mit den anerkannten Methoden der Forensik erbracht worden sein. Nur so entsteht eine Kette an Beweisen.

[35] Die Chain of Custody[24] ist auch im Deutschen ein stehender Begriff. Darunter wird die Verantwortungshierarchie oder Verantwortungskette verstanden: Der Forensiker zeichnet sich für die Beweissicherung zuständig, danach werden die Beweisgegenstände eingelagert und im Anschluss dem Gericht zugestellt oder zur Verfügung gehalten. Wer wie auf die Beweise während eines Prozesses zugreift, muss jederzeit nachweisbar sein.

[21] GESCHONNECK, S. 64 führt noch separat das Prinzip "Ursache und Auswirkung" an. Dass die gewählten Methoden am Ende dazu dienen müssen, eine Täterschaft nachzuweisen oder einen relevanten Sachverhalt zu belegen, versteht sich von selbst. Die gewonnen Resultate sinnvoll und für Gerichtspersonen zugänglich zu machen, ist eher eine Frage der Dokumentation.

[22] RFC 3227, Ziff. 3.2, Aufzählungsstrich 8 sowie Ziff. 4; Dieser Punkt wird besonders oft, wenn nicht sogar in fast jedem Fall in irgendeiner Art verletzt. Es ist z.B. ungenügend, einfach einen Rapportausdruck aus X-Wayforensics oder aus enCase in die Akten zu legen. Von der Beschlagnahme eines Datenträgers oder eines Geräts bis hin zur Einlagerung in der Asservatenkammer müssen sämtliche Schritte dokumentiert und einer Person zugeordnet werden können.

[23] Vgl. BANGERTER, S. 266 f.; ausführlich GESCHONNEK, 66 ff. und mit sehr guter Heranführung SACK, S. 49 mit dem Begriff "Provenence"; EE-MASON/SHELDON/DIRES, Rz 9.34.

[24] RFC 3227, Ziff. 4.1; ISO 27037:2012, Ziff. 6.1 vgl. auch BANGERTER, S. 266 f., RYSER, 556; BSI, 22 und 31; ausführlich GESCHONNEK, 66 ff. und erneut mit sehr guter Heranführung SACK, S. 45 f. und S. 166; EE-MASON/STANFIELD, Rz 7.9

[36] Die Chain of Custody gilt auch für die Phase *während* des Gerichtsprozesses und nicht bloss im Vorverfahren, in dem die Verfahrensherrschaft bei einer Staatsanwaltschaft liegt. Auch nachdem die Verfahrensherrschaft von den Untersuchungsbehörden an die Judikative übergegangen ist, muss unbestrittener Massen klar sein, wo die Datensätze liegen, wer darauf Zugriff hat und für die Sicherheit verantwortlich ist.[25]

2.1 Order of Volatility

When collecting evidence you should proceed from the volatile to the less volatile. Here is an example order of volatility for a typical system.

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

RFC 3227, Ziff. 2.1, February 2002

5. Grundsätzliches Vorgehen einer digitalforensischen Untersuchung

[37] Das ganz grundsätzliche Vorgehen bei einer digitalforensischen Untersuchung lässt sich auf drei Buchstaben komprimieren: SAP. **SAP** steht in diesem Kontext für **Secure, Analyze und Present**.[26]

[38] In der **ersten und heikelsten Phase**, der **Sicherungsphase**, werden die Daten ab dem Beweisstück gesichert.[27] Der Forensiker hat unter Wahrung der Integrität mit akzeptierten Methoden die relevanten Daten zu sichern.

[39] In der Sicherungsphase folgen die Forensiker einer Sicherungsreihenfolge, der sog. Order of Volatility, die im bereits erwähnten RFC 3227 niedergeschrieben ist:

[40] Flüchtige Datenbestände (RAM etc.) sind sehr viel aufwändiger zu sichern. An dieser Stelle wird auf weitere Ausführungen dazu verzichtet. In der hiesigen Prozesspraxis hat dieses Thema kaum Gewicht und die Sicherungsmethoden müssen noch als experimentell bezeichnet werden. [28]

[25] Gerade bei diesem zentralen Punkt habe ich in einem Praxisfall Verstösse erlebt: Eine Staatsanwaltschaft hat in Eigenregie, d.h. ohne gerichtliche Verfügung, eine "Zusatzanalyse" durch die Sachbearbeiter der Polizei durchführen lassen, obschon die Verfahrenshoheit beim oberen kantonalen Gericht lag.

[26] BANGERTER, S. 266; GESCHONNECK, S. 68; MARSCHALL, S. 98; DOLLE, S. 184.

[27] GESCHONNECK, S. 67; vgl. BSI S. 24; vgl. RYSER, S. 589; Für eine eingehende Darstellung der Forensik von sog. "Dead Disks", also nicht-volatilen Datenträgern, siehe das Werk von NIKKEL.

[28] Interessierte können folgende Quellen konsultieren: Vgl. BLOCK/DEWALD, Heap, S. 66, die der Forensik von flüchtigen Speichern aus technischer Sicht einen sehr hohen Stellenwert beimessen. Für Memory-Forensik von Windowsbetriebssystemen sei auf BLOCK/DEWALD, Windows, S. 3 ff. hingewiesen. ISO 27037:2012 enthält an verschiedenen Stellen Handlungshinweise in Bezug auf volatile Speichermedien.

[41] Bei nicht flüchtigen Datenbeständen (Festplatten, Sticks etc.) wird vom Beweisstück eine bitgenaue 1:1 Kopie erstellt, wobei ein Schreibschutz (ein sog. Write Blocker, wie sie z.B. von Guidance Software unter dem Namen Tableau erhältlich sind) benutzt werden muss. Diese Schreibschütze sind zertifiziert und entsprechend teuer.

[42] "Assess It All, Or Lose It All" ist das Motto jeder (computer-)forensischen Untersuchung.[29] Was man nicht sichert, hat man später für die Analyse nicht zur Verfügung. Der Forensiker durchläuft dabei folgende Phasen[30]:

1. potential digital evidence identification process;
2. potential digital evidence collection process;
3. potential digital evidence acquisition (optional);
4. potential digital evidence transportation process, and
5. potential digital evidence storage process.

[43] In der **zweiten Phase**, der **Analysephase** wendet der Forensiker sein Wissen auf den Sachverhalt an. Er sucht im gesicherten Beweismaterial nach relevanten Spuren. Dabei kann er auf eine breite Palette von Werkzeugen zurückgreifen. Quelloffene Toolkits sind hier besonders wertvoll, da der zugrunde liegende Code einsehbar ist.[31]

[44] In der **dritten Phase**, der **Present-Phase,** erstellt der Forensiker seinen Bericht.[32] Er wird sich dabei auf automatisch generierte Rapporte abstützen, die er von der eingesetzten Software erhält. Das alleine genügt aber nicht: Die Polizeikorps erstellen regelmässig zusätzliche Polizeirapporte, die die Vorgehensweise und die daraus abgeleiteten Erkenntnisse darstellen. Mit der Unterschrift unter diesen Rapport erhält das Dokument ein zusätzliches und nicht zu unterschätzendes Gewicht. Der vereidigte Polizist bezeugt mit seiner Unterschrift die Richtigkeit seiner Untersuchungsergebnisse.[33] Die Present-Phase kann auch die effektive Präsentation der Ergebnisse vor der fallführenden Staatsanwältin oder dem Gericht umfassen.

6. Abschliessende Gedanken zu den Grundlagen der Forensic Readiness (Teil I)

[45] Die dargelegten Prinzipien, Modelle und Standards haben sich in der Praxis als solide erwiesen. Es braucht aber noch einiges an Zeit, bis diese Grundsätze auch in der juristischen Zunft und insbesondere in der Prozesspraxis der Gerichte ihren Niederschlag finden. Zu sehr verlassen sich Entscheidungsgremien wie Gerichte auf verwaltungsinterne "Spezialisten", denen es manchmal aber an der einschlägigen Ausbildung fehlt.

[46] Für beschuldigte Personen (z.B. in einem Strafverfahren) oder zu einer Leistung, einem Tun oder einem Unterlassen verurteilte Personen (z.B. in einem Zivilverfahren) ist es absolut zentral, dass die

[29] DOLLE, S. 184.
[30] ISO 27043:2015, S. 16 mit dem Blick auf Forensic Readiness; weitergehende Ausführungen zu jedem einzelnen Schritt auf den nachfolgenden Seiten a.a.O. und spezifisch mit dem Fokus auf die digitale Forensik: ISO 27037:2012, S. 8 eingehenden Ausführungen zu jedem Schritt a.a.O.
[31] DOLLE, S. 184; Vgl. MARSCHALL, S. 277 und 292; Das Thema Offenlegung von Quellcode bei Quellen-TKÜ-Software (sog. Staatstrojaner) ist insbesondere in Deutschland ein noch heute brennendes Thema. Im 2011 konnte der CCC mit einer selber geschriebenen Software nachweisen, dass sich Staatstrojaner übernehmen und steuern lassen. Illustrativ zu diesem Thema: https://www.ccc.de/de/updates/2011/staatstrojaner (letztmals abgerufen am 02.02.2023).
[32] Vgl. RYSER, S. 582.
[33] Das bedeutet aber nicht automatisch, dass dieser Rapport vollkommen frei von Fehlern ist. Nur durch eine Unterschrift wird etwas Falsches nicht richtiger.

verwendeten Beweise stichhaltig sind und keine Zweifel über deren Gewinnung existieren. Das sorgt für Akzeptanz von Urteilen und im Endeffekt für Rechtsfrieden.

[47] Nicht selten trifft man in der Schweizer Gerichtspraxis noch auf eine Art Urvertrauen in den Staat. Das ist zwar schön, aber kann nicht genügen. Es gibt keine Gründe, warum sich staatliche Stellen nicht an der Einhaltung des Stands von Wissenschaft und Erfahrung messen sollten. Von privaten Akteuren wird das seit jeher verlangt.

Literaturverzeichnis

BANGERTER SIMON — *Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO*, ZStV - Zürcher Studien zum Verfahrensrecht Band/Nr. 176, 2014

BLOCK FRANK / DEWALD ANDREAS — *Linux memory forensics: Dissecting the user space process heap*, Digital Investigation 22 (2017), S. 66 ff.
(zit. BLOCK/DEWALD, Windows, S. …)

BLOCK FRANK / DEWALD ANDREAS — *Windows Memory Forensics: Detecting (Un)Intentionally Hidden Injected Code by Examining Page Table Entries*, Digital Investigation 29 (2019), S. 3 ff. (zit. BLOCK/DEWALD, Windows, S. …)

DOLLE WILHELM — *Computer-Forensik in der Praxis - Mit Open-Source-Werkzeugen die Aufklärung von Computerkriminalität unterstützen*, DuD – Datenschutz und Datensicherheit, 3/2009, S. 183 ff.

GESCHONNECK ALEXANDER — *Computer-Forensik – Computerstraftaten erkennen, ermitteln, aufklären.,* 6. Aufl., 2014

HEINSON DENNIS — *IT-Forensik*, Diss., 2014, Universität Kassel

MASON STEVEN / SENG DANIEL — *Electronic Evidence*, 4. Aufl., 2017,
zit. EE-BEARBEITER, Rz NN.

MARSCHALL KEVIN — *Rechtsverträgliche Gestaltung IT-forensischer Systeme - Eine Untersuchung am Beispiel der Aufdeckung und Beweisbarkeit von Versicherungsbetrug*, Diss., 2019, Universität Kassel

NIKKEL BRUCE — *Practical Forensic imaging - securing Digital evidence with linux tools*, San Francisco, 2016

RYSER DOMINIC — *„Computer Forensics", eine neue Herausforderung für das Strafprozessrecht*, in: Schwarzenegger Christian/ Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 553 ff.
Bemerkung: juristische Ausführungen beziehen sich auf alte ZH-StPO, nicht auf die eidgenössische StPO.

SACK KONSTANTIN — *Selektion in der digitalen Forensik*, Diss., 2017, Technische Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg

SACHOWSKI JASON — *Implementing Digital Forensic Readiness - From Reactive to Proactive Process*, 2. Aufl., Florida 2019

TAN JOHN — *Forensic Readiness*, Cambridge, 2001
elektronisch abrufbar unter:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.480.6094&rep=rep1&type=pdf

Materialienverzeichnis

DSG	Bundesgesetz über den Datenschutz
ISO 27037:2012	ISO 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
ISO/IEC 27043:2015	ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes
OR	Obligationenrecht. Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)
RFC 3227	Guidelines for Evidence Collection and Archiving, https://tools.ietf.org/html/rfc3227, letztmals abgerufen am 02.02.2023
StPO	Schweizerische Strafprozessordnung
ZPO	Schweizerische Zivilprozessordnung

Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
AD	Active Directory, siehe https://de.wikipedia.org/wiki/Active_Directory
Abs.	Absatz
Art.	Artikel
BSI	Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/
CCC	Chaos Computer Club
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSiRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures https://cve.mitre.org/
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSG	Datenschutzgesetz
Diss.	Dissertation
etc.	et cetera
etc. pp.	et cetera perge, perge
f.	folgend
ff.	fortfolgend
GPK	Geschäftsprüfungskommission
HIDS	Host-based Intrusion Detection System
ISO	Internationale Organisation für Normung
lit.	litera
IT	Informationstechnik
MELANI	Melde- und Analysestelle Informationssicherung MELANI https://www.melani.admin.ch
NIDS	Network Intrusion Detection System

NR	Nationalrat
RAM	Random Access Memory
RFC	Request for Comments
Rz	Randziffer
S.	Seite
sog.	sogenannt
StPO	Strafprozessordnung
TKÜ	Telekommunikationsüberwachung
vgl.	vergleiche
Ziff.	Ziffer
z.B.	zum Beispiel
ZPO	Zivilprozessordnung

LAYER 8 GmbH
Zentralstrasse 20
Postfach 1343
CH-6031 Ebikon/Luzern

+41 41 511 5008
contact[at]layer-8.law
https://layer-8.law