HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCE

LEHRBRIEF

für das Modul

Digitale Forensik – Grundlagen

Autoren:

Prof. Dr. Dirk Labudde

Laura Pistorius, B.Sc.

Bearbeitungsstand: 13.04.2024

Inhaltsverzeichnis

1 Digitale Forensik

„Nur wer analoge und digitale Spuren als Einheit begreift und zu deuten versteht,

hat heute eine Chance, Verbrechen aufzuklären.“

-Dirk Labudde

Bei der digitalen Forensik handelt es sich um mehr als die reine Datensicherung, vielmehr geht es auch um die Auswertung von Texten, Bildern, Chats und Videos und anderen informationsgebenden Medien (digitale Daten). Es wird in diesem Modul auf den ganzen Prozess der Entstehung der digitalen Daten, deren Speicherung und forensische Auswertung eingegangen.

Dabei unterscheidet sich die digitale Forensik stark von der Informatik, da die Informatik selbst nicht auf die Spurensuche in einem System ausgelegt ist.

Die analoge Welt und digitale Welt stehen in direktem Zusammenhang und die Spuren der digitalen Welt sind eine 100-prozentige Einlassung in die analoge Welt. Die Kunst besteht darin, die digitalen Spuren auf die analoge Welt zu projizieren und die Zusammenhänge zu offenbaren.

1.1 Einführung

Wissenschaftlichkeit der IT-Forensik

Digitale Daten und digitale Spuren unterscheiden sich augenscheinlich von den analogen Spuren. Trotzdem lassen sich die Spurenarten auch in die digitale Welt übertragen. Das Prinzip der analogen Trugspuren oder fingierten Spuren ist auch hilfreich im digitalen Raum. Allerdings entstehen so bei der Sicherung schnell Unmengen von Daten, die aber nur eine begrenzte Anzahl an Spuren birgt.

Eine Wissenschaft ist geprägt durch wissenschaftliche Methoden und Herangehensweisen. In der Forensik kommen wissenschaftliche Methoden, beispielsweise die Form der Analysen von Spuren sowie die Juristischen Voraussetzungen zusammen. So ist im Gesetz fest vorgeschrieben, wie Viele Minuten bei einem Fingerabdruck zur Identifikation übereinstimmen müssen. Die Forensik muss sich also zwingend auf die Wissenschaft und Justiz berufen. Daher ist die Klassifizierung der Forensik einzig als Wissenschaft schwierig.

1.2 Einführung in die digitale Forensik

Die IT-Forensik bzw. Digitale Forensik ist ein Teilgebiet der Forensik. Die IT-Forensik behandelt die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen und der Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung digitaler Spuren. Demnach gehört die gesamte digitale Welt dazu. [1]

Es existieren viele Definitionen für digitale- oder IT-Forensik. So gibt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) folgende Definition im Leitfaden für IT-Forensik an: „IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“ [2, S. 8]

Mittlerweile ist die Untersuchung von Computersystemen im Sinne einer inhaltlichen Auswertung der dort gespeicherten Informationen auch im Zusammenhang mit herkömmlichen Straftaten, aber auch für Zwecke der Steuerfahndung etabliert. Die digitale Forensik beschäftigt sich mit der gerichtsfesten Sicherung und Verwertung digitaler Spuren. Als forensische Wissenschaft muss die digitale Forensik wissenschaftliche Methoden anwenden und dabei beachten, dass die Beweisführung dazu führen kann, dass Menschen ihrer Freiheit beraubt werden. Nur eine verlässliche und objektive Methodik wird dieser Verantwortung gerecht. Daher muss die Methodik immer wieder neu überdacht werden.

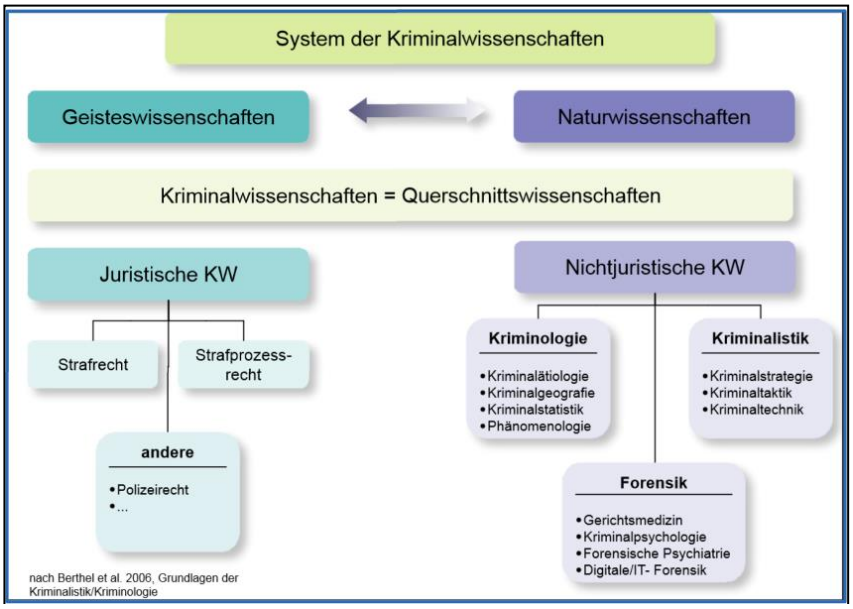


Abbildung 1: Systematische Darstellung und Verortung der Teilgebiete der Kriminalwissenschaften

Die Forensik lässt sich anhand von Abbildung 1 als Kriminalwissenschaft bezeichnen. Dabei befinden wir uns im nichtjuristischen, naturwissenschaftlichen Bereich. Auch die digitale Forensik ist dabei als Teildisziplin der Forensik aufgeführt.

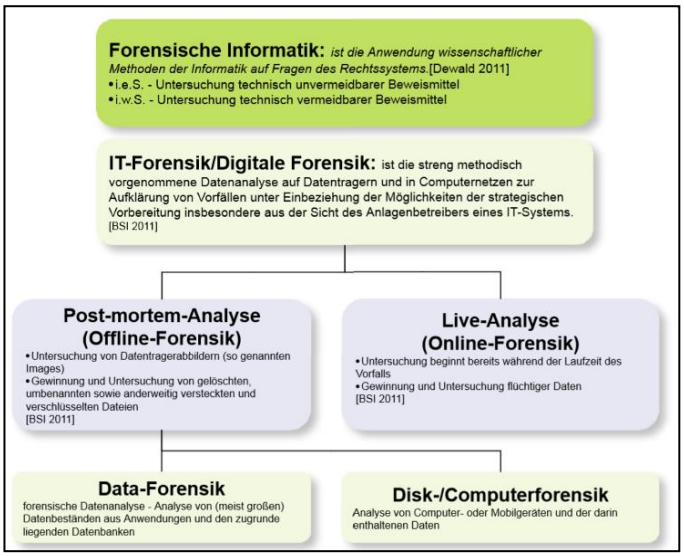


Abbildung 2: Aufteilung der Gebiete der Forensischen Informatik und digitalen Forensik

Um die Wissenschaftlichkeit der Forensik sicherzustellen, muss man sie einordnen. In der Abbildung 2 werden die forensisch relevanten Fachgebiete der Informatik dargestellt. Unterschieden wird hier in forensische Informatik und IT-Forensik. Im Digitalforensik-Bereich unterscheidet man zusätzlich in die Offline- und Online-Forensik. Die Offline-Forensik, oder auch Post-mortem-Analyse genannt, beschäftigt sich mit der Untersuchung von Datenträgerabbildern (Images) nach einem Vorfall. Dabei liegt der Schwerpunkt auf der Gewinnung und Untersuchung von gelöschten, versteckten, verschlüsselten Dateien und anderen digitalen Spuren. Die Online-Forensik, auch Live-Analyse genannt, beschreibt die Untersuchung während der Laufzeit eines Vorfalls, also unmittelbar während des Tatgeschehens. Es liegt ein besonderer Fokus auf der Gewinnung und Untersuchung von flüchtigen Daten, beispielsweise Hauptspeicherinhalten, Netzwerkverbindungen, laufende Prozesse, offene Ports etc. [2]

In der Literatur lassen sich zum Thema der digitalen Forensik diverse Aussagen finden wie beispielsweise:

"...ein pragmatisches technisches Sachverständigenwesen...unter dem Oberbegriff 'Computerforensik' oder 'digitale Forensik…" [3]

"...[es] besteht der wesentliche Unterschied zwischen der klassischen Forensik und der digitalen Forensik in der Natur der Spuren, die in beiden Bereichen untersucht werden." [4]

"Fast alle Prinzipien, die man in der klassischen Forensik für physische Spuren entwickelt hat, lassen sich auch auf digitale Spuren anwenden." [4]

Methoden

Der aus der allgemeinen Forensik bekannte Dreiklang des Suchens, Sicherns und Analysierens funktioniert in der digitalen Forensik nicht komplett, weil die letzten beiden Punkte nicht richtig getrennt werden können. Die hypothesengetriebenen Prozesse beziehen sich auf die Gesamtheit der Ermittlung. Allerdings kommt es während der Ermittlungsarbeit zu neuen Erkenntnissen und das Suchen und Sichern muss als iterativer Prozess erneut passieren. Insofern sind die Prinzipien der allgemeinen Forensik teils auf die digitale Welt anwendbar und jede Erkenntnis muss durch Hypothesen überdacht werden.

Es stehen nach einer Sicherung verschiedenste Daten zur Verfügung (Text/Video/Audio…). Diese Daten erfordern für ihre Auswertung auch verschiedene Werkzeuge. Es kann sich nicht darauf berufen werden, dass die gefundenen und gesicherten Daten vollständig sind. Durch z.B. die verteilte Speicherung von Daten oder versteckte Datenträger kann es immer sein, dass nicht die Gesamtheit aller relevanten Daten gefunden wird. Ein weiteres Problem im Zusammenhang mit der Datensicherung stellt die enorm steigende Datenmenge dar. Dieser Problembereich wird als Big Data bezeichnet. Zur Eindämmung dieses Problems wird die Methode der Datenreduktion eingesetzt. Ansätze wie Data Mining oder Big Data Analytics sollen dabei helfen, riesige Datenmengen auf relevante Daten zu reduzieren oder wichtige Daten schneller zu finden. Da die Menge an Daten weltweit immer weiter und unaufhaltsam steigt, gewinnen diese Methoden immer mehr an Wichtigkeit.

1.2.1 Forensische Informatik

Die Computerforensik (nach Geschonneck [3]) umfasst in ihrer aktuellen Form eine Vielzahl unterschiedlichster Aufgaben, wie beispielsweise die möglichst schnelle Bewertung eines

Sicherheitsvorfalls anhand erster durch Techniken der Live-Analyse [5] erhobener Daten zur Planung der weiteren Untersuchung des Vorfalls. Durch einen einzelnen Computer ohne Anbindung zu anderen oder Netzwerken können in der Regel keine Straftaten begangen werden. Die Anfertigung einer forensischen Kopie physischer Speichermedien unter Einsatz spezieller Hard- und Software und weitere Aufgabenfelder wie die Umgehung von Schutzmechanismen digitaler Systeme, um eine Erhebung von Daten zu ermöglichen, sowie die Extraktion kryptografischer Schlüssel aus Hauptspeicherabbildern, zur Erhebung verschlüsselter Daten sind Aufgaben der forensischen Informatik. Die Rekonstruktion gelöschter Daten anhand von Dateisystem Metadaten oder durch File Carving und die Erstellung von Timelines untersuchter Systeme, also die Erfassung einer zeitlichen Abfolge vergangener Ereignisse auf dem untersuchten System zählen auch zu dem Aufgabenfeld.

Das Ziel ist es, eine Timeline zu erstellen, die den digitalen Tathergang rekonstruiert. Dazu müssen die analoge und digitale Welt auf der Grundlage der sichergestellten Spuren zusammengebracht werden.

Es ist die forensische und kriminalistische Aufgabe, mittels der Rekonstruktion einen digitalen Tathergang darzustellen. Viele Ereignisse erhalten in der digitalen Welt einen Zeitstempel wie beispielsweise das Erstellen oder Ändern von Dateien. Wenn diese Zeitstempel und Daten zusätzlich durch geografische Daten mit Orten in Verbindung gebracht werden können, lässt sich daraus eine komplette Timeline ableiten. Dieser Prozess fällt durch die größere Verfügbarkeit an Informationen eleganter aus als in der analogen Welt. Bei der Erstellung solcher Timelines muss auch auf die Logik geachtet werden. Es muss also die Timeline mit der wahrscheinlichsten Eventabfolge gefunden werden. Über die Zeit verknüpfte Ereignisse sind wahrscheinlicher als andere. Trotzdem sind auch hier Manipulationen und Abweichungen möglich. Wichtig für eine korrekte Timeline ist, dass die relative Zeit Einstellung auf den einzelnen Geräten abgeglichen wird, sodass es zu keinen unterschiedlichen Zeitachsen kommt.

1.2.2 Forensische Prinzipien

Das „Basic Forensic Mindset“ wird durch die Fragen definiert:

1. Wie geht man an forensische Fragestellungen heran?
2. Welche Grundregeln sind zu beachten?
3. Wie gehe ich wissenschaftlich vor? (hypothesengetriebene Prozesse)

Es ist wichtig zu wissen, was man will, um die Wahrheit herausfinden. Das Ziel einer forensischen Untersuchung ist es herauszufinden was geschehen ist, wo und wann es passiert ist, wie es dazu kam und folglich dazu wer es getan hat (Täter?) und auch, was mögliche Präventionsmaßnahmen sind.

Objektivität

Die Effektivität einer Untersuchung hängt entscheidend von der Objektivität der Ermittler ab. Jeder Fall ist einzigartig und muss als neuer Fall behandelt werden. Ermittler beginnen sofort, Theorien über den Tathergang zu bilden. Wichtig sind dabei Fakten, nicht Vermutungen! Die „Erfahrungsfalle": Wenn ein neuer Fall ähnlich erscheint zu einem alten, ist man geneigt, den neuen mit den Mitteln anzugehen, die beim alten zum Erfolg führten. [6]

Risiken von Voreingenommenheit

Voreilige Theorien können dazu führen, dass bestimmte Spuren nicht mit der nötigen Sorgfalt untersucht oder falsch interpretiert werden. Zum Beispiel: gelöschte Datei mit Namen ,,oorn1yr5.gif" mit nacktem Kleinkind. Bei der Dateiwiederherstellung könnte ein Ermittler geneigt sein, den

Originalnamen als „porn1yr5.gif“ statt ,,born1yr5.gif“ zu wählen. Besser ist es, ein neutrales Zeichen verwenden „ orn1yr5.gif" Es muss dokumentiert werden, dass das erste Zeichen zerstört war.

Wissenschaftliche Methodik/Vorgehen

Die Grundannahme lautet: Jede Beobachtung oder Analyse kann Fehler enthalten.

Der Versuch, eine Theorie zu bestätigen, erhöht die Chancen, Fehler zu machen. Wenn eine Möglichkeit nicht ausgeschlossen werden kann, dann kann ein Fehler vorliegen. Ein besserer Ansatz ist es, viele Theorien zu entwickeln und versuchen, diese Theorien zu widerlegen. Dadurch ist es schwerer, von einer Theorie eingenommen zu werden und es gibt eine höhere Wahrscheinlichkeit, objektive Ergebnisse zu bekommen mittels hypothesengetriebener Prozesse. Es gilt immer der Grundsatz: Suche immer Fehler in Deinen eigenen Theorien!

„... das einzige Kriterium für die Wissenschaftlichkeit eines Satzes ist seine prinzipielle Falsifizierbarkeit." - Wissenschaftstheorie von Karl Popper (1902-1994)

Der Grundsatz, dass nichts verändert werden darf, bietet nur das Wissen, dass nichts verändert wurde und bedeutet somit lediglich, dass man nichts bewusst verändert hat. Änderungen passieren schnell, z.B. durch das Booten eines Systems oder dem Mounten einer Festplatte. Der schnelle Schwund der originalen digitalen Spuren ist ein Phänomen der digitalen Welt. Deshalb ist es umso wichtiger, alles immer und überall nachweisbar zu machen durch Dokumentieren! Dokumentieren! Dokumentieren!

Die Werkzeuge, mit denen an den Daten gearbeitet wurde, müssen für den Zweck evaluiert sein und anerkannte Verfahren müssen auch hinterfragt werden. Beispielsweise Softwareanwendungen unterscheiden sich in den Versionen, die anders funktionieren können. In der Verhandlung kann die verwendete Version nachgefragt werden. Daher ist es wichtig, wirklich ALLES zu dokumentieren.

1.2.3 Vergleich zur analogen Welt

Pioniere der Forensik

Objektive Befunde und Spuren sind neben den Aussagen von Beschuldigten und Zeugen die wichtigsten Beweismittel im Strafverfahren.

„Mit jedem Fortschritt der Criminalistik fällt der Wert der Zeugenaussagen, und es steigt die Bedeutung der realen Beweise.“ - Hans Groß (1899) „Handbuch für den Untersuchungsrichter“

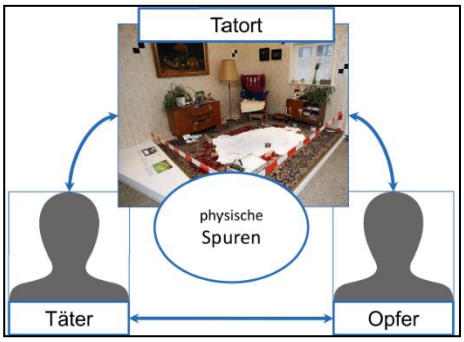


Abbildung 3: Austauschprinzip in der analogen Welt

Dr. Edmond Locards Austauschprinzip: Jeder und alles am Tatort nimmt etwas mit und lässt etwas zurück. Diese Prinzipien bilden das Grundprinzip und Eckpfeiler der Forensik und sind Basis für jede Suche nach Spuren.

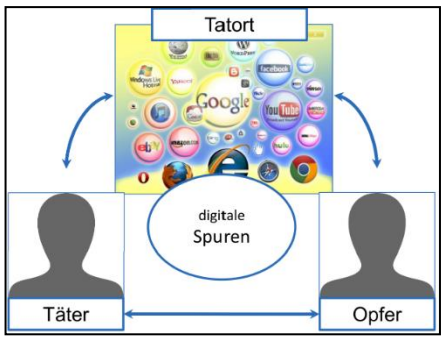


Abbildung 4: Austauschprinzip in der digitalen Welt

Zwischen Opfer Täter und Tatort können Spuren vermittelt werden, dies ist eine einfache Ontologie der analogen Welt, wie in Abbildung 3 dargestellt. Diese Ontologie lässt sich in den digitalen Raum übertragen und abstrahieren, wie in Abbildung 4 dargestellt.

1.2.4 Informatik – forensische Wissenschaft

Die digitale Welt ist vollends in die reale Welt eingebettet. Dabei umschließt die reale Welt, die durch Wissen und Fantasie ausgezeichnet ist, die digitale Welt komplett und bildet sie ab.

Die digitale Identität besteht aus einer Ansammlung von Daten mit wohldefiniertem Personenbezug und ist nur ein Teil der persönlichen Identität eines Menschen. Diese zeichnet sich durch den Leib, soziale Netzwerke und Bezüge, Arbeit und Leistung, materielle Sicherheit, Werte und Normen und im Allgemeinen die Gestalt und das Verhalten einer Person aus. All das sind Merkmale, die zu der Identität und Identifizierung einer Person beitragen.

Aus digitalen Spuren lassen sich mit dem Tatmittel Internet Merkmale über Identitäten und User finden. Durch bestimmte Merkmale und Features zeichnet sich ein Mensch zum User aus. In der IT-Forensik sind dies zwei getrennte Begriffe und die Erkenntnis, dass es sich bei einem User und Menschen um dieselbe Person handelt, muss erst gewonnen werden.

Soziale Gruppen und Strukturen ähneln sich in der analogen und digitalen Welt stark. Am Ende hat immer ein Mensch an einem anderen Menschen mittels digitaler Devices und Kommunikationswegen eine Straftat begangen. Dies ist der Zusammenhang zwischen realer Welt und digitaler Welt. Durch die Zusammenhänge von Moral, Anonymität, Umgang (mit anderen), Technische Entwicklungen und der Kriminalität wird die Entstehung neuer digitaler Kriminalitätsphänomene vorangetrieben.

Locard'sches Prinzip

Das Austauschprinzip lässt sich, wie eben festgestellt, auf den digitalen Raum übertragen. In Abbildung 5 ist schematisch dargestellt, welche Akteure digitale Spuren hinterlassen können und dass von einem Nutzer nur durch die Authentifikation auf eine Person geschlossen werden kann.

Ein Beispiel: Bei einer Hausdurchsuchung wird ein PC in der Wohnung gefunden. Damit wird die Wohnung zum physischen Tatort. Das digitale Device mit dem digitalen Tatort ist dort verortet. Digitale Spuren lassen sich am digitalen Tatort finden. Weitere zum Nutzer zugehörige Daten lassen sich durch Netzstruktur oder Netzwerk im digitalen Umfeld finden, beispielsweise durch andere verknüpfte

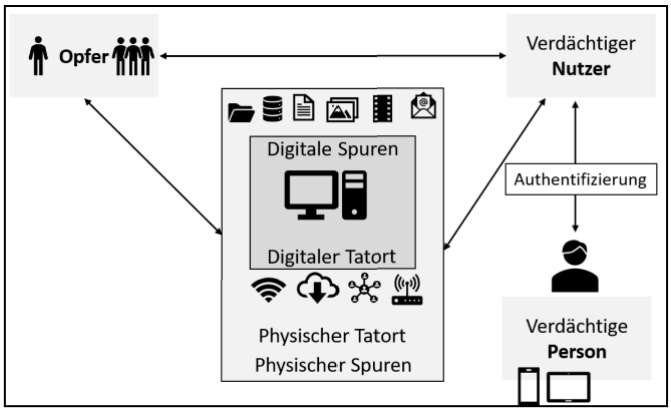


Abbildung 5: Locard´sches Prinzip im digitalen Raum

Geräte. Es stellt sich heraus, dass dieser PC einen User hat. Der Verdächtige gibt an, dass das Passwort aber vielen Leuten bekannt ist. Deshalb muss eine Untersuchung zu Zugriffsrechten, Usern, Logs und anderem gestartet werden. Wie ist die Netzwerkstruktur?

Zur Überprüfung, ob es sich bei dem User und der verdächtigen Person um die gleichen handelt, wird zunächst die Hypothese angenommen, dass es sich um die gleichen handelt. Zur Hypothesenüberprüfung werden weitere Mobile Devices untersucht, um an weitere Daten zu gelangen und möglichst eine Authentifizierung durchführen zu können.

In Abbildung 6 ist schemenhaft die Übertragung von Mustern und Materie im Zusammenhang mit dem Tatort, dem Verdächtigen und dem Opfer aufgezeigt. Der Verdächtige ist dabei mit dem User gleichzusetzen und die Verbindung zwischen dem Verdächtigem und dem Opfer geschieht durch die Übertragung von Material und Mustern. Muster sind beispielsweise Dateien oder Bilder.

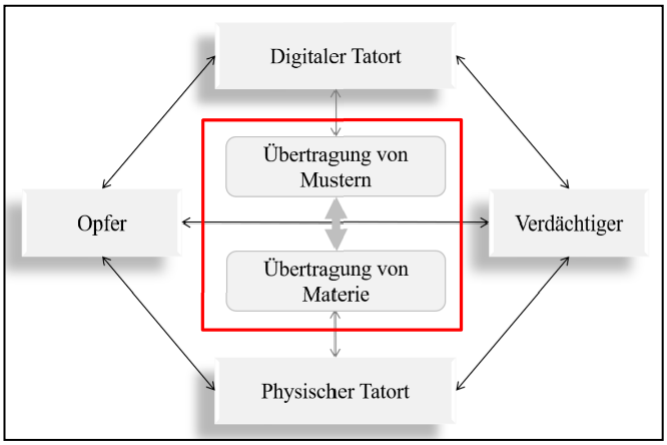


Abbildung 6: Schema zur Übertragung von Mustern und Materie am Tatort

Übertragung von Materie (physical transfer)

Hierbei geht man in der Regel davon aus, dass sich unter einer gewissen Energieeinwirkung ein Objekt zerteilt und Einzelteile davon von einer Quelle auf ein Ziel übertragen werden. Typischerweise fällt die Energie beim Kontakt an.

Übertragung von Mustern (transfer of traits)

Hierbei werden charakteristische Formeigenschaften von einem Objekt auf ein anderes übertragen, ohne dass notwendigerweise Materie ausgetauscht wird.

Wenn Materie übertragen wird, ist die Zerteilung eine notwendige Voraussetzung.
Wenn Muster übertragen werden – nicht.

Muster – Spuren - Spurenträger

Digitale Spuren ⟷ Analoge Spuren

Jede Straftat/kriminelles Ereignis ist ein Ereignis in Raum und Zeit. Alles, was für die analogen Spuren gelernt wurde, lässt sich auch auf die digitalen Spuren anwenden.

1.2.5 Wahrheitsfindung/Analyse von Spuren

Kern der Kriminalistik ist die Wahrheitsforschung. Kriminalisten sind Wahrheitsforscher. Sie versuchen eine der Realität möglichst entsprechende "Aktenwahrheit" zu schaffen, die es möglich macht, einem Gericht gegenüber bestimmten Behauptungen beweisen zu können. Hierzu bedienen sie sich des Sach- und des Personalbeweises. Der Gedanke, die Wahrheit durch Ermittlungen zu erfahren ist trügerisch und gefährlich.

Grundlage hierfür bildet die Annahme, dass sich das in der Vergangenheit liegende, kriminalistisch relevante, aufzudeckende und zu untersuchende Ereignis als Ganzes in dem Milieu, in dem es sich ereignet, widerspiegelt. Die Wirkungen, die das zugrunde liegende Ereignis erzeugt, ergeben in ihrer Gesamtheit ein Bild des Ereignisses.

Die Kriminalistik befasst sich als Wissenschaft mit den strategischen, taktischen und technischen Mitteln und Methoden zur Aufdeckung, Untersuchung (Aufklärung) und Verhütung von Straftaten und kriminalistisch-relevanten Sachverhalten.

Sie befasst sich mit den Gesetzmäßigkeiten und Erscheinungen des Entstehens von Informationen bei der Begehung von Straftaten sowie die Methoden ihres Auffindens, Sicherns und Bewertens für Ermittlungs- und Beweiszwecke.

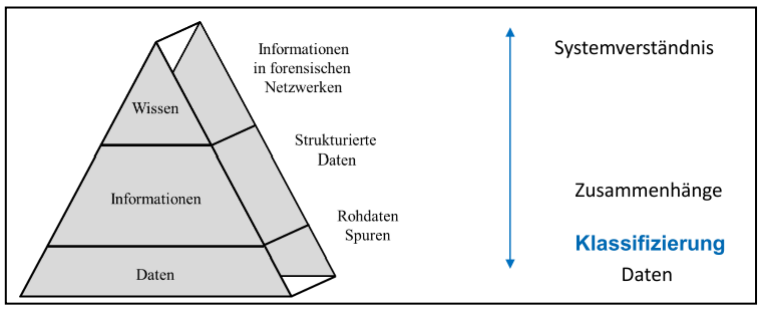


Abbildung 7: Pyramide der Entwicklung von der Information zum Wissen

Abbildung 7 stellt den Verlauf der Informationsgewinnung aus der Masse der Daten dar. Zunächst werden die auf einem Asservat gesicherten Rohdaten (digitale Spuren) in unterschiedliche Kategorien eingeteilt. Bei der Klassifizierung tritt das Problem „Big Data“ auf, weshalb in diesem Schritt Machine Learning und künstliche Intelligenzen eingesetzt werden müssen. Daraufhin werden die Rohdaten durch Analyse strukturiert. Nach der Analyse werden aus den unterschiedlichen Ergebnissen Informationen gezogen. Wenn diese Informationen dann zusammengelegt und kombiniert werden, dann entsteht das Wissen an der Spitze der Pyramide. Das Finden und Analysieren der daten und

Informationen erfolgt komplett objektiv. Der subjektive Teil erfolgt dann mit der Erkenntnis und dem daraus folgenden Urteil.

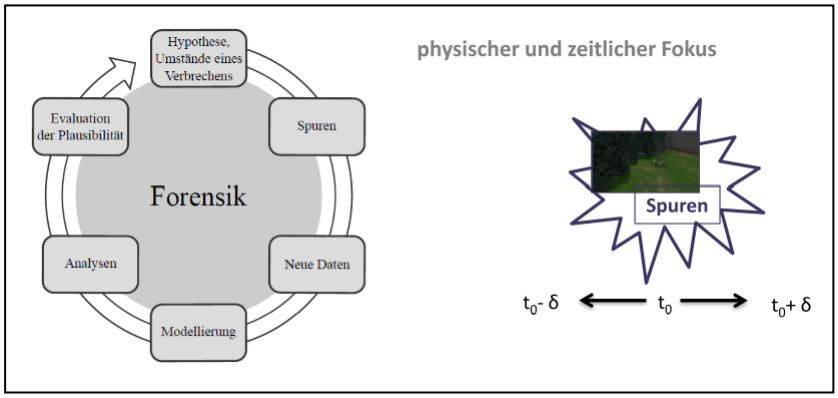


Abbildung 8: Darstellung über den Ablauf einer forensischen Ermittlung und Zusammenhang zum Aspekt der Zeit

Die Analyse und Visualisierung aller Prozesse und Spuren basieren auf einem einheitlichen Modell, das links in der Abbildung 8 dargestellt ist. Der physische und zeitliche Fokus muss in diesem Modell mit einbezogen werden.

Die Modellierung kann in Form von realen Modellen, Wahrscheinlichkeitsmodellen, Simulationen oder Denkmodellen passieren. Jede Modellform muss darauf auch evaluiert und überprüft werden.

Der rechte Teil der Abbildung 8 bezieht sich auf den physischen und zeitlichen Fokus. t_0 ist der Zeitpunkt des Findens der Spur. In die linke Richtung befindet sich die Vergangenheit mit dem Entstehungszeitpunkt der Spur t_0-δ , in die rechte Richtung befindet sich die nachfolgende Zeit nach dem Finden der Spur mit t_0+δ. Daraufhin werden die Spuren mit anderen Spuren zusammengelegt und bekommen so eine (neue) Bedeutung im Prozess der Rekonstruktion.

Die Übertragung von Mustern (Informationen) von einem Objekt auf ein anderes während des Tatherganges ist in der Abbildung 9 dargestellt.

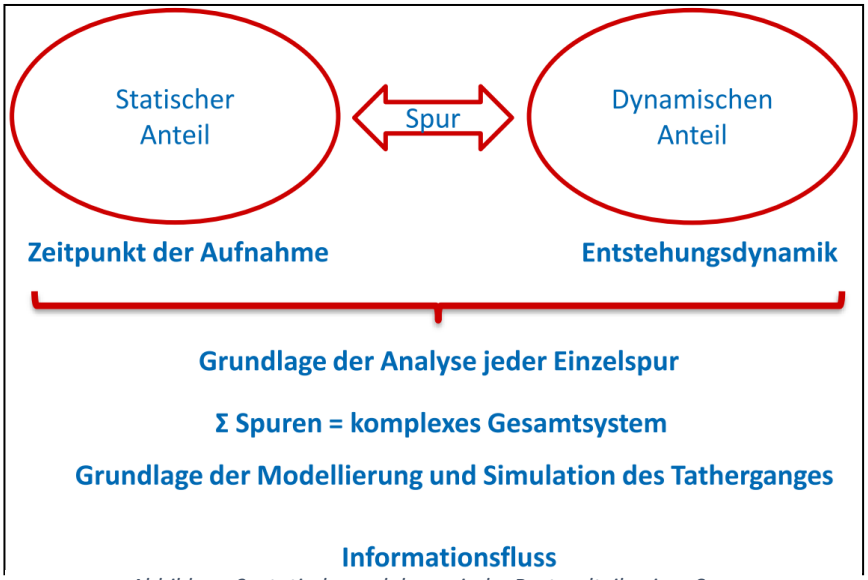


Abbildung 9: statische und dynamische Bestandteile einer Spur

Eine Spur teilt sich demnach in ihren statischen und dynamischen Anteil auf. Der statische Anteil ist durch den Zeitpunkt des Auffindens der Spur gekennzeichnet. Der dynamische Anteil der Spur beschreibt den Moment der Entshethung der Spur und wird daher mit der Entstehungsdynamik gleichgesetzt.

Die Kombination des statischen und dynamischen Anteils ist die Grundlage der Analyse jeder Einzelspur. Die Summe der Spuren lässt sich so zu einem komplexen Gesamtsystem verbinden. Dies schafft die Grundlage der Modellierung und Simulation des Tatherganges und den daraus folgenden Informationsfluss, dargestellt in Abbildung 10.

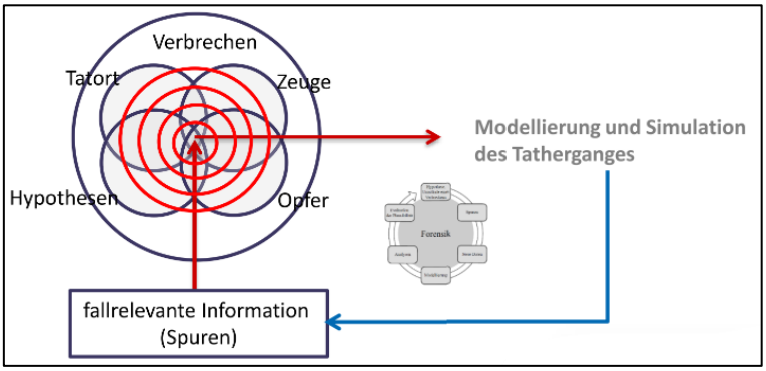


Abbildung 10: Zusammenhang zwischen Modellierung und Information

Im Digitalen Raum stellt sich also beispielsweise die Frage, wer zu welchem Zeitpunkt ein Event oder eine Veränderung z.B. in einer Datei ausgelöst hat. Bei Bildern mit gleichem Namen aber anderem Inhalt fragt sich, ob Bild 2 aus Bild 1 entstanden ist oder nicht. Events wie die Weitergabe, das Kopieren oder Verändern von Daten geben Informationen, bei denen ein statischer und dynamischer Anteil vorhanden sein können und mit einem Zeitstempel versehen sind. Mithilfe von Logik wird aus den erstellten Timelines ein erfolgreicher Ermittlungsansatz erarbeitet, der die analoge Forensik als Vorbild hat.

Inhalte der Spuren können nach verschiedenen Kriterien klassifiziert werden und in Konzepte überführt werden. Die Visualisierung von Netzwerken und darin stattfindender Prozesse bietet sich mittels Graphen an, um die Zusammenhänge im Netzwerk grafisch zu verdeutlichen.

1.3 Digitale Spuren

Die Spurenkategorien aus dem analogen Raum lassen sich auch in den digitalen Raum übertragen. Die analoge Trugspur entspricht den digitalen Daten, die reale Spur lässt sich mit der digitalen Spur und die fingierte Spur mit vernichteten/gelöschten/überschriebenen Daten gleichsetzen. Die allgemeine Einteilung der Spuren lässt sich also 1:1 übertragen.

Spuren sind alle materiellen Veränderungen an Personen und/oder Sachen bzw. Objekten, die im Zusammenhang mit einem relevanten Ereignis entstanden sind und zur Tataufklärung beitragen können, da Rückschlüsse auf den Tatablauf, die Tatumstände sowie Hinweise auf den/die Täter gezogen werden können. Entscheidend ist das der Spur innewohnende objektive Informationspotential, dieses muss beständig sein (Beibehaltung bis zur Begutachtung). Die materiellen Spuren bestimmen den Gegenstand der Spurenkunde unter anderem in der Kriminaltechnik. Grundsätzlich gilt: Es gibt keinen Tatort ohne Spuren!

Digitale Spuren (digital evidence) sind somit Spuren, die auf Daten basieren, welche in Computersystemen gespeichert oder übertragen worden sind. Dabei sind digitale Spuren nicht mit materiellen Spuren gleichzusetzen. Digitale Spuren werden erst durch ihre Interpretation von

physischen Spuren über unterschiedliche Interpretationsebenen zu einer verwertbaren digitalen Spur. Der digitale Fußabdruck hilft zum Beispiel bei OSINT mit Daten aus dem Netz ein Nutzer Profil erstellen zu lassen. Dazu sind verschiedenste Quellen nutzbar wie Netzwerke, Browser, Cloud, etc.

Digitale Spuren sind nicht personenbezogen, es ist nicht bekannt, wer vor dem PC sitzt. Man muss also über Informationen zu dem User zu der Person gelangen, zum Beispiel mittels der Authentifikation. Spuren in der digitalen Welt sind zunächst getrennt von der physischen Welt und alles Gefundene ist nutzbar. Die Zuordnung von Handlungen einer Person zu digitalen Spuren ist nur durch einen starken Authentifikationsmechanismus möglich. Eine ausschließliche Beweisführung aufgrund von digitalen Spuren ist nicht durchführbar da eine Eintragung in reale Welt benötigt wird. Daher werden andere zusätzliche Spuren zum Vergleich benötigt mit einem Verweis zur Person selbst. Darauf kann alles im Netzwerk integriert werden.

Das BSI unterscheidet sieben Arten von forensischen Daten: [2, S. 11]

- Hardwaredaten
- Rohdateninhalte
- Details über Daten
- Konfigurationsdaten
- Kommunikationsprotokolldaten
- Prozessdaten
- Sitzungsdaten
- Anwenderdaten

Wie stellt man durch Digitalisierung analoge und digitale Spuren gemeinsam dar?

Die Plausibilität von großer Bedeutung. Digitale Spuren (digital evidence) sind Spuren, die auf Daten basieren, welche in Computersystemen/ mobile Devices gespeichert oder übertragen worden sind. Zunächst handelt es sich dabei um physische Spuren (Freiling/Gewald) durch die Magnetisierung auf der Oberfläche einer Festplatte, elektromagnetische Wellen auf einem Datenkabel oder den Ladezustand von Speicherzellen im Hauptspeicher.

Die Prinzipien der klassischen Forensik sind darauf anwendbar.

- Diskrete Repräsentation
- Menschen nicht direkt zugänglichen Form
- zunächst extrahiert und in eine lesbare Form übersetzt werden

1.3.1 Eigenschaften digitaler Spuren

Digitale Spuren sind von unterschiedlicher Flüchtigkeit. Man separiert in drei Unterkategorien:

- Persistente – gespeicherte Daten
- semi-persistente Daten (im Arbeitsspeicher)
- flüchtige Spuren (nur temporär vorhanden)

Durch die Kategorien werden auch die Eintrittspunkte für Ersteinschreiter und Erstauswerter für Sicherung am Tatort definiert. Tendenziell müssen die flüchtigsten Daten am ehesten gesichert werden.

Digitale Daten sind technische vermeidbar, beispielsweise im Falle von Systemdaten. Sie sind außerdem hochgradig manipulierbar. Die Spuren können stärker und schneller manipuliert werden als im analogen Raum. Dafür besitzen digitale Daten eine perfekte Kopierbarkeit, sodass 1:1 Kopien von

den Spuren erstellt werden können. Sie zeichnen sich außerdem durch geringe Freiheitsgrade aus und bieten wenig Interpretationsspielraum. Eine solche Kopie wird Image genannt, weil sie ein exaktes Abbild/Duplikat des originalen Systems ist. Das BSI beschreibt folgende Anforderungen, die an eine forensische Duplikation gestellt sind [2, S. 26]:

- Physische Kopie: Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben;
- Fehlerbehandlung: Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden;
- Vollständigkeit des Abbildes: Reservierte Bereiche von Massenspeichern müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;
- Unveränderheit: Die Erstellung des Abbildes muss mit der Berechnung einer kryptografischen Checksumme abgeschlossen werden, um die Unveränderheit (Integrität, siehe Kapitel) des Abbildes nachweisen zu können.

In der analogen Welt arbeitet man nach dem Schema: Suchen - Sichern - Analysieren. In der digitalen Welt ist es allerdings eher: Sichern - Suchen - Analysieren. Während es in der analogen Welt schwer bis unmöglich ist einen Tatort komplett zu sichern und in ein Labor zu transportieren, besteht in der digitalen Welt diese Möglichkeit bezogen auf z.B. mobile Endgeräte, Festplatten, etc. In diesem Fall sichert der Ermittler erst alle Daten und beginnt die Suche auf der gesicherten Datenkopie.

Ein Computer lässt sich in der realen Welt verorten da es ein physisches Gerät ist. Das Internet lässt sich allerdings nicht geografisch verorten. Nur Devices lassen sich beispielsweise mittels IP-Daten oder Funkzellendaten geografisch finden. Bei der Datenübertragung von räumlich getrennten Speichermedien entsteht ein Event. Wenn ein Datentransfer geschieht, dann gibt es auch einen Nachweis darüber. Diese Events und andere Nachweise sind auf den entsprechenden Geräten gespeichert und können gefunden, ausgewertet und als Beweise genutzt werden.

Digitale Spuren und Abstraktion

Digitale Spuren benötigen Werkzeuge zur Aufbereitung. Diese Werkzeuge zeigen nur eine Abstraktion/Interpretation der physischen Spuren. Einige Abstraktionen können mehrere Abstraktionsebenen enthalten und jede Abstraktionsebene kann Interpretationsfehler enthalten.

Digitale Spuren können von Grund auf Interpretiert werden:

1. Interpretation der Magnetisierung der Festplatte (Bits)
2. Interpretation der Bits durch eine Zeichenkodierung
3. Interpretation der Zeichen durch ein Dateisystem als Daten
4. Interpretation der Daten im Dateisystem als zusammengehörige Datei
5. Interpretation der Datei als z.B. E-Mail

Manipulation digitaler Spuren

Digitale Spuren können leicht manipuliert werden. Absichtlich passiert dies zum Beispiel durch Straftäter oder auch unabsichtlich durch Ermittler. Eine Manipulation hinterlässt theoretisch keine unmittelbar sichtbaren Anzeichen, dass es sich um eine Manipulation handelt. Daher ist beim Nachweis einer Manipulation immer ein Kontext nötig.

Positive Eigenschaften digitaler Spuren

Man kann digitale Spuren exakt Duplizieren. Dadurch können Untersuchungen auf einer Kopie das Original schonen und die Übereinstimmung des Originals mit der Kopie ist nachweisbar. Manipulationen können durch Vergleich mit einer Originalkopie nachgewiesen werden.

Digitale Spuren sind schwer zu vernichte da auch gelöschte Dateien in der Regel noch lange Zeit auf der Festplatte rekonstruierbar sind. Notfalls hilft ein Rückgriff auf physische Spuren (z.B. Festplattenmagnetisierung). Wenn etwas vernichtet wurde, dann gibt es auch Hinweise, dass es vernichtet wurde und wie.

Komplexität und digitale Spuren

Heutige Systeme sind sehr komplex mit verschiedenen Betriebssystemen und davon verschiedenen Versionen. Jedes System gestaltet sich anders, weshalb niemand den kompletten Überblick hat.

Digitale Spuren entstehen heute überall. Es ist daher praktisch unmöglich, alle digitalen Spuren einer Straftat zu zerstören, die mit einem Computer verübt wurde. Die Erfahrung zeigt: Locards Austauschprinzip gilt (mit gewissen Einschränkungen) auch in der digitalen Welt.

Wo fallen digitale Spuren an?

Digitale Spuren findet man auf jedem digitalen Gerät, an verschiedenen Stellen in Betriebs- und Dateisystemen, aber auch in den einzelnen Komponenten. Die folgende Aufzählung ist nur ein Eindruck, stellt also nicht die Gänze der Fundorte digitaler Spuren dar.

- Browser-Caches
- Log-Dateien Backups
- Dateisystem (Zeitstempel, Swap Space, etc.)
- Firewalls
- Temporäre Dateien
- Windows-Registry Browser-History
- RAM (Prozessliste, Netzwerkverbindungen, eingeloggte User)
- Digitale Fotos (Multimediaforensik)
- Suchmaschinen
- Virenscanner
- Drucker
- Wahlwiederholungsfunktion am Telefon
- Autos (an mindestens 23 Stellen)
- Fotoapparate
- Digitale Überwachungskameras
- Geldautomaten
- Elektroherde
- Heizungssteuerungen
- Strom-/Wasser-/Heizungszähler
- Türschlösser
- Kühlschränke
- Fernseher
- iPods
- Videospielkonsolen
- DSL-Modems

1.3.2 Spezialgebiete der Forensik und deren resultierende Schnittmenge

Im Überlappungsbereich von allen Bereichen lässt sich feststellen, dass heutzutage ein Fall der digitalen Forensik nicht mehr nur in einem Bereich liegen kann sondern Teil von allen Bereichen ist. Daher ist es eher wichtig, die Eigenschaften, statt der Herkunft der Daten zu hinterfragen. In Abbildung 11 sind die Teilgebiete der digitalen Forensik dargestellt. Jede Disziplin hat spezielle Datentypen bzw. Datenarten, die entsprechend relevant sind. Durch die rasante Entwicklung in allen Bereichen der Technik, verlagern sich auch die Schwerpunkte in den einzelnen Bereichen. Als Beispiel sei hier die Entwicklung der Datenträgerforensik angeführt. In der jetzigen Zeit hat man im Ermittlungsumfeld den Fokus auf Festplatten, USB-Sticks, etc. Die Wahrscheinlichkeit, dass man die Beweissicherung einer Diskette durchführen muss, ist gering (aber niemals Null).

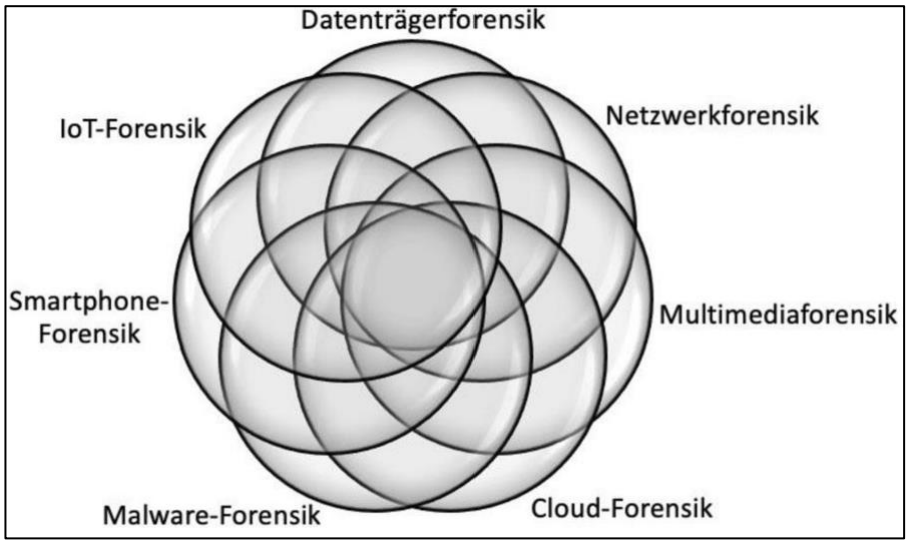


Abbildung 11: Darstellung über Teilgebiete der digitalen Forensik

Das Vorgehen in der Forensik muss also auf die modernen Bedingungen neu ausgerichtet werden. Für neue Techniken müssen wiederum neue Analysemethoden und -tools entwickelt werden.

1.3.3 Phänomene der digitalen Spuren

SIM-Swapping:

SIM-Swapping oder auch SIM-Karten-Swap genannt, ist ein Betrugsmasche, bei der sich ein Hacker die Mobiltelefonnummer eines Benutzers erschleicht, um sich (unter Umständen nur kurzfristig) der Onlineidentität des angegriffenen Opfers zu bemächtigen und als die Zielperson ausgeben zu können. Dies fällt unter den Begriff Identitätsdiebstahl, der allerdings nicht juristisch begründet ist. Zwischen 2013 und 2015 erbeuteten Betrüger auf diese Weise meist fünfstellige Euro-Beträge, der Gesamtschaden belief sich auf über eine Million Euro. Mobilfunkanbieter verstärkten darauf ihre Sicherheitsmaßnahmen, insbesondere bei der Freischaltung von Ersatz-SIM-Karten in den Mobilfunk Shops über die Hotline.

<u>Im größeren Maßstab:</u>

Straftaten im größeren Maßstab als das SIM-Swapping sind beispielsweise Computerbetrug im Onlinebanking durch Phishing und Änderung der Rufnummer für das mTAN-Verfahren. Der Modus Operandi sieht folgendermaßen aus. Zunächst erfolgt das Ausspähen der Zugangsdaten zum Konto. Dazu werden Phishing-Mails oder Schadprogramme eingesetzt. Darauf folgt die Änderung der Rufnummer für das mTAN-Verfahren durch Brief, Fax oder Anruf (Social Engineering). Die Änderungen

im Konto sind der letzte Schritt. Es wird das Onlinekonto mit Unterkonten gefüllt und Limits erhöht. Es wird bei einem solchen Vorgehen eine Vielzahl realer und digitaler Methoden aneinandergekoppelt.

Dieses Vorgehen wurde von einem Täter als kommerzielles SMS-Gateway angewandt und bei der Auswertung der Beweismittel und bekannten Buchungsvorgänge konnten 4 Geldwäschekonten bei der Fidor Bank AG ermittelt werden, siehe Abbildung 12.

Konto	DE73 7002 2200 0073 5196 91	DE67 7002 2200 0074 6753 60	DE35 7002 2200 0073 8169 04	DE14 7002 2200 0071 9214 17	gesamt
Kontoinhaber	xxxx, Steffen geb. 03.05.1989	xxxx, Andreas geb. 30-01.1951	xxxx, Martin geb. 30.01.1961	xxxx, Helmut geb. 23.09.1938	
Umsätze	115.704,69 €	268.561,33 €	135.013,12 €	52.064,50 €	**571.343,64 €**

Abbildung 12: Übersicht über Konten des Täters

Es wurden täterseitig 84 Rufnummern für ca. 14.000 Euro angemietet. Er Verifizierte sich mit komplett gefälschten Ausweisen. Die entsprechende Hardware kann ohne Probleme im Internet bestellt werden. Grundlegend lässt sich also sagen, dass keine konkrete Trennung zwischen der digitalen und analogen Welt existiert. Es macht also wenig Sinn, zu versuchen diese Bereiche zu trennen. Es muss immer allumfassend gedacht und ermittelt werden.

1.4 Forensischer Prozess

Motivation für ein wissenschaftliches Vorgehen

Wissenschaftliche Methoden, die fundiert und evaluiert sind werden auch in der Informatik benötigt. Gern werden OpenSource Produkte genutzt. Zur Wissenschaft gehört auch die wissenschaftliche Methodik. Die Qualität des Materials (der Daten) allgemein muss gegeben sein. Die Methoden müssen auch möglichst aktuell sein. Allerdings kann mit den wissenschaftlichen Methoden nicht gezaubert werden. Wenn die Datengrundlage qualitativ zu schlecht ist, können auch mit wissenschaftlichen Methoden keine verlässlichen Ergebnisse erbracht werden.

1.4.1 Abgrenzung Modell, Prozess und Methode

Das Wissenschaftliche Vorgehen soll auch wissenschaftlich begründet werden. Dazu wird ein **Modell** verwendet. Es stellt den Ablauf einer Untersuchung in vereinfachter Weise dar und besteht aus einzelnen Arbeitsschritten. Es gibt keinen Aufschluss über die Schritte innerhalb eines Abschnitts, sondern nur über die Notwendigkeit der Schritte. Der **Prozess** beschreibt den Ablauf in detaillierter Form. Die Abschnitte aus dem Modell werden in kleine Phasen unterteilt. Zum Beispiel wird erklärt, was speziell zum Analysieren oder Sichern oder Ähnlichem gehört. Die Reihenfolge des Ablaufs einer Untersuchung wird auch erläutert. Die **Methode** bezeichnet die im Arbeitsschritt eingesetzten Werkzeuge und Verfahren. Danach ist nur ein Nachweis der Evaluation notwendig, der belegt, dass die Methode überprüft wurde.

Anforderungen an die Vorgehensweise:

- **Akzeptanz**: Die angewandten Methoden und Schritte müssen in der Fachwelt beschrieben und allgemein akzeptiert worden sein. Der Einsatz neuer Verfahren und Methoden ist zwar prinzipiell nicht ausgeschlossen, jedoch sollte dann ein Nachweis der Korrektheit dieser erfolgen.
- **Glaubwürdigkeit**: Die Robustheit und Funktionalität von Methoden wird gefordert und muss ggf. nachgewiesen werden.
- **Wiederholbarkeit**: Die eingesetzten Hilfsmittel und Methoden müssen bei der Anwendung Dritter auf dem gleichen Ausgangsmaterial dieselben Ergebnisse liefern.
- **Integrität**: Sichergestellte Spuren dürfen durch die Untersuchung nicht unbemerkt verändert worden sein. Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein.
- **Ursache und Auswirkungen**: Durch die Auswahl der Methoden muss es möglich sein, logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und evtl. auch an Personen herzustellen.
- **Dokumentation (Chain of Custody)**: Jeder Schritt des Ermittlungsprozesses muss angemessen dokumentiert werden. Dies schließt lückenlose Nachweise über Verbleib/Verarbeitung/Herkunft von digitalen Spuren ein.

Vor der Auswahl des geeignetsten Modells oder der Methode, sollten einige Überlegungen getätigt werden. Aber auch während der einzelnen Schritte gibt es Hinweise, die zu beachten sind:

1. Verstehen Sie die Ziele und den Zeitrahmen der Untersuchung.

2. Listen Sie Ihre Ressourcen auf, einschließlich Personal, Zeit und Ausrüstung.

3. Identifizieren Sie mögliche Beweisquellen.

4. Schätzen Sie für jede Beweisquelle den Wert sowie den Aufwand für deren Sicherstellung.

5. Priorisieren Sie Ihre Beweissicherung.

6. Planen Sie die erste Erfassung / Analyse.

7. Legen Sie die Art und Weise bzw. Zeitpunkte für regelmäßige Kommunikation / Updates mit den Beteiligten fest.

8. Denken Sie daran, dass Sie sich nach der ersten Analyse jederzeit entscheiden können, zurückzugehen, um weitere Beweise zu sammeln. Forensik ist ein iterativer Prozess!

1.4.2 SAP-Modell

SAP steht für S(ecure)-A(nalyse)-P(resent) und stellt ein Modell des Ablaufs der forensischen Untersuchung dar. In der ersten Phase, der so genannten Secure Phase werden alle Daten sorgfältig erfasst. In der zweiten Phase, der Analyse-Phase, werden die gesicherten Spuren und Beweise sorgfältig überprüft und objektiv bewertet. In der dritten Phase wird der Ermittlungsprozess nachvollziehbar dargelegt und optional erneut bewertet (Präsentiert). Die Abbildung 13 veranschaulicht das Modell.

Abbildung 13: Schematische Darstellung des SAP-Modells

1.4.3 Modell nach Kent, Chevalier, Grance und Dang

In diesem Modell existieren vier grundlegende Phasen. Die erste Phase beschreibt die Datensammlung. In der zweiten Phase werden die Beweise selektiert und reduziert. Die Analyse der Beweise folgt in der dritten Phase und in der vierten Phase wird über den Prozess Bericht erstattet. Nach diesem Modell können auch wieder Schritte zurück gemacht werden, wie es im realen Leben auch passiert. Wenn in der Auswertung festgestellt wird, dass Aspekte fehlen, dann kann das Vorgehensmodell erneut gestartet werden. Bei Bedarf kann also ein Kreislauf errichtet werden. Das Modell ist in Abbildung 14 schematisch dargestellt.

Abbildung 14: Schematische Darstellung des Modells nach Kent, Chevalier, Grance und Dang

1.4.4 Der erweiterte forensische Prozess

Abbildung 15: Der erweiterte forensische Prozess

In Abbildung 15 ist der erweiterte forensische Prozess dargestellt. Dieser setzt sich aus sechs Phasen zusammen:

- **Strategische Vorbereitung**: Identifizierung und Bereitstellung geeigneter Werkzeuge, Tests und Sicherungstools, Vorgehensplanung, Vorbereitung von Hardware und Software, Maßnahmen seitens des Anlagenbetreibers (proaktiv)
- **Operative Vorbereitung**: nach dem Eintreten des Vorfalls, vor der Datensammlung, z.B. Identifikation potenzieller Datenquellen (auch Datenträger oder mobile Endgeräte)
- **Datensammlung**: wichtige Daten von potenziell betroffenen Systemen/Komponenten, vollständige Erfassung und Speicherung, Verfälschungen vermeiden, Fehler und Lücken dokumentieren (und rechtfertigen), Flüchtigkeitsreihenfolge beachten
- **Datenreduktion**: wichtige (forensisch wertvolle) Daten/Spuren identifizieren, unwichtige aus Untersuchung ausschließen
- **Datenanalyse**: Ergebnisse der reduzierten Daten in logischen Zusammenhang bringen, einheitlichen Zeitverlauf generieren,
  → Detailanalyse; (möglicherweise Wiederholung von Schritt 3 und 4)
- **Dokumentation**: Zusammenfassung aller Abläufe zu einem Bericht

1.4.5 BSI-Modell

Dieses Modell wird 7 Phasen-Zyklus-Modell genannt und vom Bundesamt für Sicherheit in der Informationstechnik erstellt. Es ist in Abbildung 16 dargestellt.

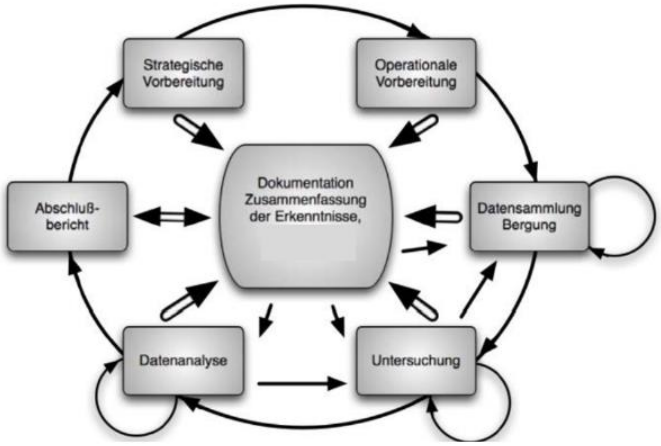


Abbildung 16: grafische Darstellung des BSI-Modells

Die Dokumentation erfolgt über den gesamten Zeitraum, während aller Schritte. Den Anfang bildet die strategische Vorbereitung. Auf die strategische Vorbereitung folgt die operationale Vorbereitung. Daraufhin können die Datensammlungen gesichert und geborgen werden. Wenn im darauffolgenden Schritt der Untersuchung der Daten festgestellt wird, dass eine erneute Datensammlung benötigt wird, dann kann der Schritt der Datensammlung beliebig wiederholt werden. Die Schritte der Datensammlung, Untersuchung und Datenanalyse können aus ihrer Position selbst immer wieder wiederholt werden. Um zielführend zu arbeiten, bietet es sich an, den Aspekt der Datenreduktion bereits bei der Datensicherung zu berücksichtigen. Schlussendlich folgt der Abschlussbericht. Durch die ständige Dokumentation ist dieses Modell für die forensische Arbeit sehr gut geeignet. Im Anschluss auf die erfolgreiche Anwendung des Modells kann optional eine Fehlerauswertung erfolgen, die für die zukünftigen Fälle von Vorteil ist.

1.4.6 Casey‘s Investigative Process

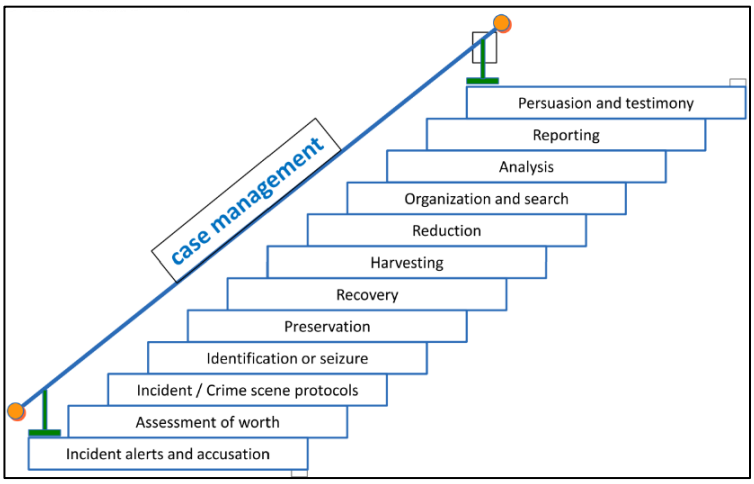


Abbildung 17: Der Forensische Ermittlungsablauf nach Casey

Dem Prozess in der realen Welt ähnelt diesem Modell von Casey, welches in Abbildung 17 zu sehen ist, am meisten. Es wird der Schritt der Reduktion und Wiederherstellung einbezogen und von jeder

einzelnen Stufe kann wieder zu vorhergegangenen Stufen zurückgekehrt werden. Außerdem können auch Stufen übersprungen werden.

Bei der Auswertung digitaler Spuren sollte eine allgemein akzeptierte und erprobte Vorgehensweise angewendet werden, die im besten Fall auf wissenschaftlicher Methodik basiert. Im Folgenden wird ein Rahmen für das Vorgehen bei der Sicherung und Auswertung digitaler Spuren vorgestellt. Man spricht deshalb auch von einem Vorgehensmodell. Beschrieben wird dieses auch in „Forensische Informatik“ von Andreas Dewald, Felix C. Freiling [4].

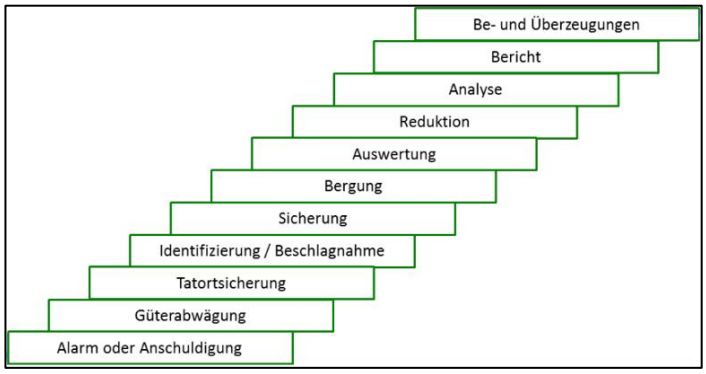


Abbildung 18: Der investigative Prozess in der Übersetzung von Dornsteif aus 2004

Das in Abbildung 18 aufgezeigte Vorgehensmodell leitet sich direkt aus dem Modell von Casey (Abbildung 17) ab. Es hat insgesamt 11 Stufen, beginnend mit der Stufe Alarm oder Anschuldigung. Darauf Folgen die Stufen Güterabwägung und Tatortsicherung. Die Vierte Stufe der Identifizierung und Beschlagnahme befasst sich mit der Einordnung und Erkennung. Darauf folgen die Stufen der Sicherung, Bergung, Auswertung, Reduktion und Analyse. Die letzten beiden Stufen sind der Bericht und Be- und Überzeugung.

Anschuldigung

Die Anschuldigung stellt das Startsignal für den Prozess dar. Es müssen in diesem Schritt die Quellen eingeschätzt werden und erste Erkundigungen getan werden.

Güterabwägung

In diesem Schritt wird abgewogen, wie groß das Interesse an der Verfolgung ist, im Vergleich mit den Kosten der Verfolgung. Diese Entscheidung fällt für Unternehmen häufig gegen eine Verfolgung aus.

Für die Verfolgung sprechen die Aspekte der Abschreckungswirkung, Schadensersatz und die Verbesserung der eigenen Sicherheit. Gegen eine Verfolgung spricht der Ressourcenverbrauch, die Downtime und negative Öffentlichkeit.

Beschlagnahme

Die traditionelle Herangehensweise ist Alles einsacken, absaugen und abstauben. Dies muss geschehen, ohne etwas zu verändern, da auch das Drumherum kann wichtig sein kann. Alle Gefahren müssen eingedämmt werden.

Tatortsicherung

Im Idealfall kann der Tatort weiträumig abgesperrt werden. *„freeze the evidence in place and provide ground truth for all activities that follow“* [6], gibt Casey dazu an. Dies ist allerdings mit dem Internet kaum möglich.

Daher wird beim Sichern gefragt, was, wie und wo aufgrund der Eigenschaften digitaler Spuren gesichert werden muss. Was kann nützliche Daten und Informationen bringen?

Abbildung 19: Diversität des physischen Auftretens von USB-Sticks

In den Bereich fallen vor allem Festplatten, Monitore, CD/DVD/Blue-Ray-Laufwerke, Lautsprecher, Tastatur, Maus, Drucker, Router, Webcam, Sticks, Server, USB-Sticks u.v.m.

Je kleiner die Speichermedien sind, desto schwerer ist es, sie zu finden. SD-Karten auf Türrahmen oder unter Tischplatten geklebt, werden oft übersehen. USB-Sticks gibt es in allen Formen, Farben und Auffälligkeiten. In Abbildung 19 sind einige aufgeführt. Aber auch Anhänger an Ketten können versteckte USB-Sticks beinhalten. Deshalb muss die Tatortsicherung und spätere Sicherung der Daten auf den Beweismitteln mit größter Sorgfalt erfolgen.

Sicherung

Es muss sichergestellt werden, dass alle Beweise unverändert bleiben. Dafür muss der Zustand fotografiert, die Beweismittel versiegelt und weggeschlossen werden.

Bei digitalen Spuren werden Kopien erstellt und alle weiteren Untersuchungen nur auf den Kopien durchgeführt. Zum Nachweis der Echtheit verwendet man kryptographische Hashes und ausschließlich vertrauenswürdige Tools. Alles, was getan wird muss auch hinterfragt werden. Hier beginnt die Arbeit von Informatik-Spezialisten.

Bergung und Auswertung

Bergung von Daten, die gelöscht, versteckt, getarnt oder anderweitig unzugänglich gemacht worden sind. Hier können Synergien mit anderen Beweismitteln genutzt werden. Zum Beispiel: Ist ein Zettel mit Passwörtern am Tatort gefunden worden?

In der Auswertung müssen großen Datenmengen organisiert werden. Zunächst werden die Meta-Daten statt der eigentlichen Datenuntersucht und die Daten im Allgemeinen gruppiert (z.B. nach Dateityp oder Zugriffszeiten).

Reduktion

Bei der Reduktion werden irrelevante Daten eliminiert. Es wird im Prozess fortgefahren, ohne die eigentlichen Daten anzuschauen. Die Reduktion erfolgt nach Dateityp, zum Beispiel: Bei der Anschuldigung „Besitz von Kinderpornografie“ wird eine Reduktion auf Dateien mit Endung .gif oder .jpg durchgeführt. Es handelt sich dabei um keinen simplen Prozess.

Das Ziel ist es, *„smallest set of digital information that has the highest potential of containing data of probative value“* [6] zu finden. Hilfreich können dafür Hash-Datenbanken von bekannten Dateien sein oder Verfahren wie das Whitelisting.

Strukturierung / Suche

In diesem Schritt erfolgt die Organisation der Daten nach der Reduktion. Oftmals werden hier Indizes und Übersichten erstellt. Dies macht das Referenzieren der Daten in den folgenden Schritten einfacher. Das Indexieren ist allerdings ein sehr aufwendiger Prozess.

Analyse

Es wird eine Detailanalyse unter Beachtung der Dateiinhalte durchgeführt. Dabei werden beispielsweise Verbindungen hergestellt oder Verantwortliche ermittelt. Inhalt und Kontext werden bewertet - „means, motivation, opportunity“.
Zusammenführung und Korrelationen, Assoziationen Netzwerken und Graphen von Daten. Anschließend wird mittels wissenschaftlicher Methodik überprüft.

Bericht

In dem Schritt wird der KT-Bericht oder das Gutachten erstellt. Dabei werden nicht nur Ergebnisse präsentiert, sondern auch der Weg des Erlangens dieser. Es muss immer über die befolgten Regeln und Standards berichtet werden. Alle Schlüsse werden begründet und alternative Erklärungsmodelle erörtert.

1.4.7 OSCAR-Modell

Das OSCAR-Modell dient zur Durchführung einer netzwerkforensischen Untersuchung (nach Davidoff & Ham). Das Akronym OSCAR steht für insgesamt fünf Einzelschritte, aus denen sich der Ermittlungsprozess zusammensetzt:

(1) Obtain Information

(2) Strategize, (Planung der Untersuchung, hinsichtlich des Ablaufes und der Festlegung der Datensicherungsmethoden, Prioritätenliste enthält beispielhaft etwa Spalten zum vermuteten Informationsgewinn, dem wahrscheinlichen Aufwand für die Sicherung und Erfassung, der mit der Sicherstellung verbunden ist und die vermutete Volatilität.)

(3) Collect evidence (Beweise zusammentragen, Beweise aufnehmen, Dokumentation, …)

(4) Analyze (Auswertung des Materials, wertet der Ermittler Beweismaterial anhand einer Reihe unterschiedlicher Informationen, Methoden und Werkzeuge aus, Die für die Analyse gewählte Methode hängt naturgemäß vom jeweiligen Fall ab.

(5) Report

1.4.8 Zusammenhang der verschiedenen Modelle

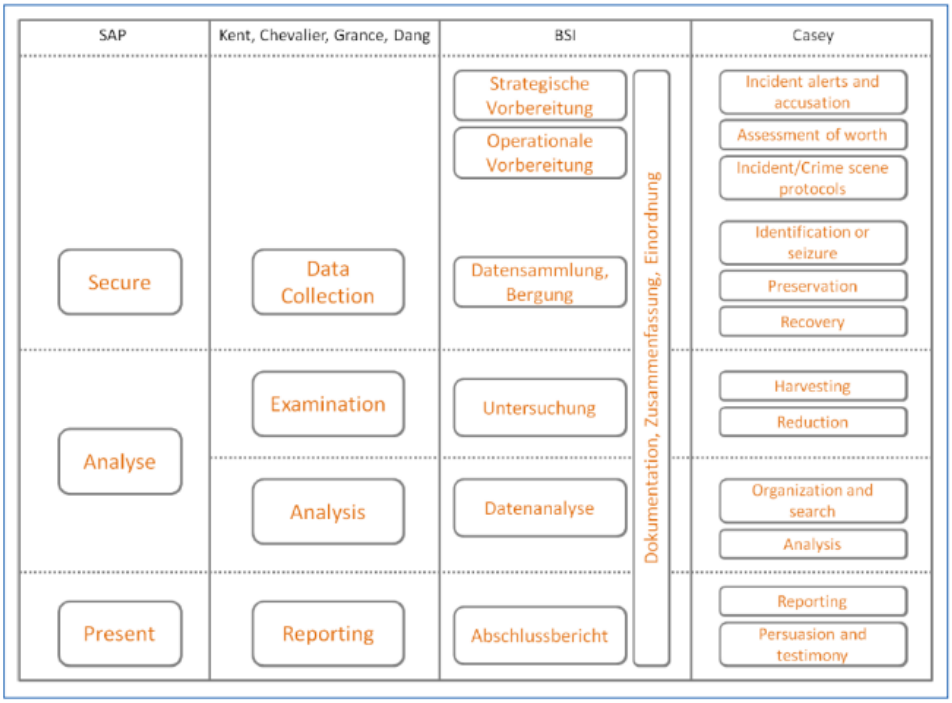


Abbildung 20: Zusammenhang der Modelle SAP, Kent et al., BSI und Casey

Wie in Abbildung 20 dargestellt wird, lassen sich die einzelnen Modelle ineinander überführen. Die Grundstruktur bildet dabei das SAP-Modell. Die Phasen der anderen (feineren) Modelle lassen sich den drei Phasen des SAP-Modells zuordnen.

1.5 Dokumentation

Bei der Dokumentation unterscheidet man zwischen prozessbegleitender und abschließender Dokumentation

Prozessbegleitend: parallel zur Durchführung, Protokollierung der gewonnenen Daten und durgeführten Prozesse, auch Parameter der Durchführung (Name und Versionsnummer des Programms, Kommandozeilenparameter des Aufrufs, Motivation zur Auswahl des Werkzeugs…)

Abschließend: Erstellen eines Gesamtbildes aus Daten, welche Information gewonnen, Ablauf der Untersuchung (für Dritte nachvollziehbar), Voraussetzung zur Abschätzung der Beweiskraft der Ergebnisse (Ist der Untersuchungsweg mit gleichen Ergebnissen wiederholbar? Sind die eingesetzten Werkzeuge und Methoden allgemein anerkannt? Ist die Wahl der eingesetzten Werkzeuge und Methoden nachvollziehbar? War der Untersuchende mit diesen ausreichend vertraut, um potenzielle Hinweise zu erkennen?)

Automatische Dokumentation

Auf der Kommandozeilenebene unter Linux Systemen gibt es Toolunterstützung, die sich mit dem Unix-Kommando script aufrufen lässt.

Auf der Manual Page wird dazu folgendes Beschrieben:

- script makes a typescript of everything printed on your terminal. It is useful for students who need a hardcopy record of an interactive session as proof of an assignment, as the typescript file can be printed out later with lpr (1).
- If the argument file is given, script saves all dialogue in file. If no file name is given, the typescript is saved in the file typescript.

Auch forensische Programme wie beispielsweise X-Ways bieten Funktionen zur automatischen Dokumentation. Hierbei werden alle Schritte aufgeführt, die im Programm ausgeführt wurden.

Dokumentation von Zeit

Dokumentieren Sie, wann Sie welche Aktionen durchführen. Notwendig bei einer automatischen Dokumentation ist eine korrekte Zeit an Ihrem Arbeitsplatz (NTP), Dokumentieren Sie dies. Dokumentieren Sie auch die Zeit des Untersuchungsobjekts. Dies ist wichtig für die Interpretation von Zeitstempeln.

Jedoch ist eine eigene per Hand (auf Papier) durchgeführte Dokumentation verlässiger!

2 Informationstechnik

2.1 Mathematische Grundlagen

Damit Daten bzw. Informationen mit Computerprogrammen verarbeitet werden können, müssen sie in maschinenlesbarer Form repräsentiert werden. Dazu werden unterschiedlichste Systeme verwendet. Das Problem dabei ist, dass Computerprogramme mit für den Menschen verständlichen Repräsentationsformen wie Bildern, Buchstaben, Tönen nichts anfangen können.
Computer verarbeiten nur Zahlen: Daten jeglicher Art müssen also in ein Zahlenformat transformiert werden. Diesen Vorgang nennt man Digitalisieren.
Im Rahmen der IT-Forensik müssen wir die Daten sichern, analysieren und auswerten. Daher ist ein Grundverständnis über die Repräsentation der Daten notwendig.

Zahlensysteme dienen zur Darstellung von Zahlen und Zeichen sich durch die Folge von Ziffern und Zeichen aus. Das Dezimalsystem wird als Standard-Zahlensystem angesehen. Zahlensysteme sind wichtig für Digitaltechnik. Es werden hauptsächlich das duale Zahlensystem (Binärsystem), oktale Zahlensystem und hexadezimale Zahlensystem eingesetzt. Dafür stehen meist sog. Übersetzungstabellen zur Verfügung.

2.1.1 Herleitung

2.1.1.1 Bits und Bytes

Die beiden Grundeinheiten in jedem heutigen Computer sind die Einheiten Bit und Byte. Die elementarste Informationseinheit, mit der Computer arbeiten, ist das Bit (engl. Binary Digit = Binärziffer). Computer arbeiten physikalisch mit zwei alternativen Spannungszuständen: ein relativ hohes Spannungspotential oder ein relativ niedriges Spannungspotential. Diese werden mit den Ziffern 1 (hoch) und 0 (niedrig) bezeichnet. Informationen sind dadurch eindeutig durch Zahlenfolgen kodierbar. Diese Technik stellte sich als technisch einfach realisierbar, gut speicher- und übertragbar heraus. Weitere fortgeschrittene Techniken wie das Quantencomputing oder DNA-Computing mit langen Zeichenfolgen aus vier Grundbuchstaben stellen die zukünftige Entwicklung dar. Aus der Kombination der Technologie mit Kryptologie und Kryptoanalyse wird sich in der Wissenschaft mehr Rechenleistung erhofft.

2.1.1.2 Zeichen, Daten, Information

Zeichen  → 101010 → 2A → 42

Physikalisch gesehen ist ein Zeichen eine zeitliche Änderung einer messbaren Größe. Die Informatik abstrahiert von den konkreten physikalischen Größen und spricht von „Zeichen“ (elementare Muster). Dieses Wissen wird zur Datenwiederherstellung benötigt.

Daten sind Zeichen, die zur Darstellung von Informationen genutzt werden. Sie beinhalten syntaktische Dimensionen. Die Information beinhaltet Form (Syntax) und Inhalt (Semantik).

2.1.1.3 Kommunikation, Nachricht, Information

Kommunikation dient dem Austausch von Information in Form von Daten oder einer Folge von Zeichen. Man kann auch vom Austausch von gebundenen immateriellen Objekten (Information ist

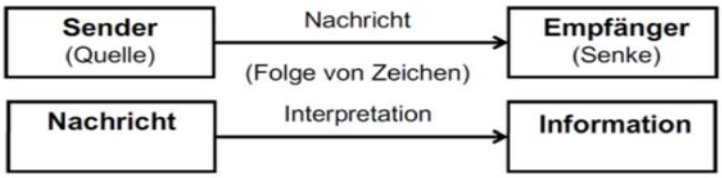


Abbildung 21: Kommunikationsmodell

immateriell) sprechen. Nachrichten sind konkrete immaterielle Objekte, die von einem Sender zum Empfänger übertragen werden.

Nachrichten sind Zeichenfolgen, die aus einem vorgegebenen Alphabet gebildet werden. Mit dem Alphabet wird die Kodierung vorgenommen Informationen sind zweckdienliche, handlungsbestimmende Daten über Zustände und Ereignisse der Realität, die das Wissen erweitern. An die Information gelangt man durch die Interpretation einer Nachricht. Diese ist häufig nicht eindeutig, sondern subjektiv. Das Prinzip ist in den Kommunikationsmodellen bekannt. Digitale Devices sind in dem Fall nichts anderes als Kommunikationsnetzwerke. In Abbildung 21 ist sowohl das Übermitteln der Nachricht zwischen Sender und Empfänger dargestellt als auch die Verbindung zwischen Nachricht und Information. Aus Nachrichten kann man durch Interpretation auf die Information schließen. Der Begriff Nachricht kann hier auch durch Daten ersetzt werden. Interpretiert man Daten, kann man auch die entsprechende Information erlangen. Beispielsweise die Interpretation von Daten durch ein Dateisystem, welches einem dann die Information über eine Datei ergibt, aber auch die Interpretation von Daten durch einen Ermittler (analog). Hierbei ist die Fehlerquote, die sich durch das Interpretieren ergibt, nicht zu vernachlässigen.

2.1.1.4 Alphabet

Um Informationen darstellen zu können, müssen Zeichen immer Elemente eines bestimmten Zeichenvorrats sein, dessen Bedeutung sowohl dem Sender als auch dem Empfänger bekannt ist. Ein Alphabet ist ein geordneter Zeichenvorrat. Alphabete müssen mindestens zwei Zeichen enthalten, um einen „Unterschied“ darstellen zu können. Ein binäres Alphabet enthält genau zwei Zeichen. Ein Zeichen eines binären Alphabets heißt Binärzeichen oder Bit (binary digit). Das Standardalphabet der Informatik besteht aus den Zeichen 0 und 1.

In der Informationstechnik existieren auch andere Alphabete, deren Bedeutung für Experten groß ist. Neben dem Binärsystem mit den Zeichen 0 und 1 ist besonders das Hexadezimale System wichtig. Dieses besteht aus 16 Zeichen: 0 bis 9 und A bis F.

2.1.1.5 Kodierung, Code, Zeichensatz

Eine Kodierung ist die Informationsdarstellung in Form von Ziffern. Alle Daten liegen auf der Festplatte in Kodierter Form da. Das Ziel der Kodierung ist die Speicherung und Verarbeitung von Informationen. Dieser Zweck kann auf das „Rechnen“ zurückgeführt werden. Im Computer werden alle Informationen durch Bits dargestellt und kodiert. Ein Code lässt sich als eine eineindeutige Abbildung zwischen zwei Zeichenvorräten sehen. Ein Zeichenvorrat ist dabei eine endliche Menge von eindeutig unterscheidbaren Symbolen (binärer Zeichenvorrat besteht nur aus zwei Zeichen).

Beispiel Digitalisierung

Die Aussage „Bayern München hat 2, die Dynamos 5 Tore geschossen.“ enthält eine Information, die für den Menschen verständlich ist. Eine problemnahe Darstellung der gleichen Information wäre „2:5“. Die maschinennahe Darstellung der Information „00000011 00011111“. Die technische Realisierung mit einem Zweizustandssystem ist in Abbildung 22 zu sehen. Diese Varianten sind für den Computer verständlich. Dabei ist zu beachten, dass es sich bei dieser Form der Darstellung **noch nicht um die Kodierung durch das Bitsystem** handelt. Es ist nur eine aufsummierbare Darstellung durch Einsen und Nullen.

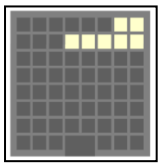


Abbildung 22: Technische Realisierung des Beispiels

2.1.2 Zahlensysteme

2.1.2.1 Binärsystem

Die Aussage „Hello World!“ wird kodiert in „01001000011001010110110001101100011011110101011101101111011100100110110001100100000100001“. Wie kann man von einem (für uns verständlichen) Zeichenvorrat in einen anderen übersetzen?

Ein Bit ist dabei eine einzelne Zahl und ein Byte die Folge von 8 Bit (Grundstruktur). Bytes werden von rechts nach links gelesen.

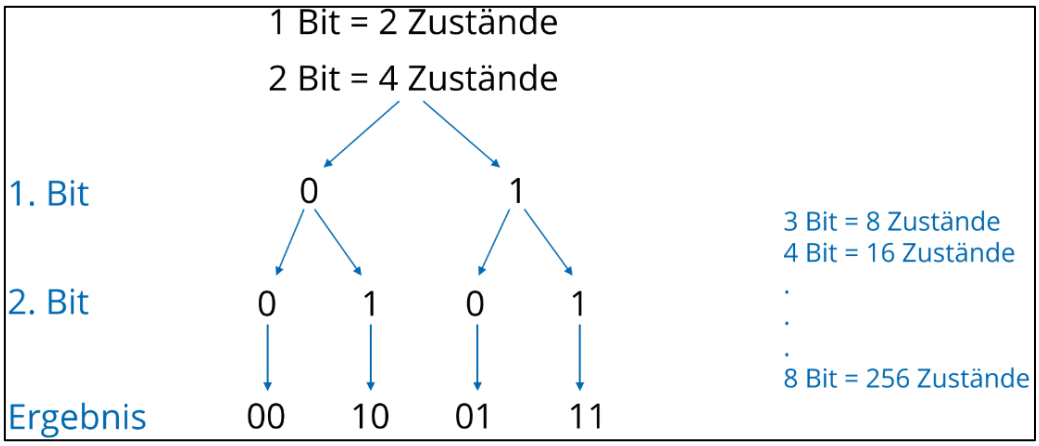


Abbildung 23: Zusammenhang zwischen Bitanzahl und Anzahl der Zustände

In Abbildung 23 wird der Zusammenhang der Bitanzahl und den möglichen Zuständen dargestellt. Ein Bit kann entweder 0 oder 1 sein. Es liegen also zwei mögliche Zustände vor. Hat man zwei Bit zur Verfügung, wobei jedes Bit 0 oder 1 sein kann, ist es möglich vier Zustände zu erzeugen: 00, 10, 01 und 11. Wie bereits erwähnt ist die Grundstruktur, in der gearbeitet wird, 8 Bit. Das bedeutet 1 Byte kann 256 Zustände haben von 0000 0000 bis 1111 1111 (die Lücke nach jeweils 4 Bit dient der Übersichtlichkeit). Jeder Zustand ist so gesehen ein Wert, der vergeben werden kann. Diese 256 Werte können nun durch den ASCII-Code in Buchstaben umgewandelt werden, um daraus für uns verständliche Wörter darzustellen.

ASCII

ASCII ist der Standard zur Darstellung von Zeichen durch elektronische Geräte. Es werden 7 Bit zur Darstellung und 1 Bit zum Prüfen verwendet. Dadurch wird die Kodierung von Steuerzeichen, Sonderzeichen, Ziffern und Buchstaben mithilfe der ASCII-Table erzielt. Spätere Versionen nutzen 8 Bit, wodurch 256 Zeichen kodierbar sind. In Abbildung 24 ist beispielhaft die Übersetzung von Binär-Codes in ASCII-Zeichen dargestellt. Man findet im Internet die Kodierungstabellen. Sie dienen als Hilfestellung.

Binär	ASCII-Zeichen
100 0110	F
100 1111	O
101 0010	R
100 0101	E
100 1110	N
101 0011	S
100 1001	I
100 1011	K

Abbildung 24: Kodierung des Wortes "Forensik" in ASCII- und Binär-Zeichen

Die Binärcodierung

Binär kodierte Daten stellen Informationen durch Binärzeichen dar und sind technisch einfach realisierbar Sie sind gut speicher- und übertragbar, sowie universell verwendbar, da jedes beliebige endliche Alphabet binär kodiert werden kann. Mit n Bits können 2^n verschiedene Bitmuster (Zustände) gebildet werden. Kontinuierliche Größen können durch Diskretisierung beliebig genau angenähert werden.

<u>Byte</u>

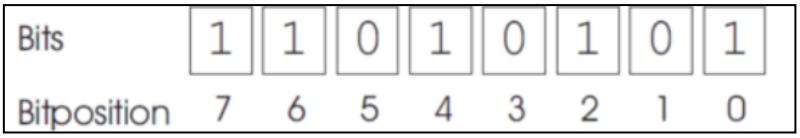


Abbildung 25: Darstellung der Bitpositionen (Zählweise)

Die Zusammenfassung von 8 Bit entspricht einem Byte und ist die Grundeinheit aller Datendarstellungen in Computern. 1 Byte entspricht 256 kodierbaren Zeichen. 2 Byte entsprechen 65.536 kodierbaren Zeichen. Dabei wird (wie in Abbildung 25 ersichtlich) von rechts nach links gezählt und (wie fast immer in der Informationstechnik) bei null begonnen.

Die Maßeinheiten für Datenmengen:

- 1 Kbyte (Kilobyte) = 2^{10} Byte = 1024 Byte
- 1 Mbyte (Megabyte) = 2^{20} Byte = 1.048.576 Byte
- 1 Gbyte (Gigabyte) = 2^{30} Byte = 1.073.741.824 Byte

Binärnotation

Bytes und Worte können dazu verwende werden, um Ganzzahlen beliebiger Größe zu repräsentieren. Bei der binären Kodierung wird lediglich eine andere Zahlenbasis verwendet. Das nächste höhere Bit ist immer um Faktor 2 erhöht gegenüber dem rechts von ihm stehenden Bit. Mit dieser Notation kann man die Ganzzahlen im Rechner darstellen.

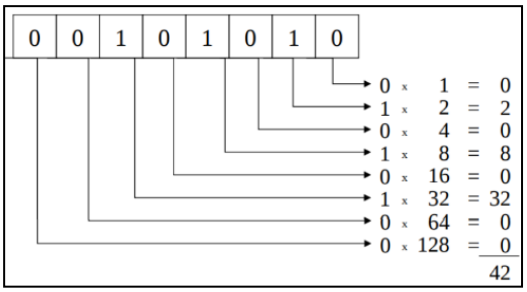


Abbildung 26: Aufschlüsselung der Binärnotation

In Abbildung 26 ist die Aufschlüsselung der Binärnotation gezeigt. Die Rechnung auf der linken Seite des Bildes besteht immer aus dem Wert des jeweiligen Bits (0 oder 1) und der Wertigkeit der Position. Diese Wertigkeit errechnet sich mit 2^n, wobei n für die Position steht. Beispielhaft für Bit 3 ergibt sich eine Wertigkeit von 2^3, also 8. Das 3. Bit ist mit 1 gesetzt, also fließt seine Wertigkeit in die Rechnung mit ein. Ebenso sind die Positionen 1 und 5 gesetzt. Wir erhalten demnach für das Aufaddieren der Wertigkeiten von Bit 1, 3 und 5 die Summe 42. Da die anderen Positionen mit 0 gesetzt sind, fließen sie nicht in die Summenbildung ein. Die Umrechnung die hier erfolgt, stellt das Byte in seiner dezimalen (unser vertrautes Zahlensystem) dar. Die dezimale Wertigkeit des Bytes 0010 1010 entspricht also 42.

Umrechnung Binärsystem ins Dezimalsystem

In Abbildung 27 ist das oben beschriebene Verfahren etwas aufegschlüsselter abgebildet. Es erfolgt die Umrechnung für das Byte 1011 1101:

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte: Bit	1	0	1	1	1	1	0	1
Wertigkeit	$2^7 = 128$	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
	1*128	0*64	1*32	1*16	1*8	1*4	0*2	1*1

Abbildung 27: Umrechnung vom Binärsystem ins Dezimalsystem

Durch das Aufaddieren der gesetzten Wertigkeiten erlangt man das Ergebnis: in diesem Fall 189.

Für die Notation der Zahlen, um Missverständnisse zu vermeiden, werden oft die Zahlensysteme am Ende der jeweiligen Zahlenfolgen vermerkt. In Abbildung 28 sind die Kennzeichnungen nochmal markiert.

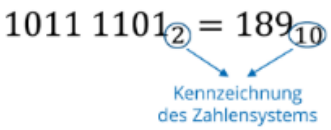


Abbildung 28: Kennzeichnung der Zahlensysteme

Umrechnung Dezimalsystem ins Binärsystem

Die Umrechnung kann auch in die andere Richtung erfolgen. Verfährt man von der höchsten Wertigkeit beginnend. In Abbildung 29 ist das Ergebnis der Umrechnung tabellarisch für die Dezimalzahlen 167 und 108 dargestellt. Man verfährt so: Es wird immer geprüft, ob die nächstgrößte Wertigkeit kleiner ist als die Zahl, die umgerechnet werden soll. Ist dies der Fall, setzt man an die Position der entsprechenden Wertigkeit die 1 und subtrahiert die Wertigkeit der umzurechnenden Zahl. Mit dem Rest wird dieser Ablauf wiederholt. Ist die Wertigkeit der Bitposition größer als die Zahl (oder der Rest), wird an der Bitposition die 0 eingetragen und mit der nächsten Wertigkeit weiter geprüft.

167

Wertigkeit	Enthalten?	Rest
128	**1**	39
64	**0**	39
32	**1**	7
16	**0**	7
8	**0**	7
4	**1**	3
2	**1**	1
1	**1**	0

108

Wertigkeit	Enthalten?	Rest
128	**0**	108
64	**1**	44
32	**1**	12
16	**0**	12
8	**1**	4
4	**1**	0
2	**0**	0
1	**0**	0

Abbildung 29: Umrechnung vom Dezimalsystem in das Binärsystem

2.1.2.2 Hexadezimales Zahlensystem

Die Binäre Darstellung von Daten fällt oft sehr lang aus. Daher wird alternativ gern die Hexadezimale (oder oktale) Darstellung verwendet.

Diese basiert auf 16 Zeichen, welche auch in Abbildung 30 zu sehen sind: 0 bis 9 und A bis F (stellvertretend für die Dezimalzahlen 10 bis 15). So kann ein Byte in 2 Stellen darstellbar gemacht werden. Dazu fasst man immer 4 Bit zu einer hexadezimalen Zahl zusammen. Die hexadezimale Darstellung wird in der Forensik unter anderem zur Bestimmung von Cluster und Sektorengrößen und deren Auslesung verwendet.

0	1	2	…	9	A	B	C	D	E	F
0	1	2		9	10	11	12	13	14	15

Abbildung 30: Zeichensatz des Hexadezimalen Zahlensystems

Die Aufschlüsselung der hexadezimalen Notation ist in Abbildung 31 dargestellt. Die Rechnung verhält sich ähnlich zu der des Binärsystems, mit dem Unterschied, dass 16 Möglichkeiten der Zeichenwahl bestehen, wodurch die Basis nicht 2, sondern 16 ist.

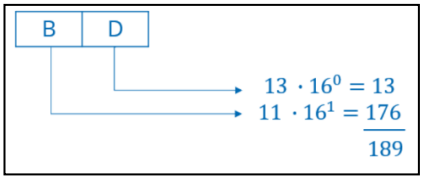


Abbildung 31: Aufschlüsselung der Hexadezimalnotation

2.1.2.3 Oktales Zahlensystem

Das oktale Zahlensystem basiert auf 8 Zeichen (0 bis 7). Es ähnelt ebenfalls dem binären, aber auch dem hexadezimalen System. Die Aufschlüsselung der oktalen Notation ist in Abbildung 32 dargestellt. Hier rechnet man mit der Basis 8.

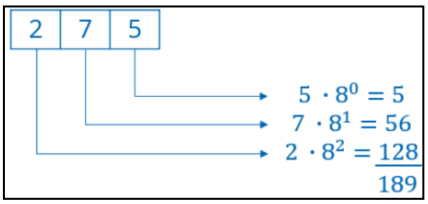


Abbildung 32: Aufschlüsselung der Oktalnotation

2.1.2.4 Grundformel der Umrechnung

Es existiert eine Grundformel, mit der sich von jedem Zahlensystem in das Dezimalsystem umrechnen lässt.

$$\Sigma\ Zeichen\ an\ der\ Position \cdot Basis\ des\ Zahlensystems^{Position}$$

Diese Formel ermöglicht es nicht nur, die Umrechnung in die bereits besprochenen Zahlensysteme zu realisieren, sondern theoretisch in alle beliebigen. Als Beispiel hier einmal die Darstellung der dezimalen Zahl 42 in allen relevanten Systemen:

- Dezimal: $4 \cdot 10^1 + 2 \cdot 10^0 = 42$
- Binär 101010: $1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 42$
- Oktal 52: $5 \cdot 8^1 + 2 \cdot 8^0 = 42$
- Hexadezimal 2A: $2 \cdot 16^1 + 10 \cdot 16^0 = 42$

<u>Umrechnung zwischen den Systemen</u>

Tipp: Die Umrechnung zwischen den Systemen ist in einigen Fällen komplizierter. Deshalb als Vorschlag (der Einfachheit halber) – erst die Umrechnung ins Binärsystem, von dort aus, ergeben sich die anderen Darstellungen einfacher. In Abbildung 33 ist die Umrechnung vom Binärsystem in das Oktal- und Hexadezimalsystem dargestellt. Anstatt direkt von oktal zu hexadezimal rechnen zu wollen, sollte der Umweg über das Binärsystem gegangen werden. Dieser Ansatz ist rein theoretisch. In der Praxis ist man selten damit konfrontiert.

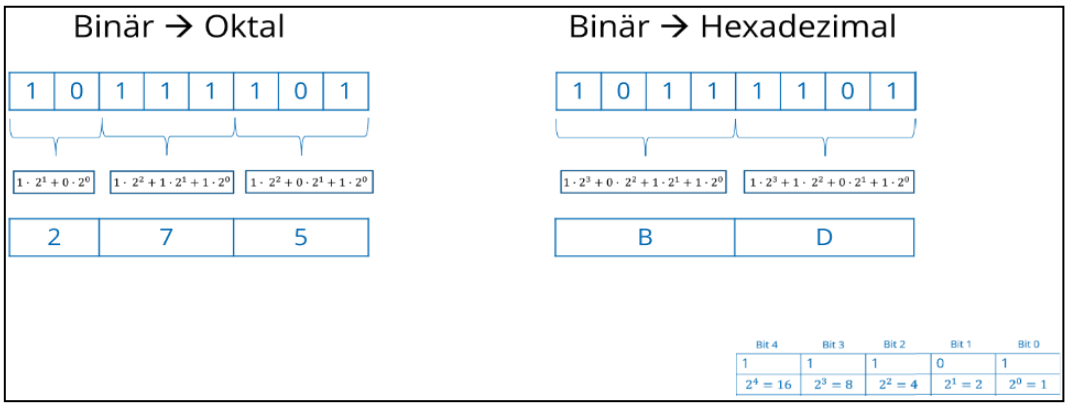


Abbildung 33: Darstellung über die Umrechnung vom Binärsystem in das Oktal- und Hexadezimalsystem

2.2 Kryptologie

Joseph Pulitzer, bekannter Journalist und Stifter des Pulitzer-Preises im Bereich Literatur und Journalismus, sagte einmal: „Es gibt kein Verbrechen, keinen Kniff, keinen Trick, keinen Schwindel, kein Laster, das nicht von Geheimhaltung lebt.“. Kryptologie beschreibt die Lehre von den Geheimschriften (griech: kryptos = verborgen, logos = Lehre) und ist die wissenschaftliche Disziplin, die sich mit der Verschlüsselung von Informationen, der Sicherstellung ihrer Vertraulichkeit und Integrität sowie der Entschlüsselung von verschlüsselten Daten befasst. Sie umfasst zwei Hauptbereiche: Kryptografie und Kryptoanalyse.

Kryptografie beschäftigt sich mit der Entwicklung von Verschlüsselungstechniken und -algorithmen, um Daten vor unbefugtem Zugriff zu schützen. Ziel ist es, Informationen so zu verschlüsseln, dass sie nur für autorisierte Empfänger lesbar sind. Verschiedene Verschlüsselungsmethoden werden verwendet, darunter symmetrische Verschlüsselung, bei der derselbe Schlüssel zum Verschlüsseln und Entschlüsseln verwendet wird, und asymmetrische Verschlüsselung, bei der unterschiedliche Schlüssel für Verschlüsselung und Entschlüsselung verwendet werden.

Kryptoanalyse befasst sich mit der Analyse von verschlüsselten Daten und der Suche nach Schwachstellen in Verschlüsselungssystemen, um verschlüsselte Informationen ohne den richtigen Schlüssel zu entschlüsseln. Kryptoanalytiker verwenden mathematische und algorithmische Techniken, um Verschlüsselungsverfahren zu analysieren, Schwachstellen aufzudecken und effektive Angriffe zu entwickeln.

Die Kryptografie erfüllt mehrere grundlegende Aufgaben:

- Geheimhaltung (Datenschutz): Eine der wichtigsten Aufgaben der Kryptografie ist es, die Vertraulichkeit von Informationen zu gewährleisten, indem sichergestellt wird, dass nur autorisierte Parteien die Nachricht lesen können. Dies wird durch Verschlüsselungstechniken erreicht, die es unbefugten Personen sehr schwer machen oder sogar unmöglich machen, den Inhalt der Nachricht zu entschlüsseln.
- Authentifizierung: Kryptografie wird auch verwendet, um die Identität von Personen oder Kommunikationsteilnehmern zu überprüfen und zu bestätigen. Dies ermöglicht es, sicherzustellen, dass die Kommunikation mit der beabsichtigten Partei erfolgt und nicht von einer unbefugten Person oder einem falschen Teilnehmer stammt.
- Integrität: Eine weitere wichtige Aufgabe der Kryptografie ist es, die Integrität von Daten sicherzustellen, indem sichergestellt wird, dass Nachrichten während der Übertragung oder Speicherung nicht unbemerkt verändert wurden. Dies wird durch die Verwendung von Integritätsprüfungen und kryptografischen Hash-Funktionen erreicht, die sicherstellen, dass die Nachricht unverändert ist.
- Anonymität: Kryptografie kann auch dazu verwendet werden, die Anonymität von Benutzern oder Kommunikationsteilnehmern zu gewährleisten, indem verschlüsselte Kommunikationen oder Transaktionen ohne Offenlegung der Identität durchgeführt werden können. Dies kann beispielsweise in digitalen Währungen oder bei der sicheren Kommunikation über anonyme Netzwerke wie das Tor-Netzwerk der Fall sein.

2.2.1 Historisches Beispiel

Ein historisches Beispiel aus dem 5. Jahrhundert vor Christus ist die Verwendung der sogenannten "Skytale" (auch "Scytale" geschrieben) als Verschlüsselungsmethode im antiken Griechenland. Die Skytale war ein zylinderförmiges Werkzeug, das aus einem dünnen Streifen aus Leder oder Pergament bestand, der um einen festen Stab gewickelt wurde.

Die Methode funktionierte folgendermaßen: Der Absender wickelte den Streifen um die Skytale und schrieb seine Nachricht längs über den Streifen. Wenn der Streifen dann abgewickelt wurde, erschien die Nachricht jedoch als scheinbar sinnlose Reihe von Buchstaben, da sie ohne den richtigen "Entschlüsselungsstab" nicht verständlich war. Ein Beispiel für eine Nachricht in Kombination mit dem passenden Entschlüsselungsstab ist in Abbildung 34 zu sehen.

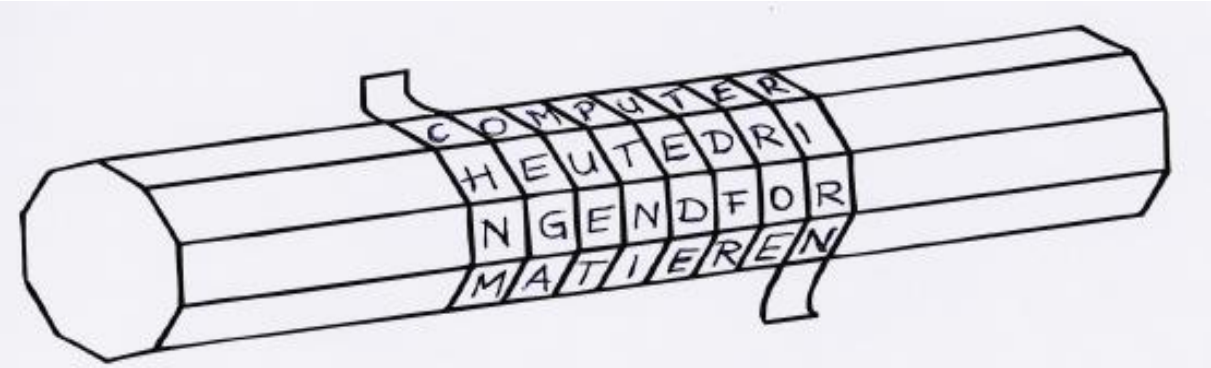


Abbildung 34: Skytale -- Entschlüsselungsstab, umwickelt mit Nachrichtenstreifen, Inhalt der Nachricht erkennbar

Der Empfänger besaß einen Stab mit dem gleichen Durchmesser wie der des Absenders. Wenn er den Streifen um seinen eigenen Stab wickelte, konnten die Buchstaben wieder in der richtigen Reihenfolge gelesen werden und die Nachricht entschlüsselt werden. Dadurch war die Skytale eine einfache, aber effektive Methode der Verschlüsselung und war besonders bei militärischen Kommunikationen beliebt, da sie schnell und einfach anzuwenden war und ohne spezielle Kenntnisse oder Werkzeuge auskommen konnte.

Ein weiteres historisches Beispiel für Verschlüsselung ist die Caesar-Chiffre, benannt nach dem römischen Kaiser Julius Caesar, der sie angeblich zur Kommunikation mit seinen Generälen verwendete. Die Caesar-Chiffre ist eine der ältesten bekannten Verschlüsselungsmethoden und basiert auf einer einfachen Verschiebung des Alphabets.

Bei der Caesar-Chiffre wird jeder Buchstabe im Klartext um eine feste Anzahl von Positionen im Alphabet verschoben. Zum Beispiel könnte die Verschiebung um drei Positionen nach rechts erfolgen, wobei der Buchstabe A zu D, B zu E usw. wird, wie in Abbildung 35 dargestellt. Wenn das Ende des Alphabets erreicht wird, wird die Zählung wieder von vorne begonnen.

Klartext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Abbildung 35: Caesar-Chiffre -- Verschiebung um den Faktor 3

Um eine Nachricht zu verschlüsseln, wird jeder Buchstabe entsprechend der Verschiebung ersetzt. Um die verschlüsselte Nachricht zu entschlüsseln, wird jeder Buchstabe um die gleiche Anzahl von Positionen verschoben, jedoch in die entgegengesetzte Richtung.

Obwohl die Caesar-Chiffre einfach zu verstehen und anzuwenden ist, ist sie nicht besonders sicher, da es nur 25 mögliche Verschiebungen gibt, was relativ einfach zu brechen ist, insbesondere durch statistische Analysen der Buchstabenhäufigkeiten (Häufigkeitsanalyse) in der Sprache des Klartexts. Dennoch diente die Caesar-Chiffre als Grundlage für viele weitere Verschlüsselungstechniken und illustriert das grundlegende Konzept der Verschiebungsalgorithmen in der Kryptografie.

2.2.2 Terminologie

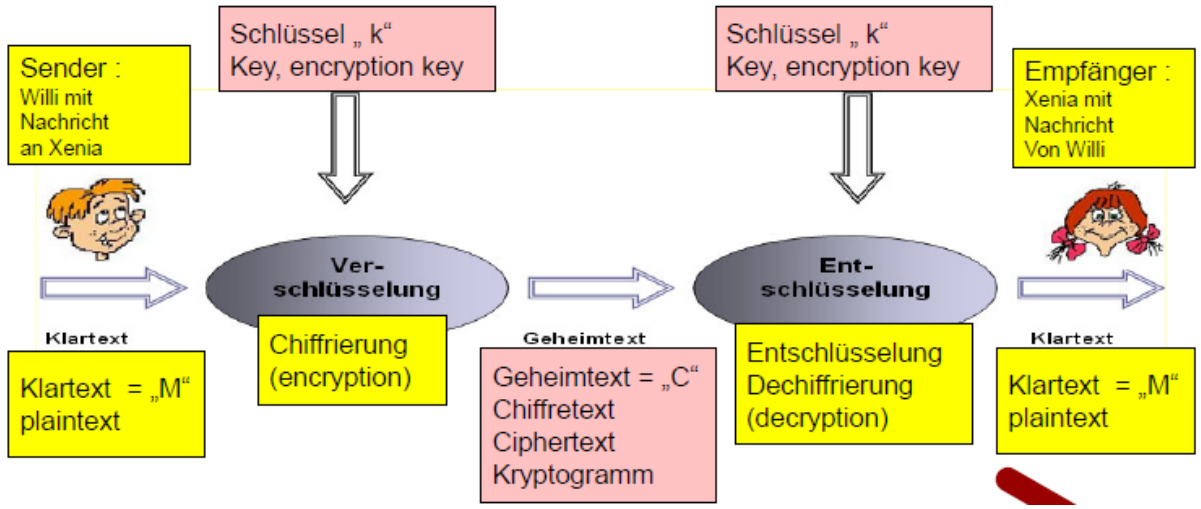


Abbildung 36: Terminologie und Ablauf eines kryptologischen Systems

Abbildung 36 stellt den Ablauf eines kryptologischen Systems mit der Verschlüsselung und Endschlüsselung dar. Hier existieren verschiedene Schlüsselbegriffe, die die Aspekte der Verschlüsselung und Entschlüsselung von Nachrichten beschreiben:

- Sender: Die Person oder Entität, die die Nachricht verschickt.
- Empfänger: Die Person oder Entität, die die verschlüsselte Nachricht empfängt und entschlüsselt.
- Klartext: Die ursprüngliche Nachricht oder Information, die verschlüsselt werden soll.
- Geheimtext: Die verschlüsselte Form des Klartexts, die an den Empfänger gesendet wird.
- Verschlüsselung: Der Prozess der Umwandlung eines Klartexts in einen Geheimtext unter Verwendung eines Verschlüsselungsalgorithmus und eines Schlüssels.
- Entschlüsselung: Der Prozess der Umwandlung eines Geheimtexts in Klartext unter Verwendung eines Entschlüsselungsalgorithmus und eines Schlüssels.
- Schlüssel: Ein Parameter, der vom Verschlüsselungsalgorithmus verwendet wird, um die Transformation des Klartexts in Geheimtext (und umgekehrt) zu steuern. Der Schlüssel ist eine entscheidende Komponente des kryptografischen Systems und wird sowohl vom Sender zum Verschlüsseln als auch vom Empfänger zum Entschlüsseln verwendet.

2.2.3 Verschlüsselungsverfahren

Grundsätzlich wird zwischen symmetrischer und asymmetrischer Verschlüsselung unterschieden.

Symmetrische Verschlüsselung

Bei Symmetrischer Verschlüsselung wird der gleiche Schlüssel für die Verschlüsselung als auch die Entschlüsselung verwendet. Ein typisches Beispiel ist die Verschlüsselung eines Datenträgers. Hier wird beim Einrichten der Verschlüsselung der Schlüssel meist als Passwort festgelegt und anschließend bei jeder Entschlüsselung verwendet. Der Schlüssel darf nur den entsprechenden Parteien bekannt sein. Ist der Schlüssel Dritten zugänglich, ist die Entschlüsselung auch ihnen möglich. Symmetrische Verschlüsselung lässt sich bildlich, wie ein Zahlenschloss vorstellen. Jeder, der die richtige Zahlenkombination kennt, kann das Schloss öffnen. Als Algorithmus kommt bei symmetrischer Verschlüsselung meist der Advanced Encryption Standard (AES) zum Einsatz. AES lässt sich bei einem ausreichend sicher gewählten Schlüssel nicht entschlüsseln.

Man unterscheidet zwei Unterformen der symmetrischen Verschlüsselung: Stromverschlüsselung und Blockverschlüsselung.

Bei der Stromverschlüsselung werden Daten kontinuierlich oder stromartig verschlüsselt. Das bedeutet, dass jeder Datenstrom in kleine Einheiten aufgeteilt wird, und jeder dieser Datenbits oder Bytes einzeln mit einem Schlüssel verschlüsselt wird. Typischerweise wird bei der Stromverschlüsselung ein Stromchiffrier-Algorithmus wie der RC4-Algorithmus verwendet. Dieser Algorithmus erzeugt eine Schlüsselstromfolge, die dann mit den Daten kombiniert wird, um den verschlüsselten Datenstrom zu erzeugen. Stromverschlüsselung eignet sich gut für die Verschlüsselung von Daten in Echtzeit, wie z. B. bei der Verschlüsselung von VoIP-Gesprächen oder bei der sicheren Datenübertragung über Netzwerke.

Bei der Blockverschlüsselung werden Daten in fest definierte Blöcke aufgeteilt, die jeweils eine bestimmte Anzahl von Bits oder Bytes enthalten. Jeder Block wird dann mit einem Schlüssel verschlüsselt, wobei ein spezieller Verschlüsselungsalgorithmus wie AES (Advanced Encryption Standard) oder DES (Data Encryption Standard) verwendet wird. Im Gegensatz zur Stromverschlüsselung werden bei der Blockverschlüsselung die Daten in diskreten Blöcken verschlüsselt, was zu einem klar strukturierten und deterministischen Prozess führt.Blockverschlüsselung eignet sich gut für die Verschlüsselung von Daten in Ruhe, wie z. B. das Verschlüsseln von Dateien auf einer Festplatte oder das sichere Speichern von Daten in einer Datenbank.

Asymmetrische Verschlüsselung

m Gegensatz zur symmetrischen Verschlüsselung, verwendet die asymmetrische Verschlüsselung ein Schlüsselpaar. Dieses besteht aus einem öffentlichen Schlüssel, dem Public-Key, und einem privaten Schlüssel, dem Private-Key. Der öffentliche Schlüssel kann, wie der Name verrät, jedem in der Öffentlichkeit mitgeteilt werden. Er ist nicht geheim. Dagegen darf der private Schlüssel nie preisgegeben werden. Dieser sollte das benutzte Endgerät nie verlassen und auch nur von berechtigten Programmen genutzt werden dürfen.

Asymmetrische Verschlüsselung lässt sich vergleichen mit der Nutzung eines Vorhängeschlosses. Das Vorhängeschloss (Public-Key) selbst kann ohne Bedenken jedem übergeben werden. Damit ist diese Person in der Lage etwas zu verschließen (verschlüsseln). Das Verschlossene (verschlüsselte

Informationen) lässt sich nun jedoch erst durch den passenden Schlüssel (Private-Key) öffnen. Da diesen nur der Empfänger hat, sind die Informationen gegen Dritte gesichert.

Das asymmetrische Verfahren hat den großen Vorteil, dass im Vorfeld kein Schlüsselaustausch stattfinden muss. Erst bei Beginn einer Verbindung wird der öffentliche Schlüssel angefordert. Um die Herkunft des Public-Keys zu gewährleisten, wird dieser häufig durch eine übergeordnete Vertrauensstelle signiert.

Die am häufigsten genutzten asymmetrischen Verschlüsselungsverfahren sind Rivest Shamir Adleman (RSA) und Elliptic Curve Diffie-Hellman (ECDH). RSA basiert auf der Schwierigkeit ein Produkt in seine Primfaktoren zu zerlegen. ECDH basiert auf der Komplexität einen diskreten Logarithmus zu errechnen und arbeitet im mathematischen Ring der elliptischen Kurven.

Diffie-Hellman-Schlüsselaustausch

Der Diffie-Hellman-Schlüsselaustausch ist ein Verfahren in der Kryptografie, das es ermöglicht, einen symmetrischen Schlüssel sicher über eine asymmetrische Verschlüsselung zwischen zwei Kommunikationspartnern auszutauschen. Dabei wird der Schlüssel für die Verschlüsselung der Nachrichten nie direkt ausgetauscht, sondern von den Kommunikationspartnern auf beiden Seiten errechnet, indem sie asymmetrische Schlüssel austauschen und kombinieren. Der Vorgang ist in Abbildung 37 anschaulich dargestellt.

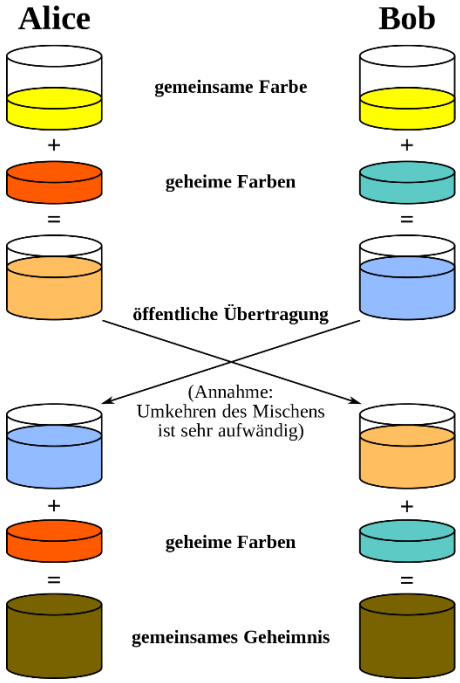


Abbildung 37: Prinzip des Schlüsselaustauschs nach Diffie-Hellman

Dieses Verfahren wird häufig in Kombination mit anderen Sicherheitsmechanismen verwendet, um sicherzustellen, dass die Datenübertragung zwischen den Parteien sicher ist. Die Verschlüsselung wird aufgebaut, bevor Daten übertragen werden, um sicherzustellen, dass die Kommunikation geschützt ist.

Ein bekanntes Beispiel für die Anwendung des Diffie-Hellman-Schlüsselaustauschs ist das Transport Layer Security (TLS) Protokoll, das auf Anwendungsbasis arbeitet. Bei der Einrichtung einer sicheren Verbindung zwischen zwei Systemen, wie zum Beispiel einem Webbrowser und einem Server, wird ein verschlüsselter Kanal aufgebaut. Dies geschieht durch einen TLS-Handshake (Abbildung 38), bei dem

die Kommunikationspartner die Protokollversion vereinbaren, die kryptografischen Verfahren abgleichen, die TLS-Zertifikate prüfen und einen Session-Schlüssel erzeugen.

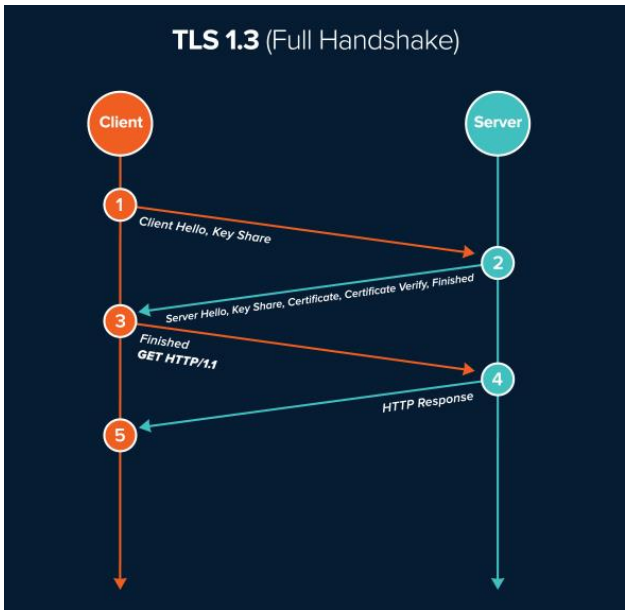


Abbildung 38: TLS-Handshake zum Aufbau einer abgesicherten Verbindung

In Webbrowsern wird TLS häufig für das Hypertext Transfer Protocol Secure (HTTPS) verwendet, um eine sichere Datenübertragung und Datenverschlüsselung zwischen dem Benutzer und dem Server zu gewährleisten. Durch den Einsatz von TLS wird vertrauliche Information geschützt und die Integrität der Daten sichergestellt.

2.2.4 Steganografie

Im Vergleich zur Kryptografie werden Daten bei der Steganografie nicht durch Verschlüsselung unkenntlich gemacht, sondern versteckt. Beide Disziplinen teilen jedoch das gleiche Ziel: Informationen nur einem definierten Empfänger oder einer ausgewählten Entität zugänglich machen.

Das Wort Steganografie beschreibt die Kunst, Inhalte versteckt zu schreiben und setzt sich aus den griechischen Wörtern steganós „bedeckt“ und gráphein „schreiben“ zusammen. Um eine höhere Sicherheit der Geheimhaltung zu gewährleisten, können sensible Daten erst verschlüsselt und dann versteckt werden. Das sichtbare Übertragen verschlüsselter Inhalte kann verdächtig sein und potenzielle Angreifer können sich explizit auf die chiffrierten Daten konzentrieren. Beim Einbetten von geheimen Daten in unauffällige Dateien erzeugt man ein Steganogramm. Im Idealfall weiß niemand, außer dem Sender und dem Empfänger, um die Existenz der versteckten Informationen. Ein gezieltes Angreifen ist nur schwer möglich.

Ein klassisches Beispiel für Steganografie ist in Abbildung 39 zu sehen. Auf den ersten Blick ist es eine normale Zeichnung des San Antonio Flusses in Texas, USA. Die Geheimnachricht ist im Morsecode in den Grashalmen dargestellt. Die kurzen und langen Halme auf der linken Seite des Flusses und entlang des Flusses im Vordergrund stellen die Nachricht dar. Das Bild könnte somit verbreitet werden, ohne dass unbefugte Personen die Informationen zu entnehmen wüssten.

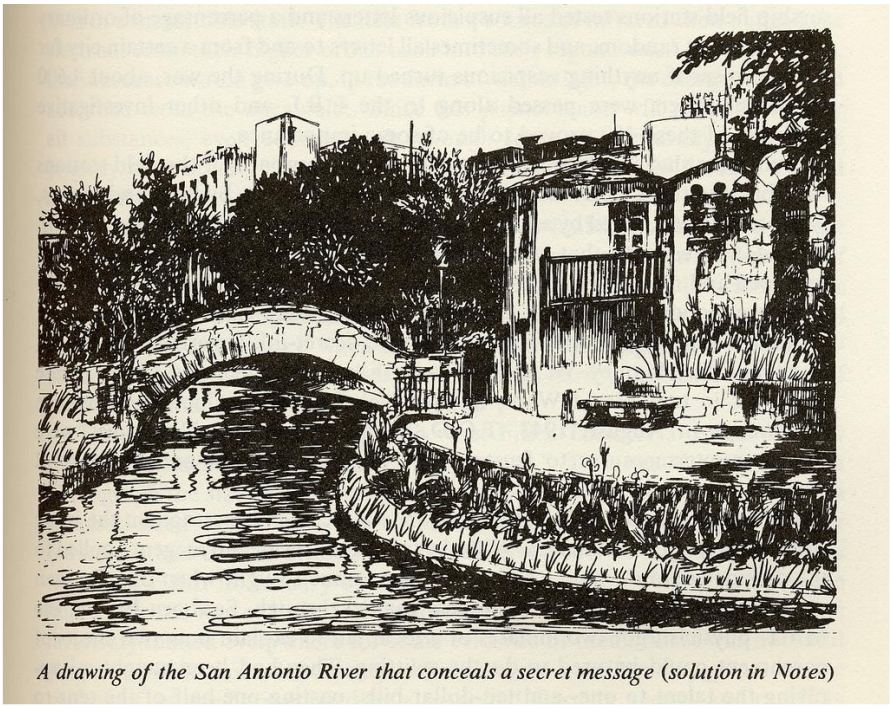


Abbildung 39: San Antonio River mit versteckter Nachricht

Das steganografische System ist in Abbildung 40 dargestellt. Durch die Eingabe einer Trägerdatei (X) und einem Geheimtext (M) in einen Steganografie Kodierer wird mittels einer steganografischen Funktion ein Steganogramm erzeugt und ausgegeben. Dieses kann über beliebige Kommunikationskanäle verbreitet werden. Auf der Empfängerseite kann der Geheimtext (M) durch einen Steganografie Dekodierer extrahiert werden. Ein Schlüssel (K) kann während der Kodierung verwendet werden, ist dann aber zur Dekodierung zwingend erforderlich.

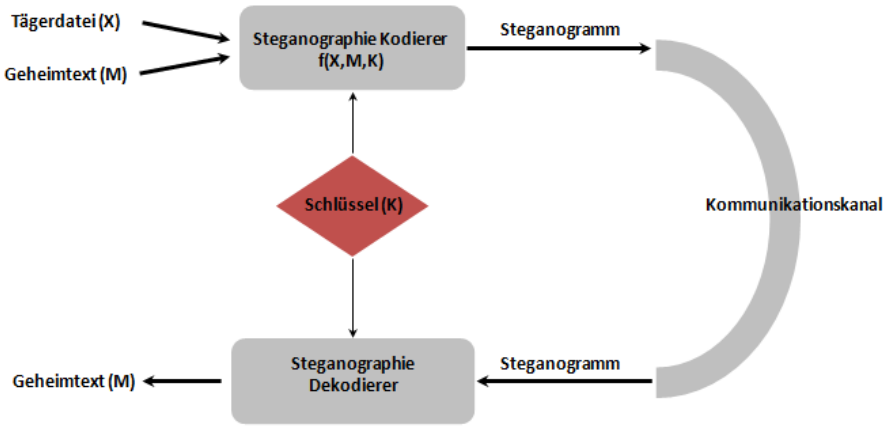


Abbildung 40: Steganografiesystem, Terminologie und Ablauf

Es gibt die verschiedensten Algorithmen und Ideen, wie das Verstecken von Daten realisiert werden kann. Das einfachste Beispiel ist der EndOfFile-Algorithmus (EOF). Er ist so konzipiert, dass der Geheimtext einfach an das Ende einer Datei geschrieben wird. Durch das Betrachten der Datei in einem Hexadezimaleditor, beispielsweise HxD oder Bless Hex Editor, kann man die versteckten Informationen sehen. Die Daten sind dadurch sowohl detektierbar als auch komplett auslesbar. Ein potenzieller Angreifer hätte mit wenig Aufwand nicht nur die Bestätigung, dass es sich um ein Steganogramm handelt, sondern kann auch die gesamten geheimen Daten problemlos extrahieren.

Um Objekte oder Daten sicherer zu verstecken, gibt es grundlegend drei Möglichkeiten: Filterung, Maskierung, Verteilung. Bei der Filterung wird ein Trägermedium mit Hilfe eines Algorithmus überprüft, um die Stellen zu finden, an denen Veränderungen am wenigsten auffallen. Beim Maskieren wird lediglich eine Maske verwendet, um Informationen unsichtbar zu machen. Man könnte einen Text über ein Bild legen und die Transparenz so weit erhöhen, bis nur noch das Bild sichtbar ist. Das Bild stellt in diesem Fall eine Maske dar. Bei einer Verteilung werden die Daten verstreut, sodass sie nicht sequenziell abgelegt werden. Diese drei Prinzipien werden in vielen Algorithmen und Methoden aufgegriffen und modifiziert.

Eine der wichtigsten Grundmethoden zur Durchführung ist das Einbetten der Daten in die Least Significant Bits (LSB). Daten in das letzte Bit der Bytes einer Trägerdatei zu injizieren, stellt dabei die Grundlage dar. Varianz für diese Methode bieten dann beispielsweise die Reihenfolge oder das Format der einzubettenden Daten. In Abbildung 41 wird die LSB-Methode anhand der Pixelwerte eines Bildes erklärt

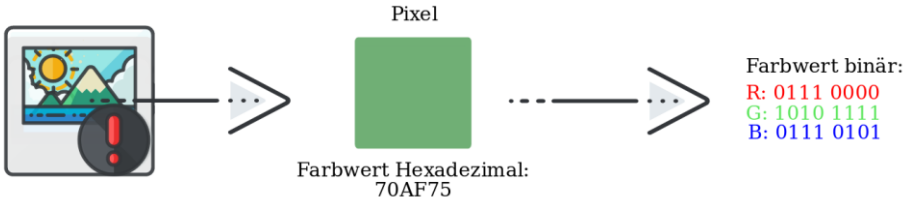


Abbildung 41: Farbwerte eines Pixels: Ein grüner Pixel aus dem Bild wird sich angesehen. Die

Ein Pixel besteht im RGB-Raum aus drei Werten, die jeweils ein Byte groß sind. In Abbildung 41 wird ein grüner Pixel des Farbwertes „70AF75“ in seine drei Farbkomponenten, Rot, Grün und Blau, zerlegt. Das jeweils letzte Bit der einzelnen Farbkomponenten trägt zur endgültigen Farbe am wenigsten bei, hat also den geringsten Informationsgehalt.

Im Zuge der LSB-Methode wird jeweils das letzte Bit eines jeden Bytes des Trägerbildes durch ein Bit der zu versteckenden Daten ersetzt. Diese Manipulation wird in Abbildung 42 verdeutlicht:

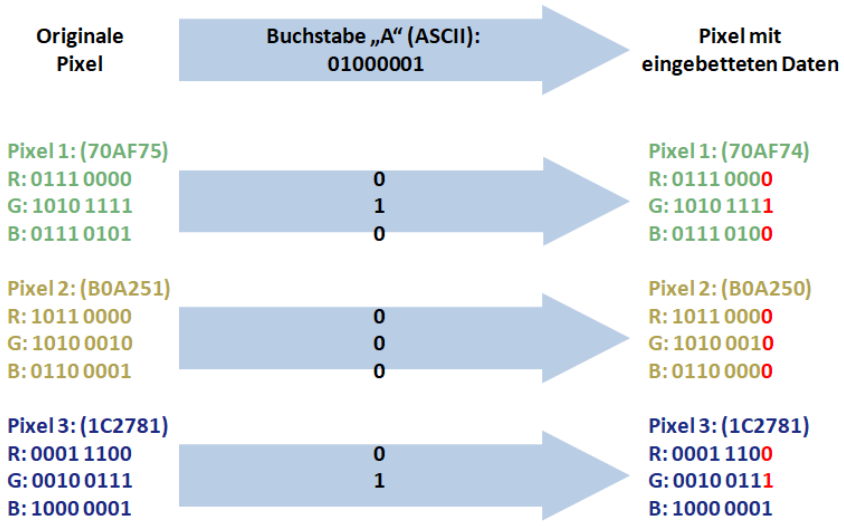


Abbildung 42: Schematische Darstellung der Einbettung des Buchstabens „A“ in drei Pixel eines Trägerbildes

Der grüne Pixel aus Abbildung 41 und zwei weitere beliebig gewählte Pixel dienen als Trägerpixel für den Buchstaben „A“. Dabei wird die binäre Schreibweise des Buchstabens, also die Bitfolge in das letzte Bit eines jeden Farbkanals eingebettet. Die entstandenen neuen Pixelwerte sind auf der rechten Seite

zu sehen. Dadurch erfolgt keine für den Menschen wahrnehmbare Veränderung im Bild, so ist auch die Farbveränderung in Abbildung 42 nicht erkennbar. Die letzten Bits können jedoch extrahiert und wieder zu den originalen Daten zusammengesetzt werden.

Für die LSB-Methode gibt es verschiedene Ergänzungen bzw. Variationen. So werden nicht immer die originalen Daten in das LSB eingebettet, beispielsweise, wenn vorher die Verschlüsselung der Daten stattfand. Auch die Reihenfolge und der Anfangspunkt können variieren. Der LSB-Algorithmus funktioniert nicht nur mit Bildern als Trägermedien. Es können zum Beispiel auch in Audiodateien die letzten Bits der Frequenzdaten ersetzt werden. Unabhängig vom Trägermedium werden durch den LSB-Algorithmus die niederwertigsten Bits ersetzt. Das Bit-Selektions-Level bezeichnet die Anzahl der zu ersetzenden Bits und ist bei einigen Tools manuell einstellbar. Das letzte Bit macht nur weniger als 0,4 % des Informationsgehalts eines Bytes aus, die letzten zwei Bits etwa 1 %. In Abbildung 43 sind Steganogramme mit verschiedene Bit-Selektions-Level dargestellt. Sowohl das Trägerbild als auch die eingebettete (versteckte) Datei sind gleich.

Abbildung 43: Steanogramme mit unterschiedlichem Bit-Selektions-Level: (a) Selektions-Level 1, (b) Selektions-Level 2, (c) Selektions-Level 3, (d) Selektions-Level 4 mit gekennzeichneten Artefakten

Während im ersten Bild (a) nur das letzte, also ein Bit pro Byte ersetzt wurde, sind im vierten Bild (d) die hinteren vier Bits der Trägerdateibytes durch die vorderen vier Bits der Geheimdateibytes ausgetauscht worden. Im zweiten und dritten Bild wurden entsprechend der Level die jeweilige Anzahl an Bits ausgetauscht. Vergleicht man nun Bild (a) mit Bild (b) können mit bloßem Auge keine Unterschiede festgestellt werden. Im Gegensatz dazu sind im Bild (d) deutliche Unterschiede in der Qualität wahrnehmbar. Beispielsweise im Bereich der vom Auto aufgewirbelten Staubwolke sind weniger Details erkennbar, was durch eine flächenhaft gleiche Farbgebung auffällt. Die Artefakte sind im Bild mit roten Kreisen gekennzeichnet. Bei der visuellen Untersuchung solcher Bilder sind sichtbare Artefakte, wie im Bild (d), ausschlaggebend für eine gezielte Steganalyse.

Steganografie kann in verschiedenen Medien umgesetzt werden. Dazu gehört beispielsweise Audiosteganografie, Videosteganografie und auch Netzwerkprotokollsteganografie.

2.3 Hash-Werte

Hashwert ist ein Begriff aus der Computertechnik im Bereich der Kryptologie und bezeichnet einen alphanumerischen Wert, der durch eine besondere Form der Hashfunktion erzeugt wird. Er dient in der Forensik als eindeutige Prüfsumme des Ist-Zustandes des Datenträgers.

„Hash-Funktionen berechnen aus einer gegebenen Nachricht eine Bitfolge mit fester Länge, die ein Repräsentant der Nachricht ist. Der so erzeugte Hash-Wert kann als ein Fingerabdruck der Nachricht betrachtet werden.“ [7, S. 335]

Aus digitalen Daten wird mittels einer Hash-Funktion ein Hash-Wert erzeugt. Dabei ist die Hash-Funktion oder Scatter-Funktion eine Abbildung, die eine große Eingabemenge, die Schlüssel, auf eine kleinere Zielmenge, die Hash-Werte, abbildet. Es existieren verschiedene Hash-Algorithmen:

- MD2 - Message Digest 2 (128 Bit)
- MD4 - Message Digest 4 (128 Bit)
- MD5 - Message Digest 5 (128 Bit)
- RIPEMD
- RIPEMD-160
- Tiger
- WHIRLPOOL
- SHA-1 160 Bit
- SHA-2 224, 256, 384 and 512 Bit
- SHA-3 224, 256, 384 and 512 Bit

Kryptografische Hash-Funktionen bilden einen eigenen Bereich der Kryptografie. An ihrer Entwicklung waren oft bekannte Kryptografen beteiligt, die aus anderen kryptografischen Verfahren bekannt sind. Hash-Funktionen haben bestimmt Eigenschaften, die sie effizient für den forensischen Anwendungsbereich machen [7, S. 345]:

- **Beliebige Nachrichtenlänge**: Eine Hash-Funktion kann Nachrichten beliebiger Länge verarbeiten
- **Feste Ausgangslänge**: Eine Hash-Funktion erzeugt Hash-Werte fester Länge
- **Effizienz**: Eine Hash-Funktion kann einfach berechnet werden
- **Einwegfunktion**: Es ist rechnerisch unmöglich, für einen gegebenen Ausgangswert (Hash) den Eingangswert zu finden
- **Kollisionsresistenz:** Es ist rechentechnisch unmöglich, zwei Eingangswerte zu finden, für die die Hash-Werte gleich sind

Je besser die Eigenschaften durch einen bestimmten Hash-Algorithmus erfüllt sind, desto sicherer ist er. Eine weitere wichtige Eigenschaft, die besonders für die Datenträgersicherung von Bedeutung ist, ist die Reaktion der Hash-Funktion auf sehr ähnliche Werte. Hierzu ein Beispiel:

Der Satz „Tim studiert an der Hochschule Mittweida.“ Hat den MD5-Hash-Wert „f8461354aa8060c8b0959caf438c38d8“. Wenn jetzt nur ein einziger Buchstabe verändert wird, beispielsweise zu „Tom studiert an der Hochschule Mittweida.“ Verändert sich der Hash-Wert komplett: „c12e6dbf214e2d7eb24e1530bba727fa“. Im Gegenzug können zwei sehr ähnliche Hash-Werte aus völlig unterschiedlichen Eingaben entstanden sein. Wichtig ist diese Eigenschaft, um auch kleinste Veränderungen aufzuzeigen.

2.4 Rechnerarchitektur

Ein Computer hat verschiedene Komponenten, die in ihrem Zusammenspiel die Nutzung eines Gerätes realisieren. Zu den wichtigsten Komponenten gehören folgende:

- Processor (CPU – Central Processing Unit)
- Mainboard (Hauptplatine)
- Optisches Laufwerk (optional)
- Festplatte
- Hauptspeicher
- Display/Monitor
- Maus, Tastatur

Es gibt noch weitere Gräte und Komponenten, die mit Computersystemen einhergehen. Um das Zusammenspiel zu verstehen, muss man erst die allgemeinen Grundprinzipien beleuchten. Hierbei ist eine der wichtigsten Grundlagen die Von-Neumann-Architektur.

2.4.1 Von-Neumann-Architektur

Die Von-Neumann-Architektur beschreibt folgende Grundprinzipien: Ein Rechner besteht aus Hauptspeicher, Steuereinheit, Recheneinheit, Ein- und Ausgabe-Einheiten und Langzeitspeicher. Es existiert ein sogenannter Systembus, der die Einheiten miteinander verbindet. Dabei existiert zusätzlich eine Programmsteuerung. Diese ist eine Rechnerstruktur, die unabhängig von konkreten Aufgaben arbeitet.

Das Verarbeitungsprinzip ist dabei immer gleich: Der Hauptspeicher besteht aus fortlaufend nummerierten Speicherplätzen, die je 1 Byte groß sind. Eine Adresse ist dann die Nummer eines Speicherplatzes. Ein Programm ist eine Folge von Maschinen-Befehlen, die sequenziell (der Reihe nach) ausgeführt werden. Die Abweichung von der sequenziellen Programm-Ausführung ist durch Sprungbefehle möglich, dadurch wird die Programm-Ausführung an anderer Stelle fortgesetzt. Daten und Programme werden binär codiert, Zahlen werden dual dargestellt.

Die Komponenten der Von-Neumann-Architektur werden nun durch die Hardware eines Rechners realisiert.

2.4.2 Prozessor

Der Prozessor wird auch als Central Processing Unit (CPU) bezeichnet. Er bearbeitet Daten, z.B. mit arithmetischen oder logischen Verknüpfungen und regelt das Zusammenspiel aller Bauteile des Motherboards. Der Prozessor setzt sich dabei aus einem Steuerwerk, das alle Abläufe im System steuert, und einem Rechenwerk, welches verschiedenartige arithmetische und logische Operationen so durchführt, wie es vom Steuerwerk vorgegeben wird, zusammen. Zusätzlich beinhaltet er weitere wichtige Komponenten wie das Bus Interface (Busschnittstelle), die AGU (Address Generation Unit, Adressierungseinheit) und das Register (Speicherstellen im Prozessor, mit denen der Prozessor besonders schnell und flexibel arbeiten kann). In Abbildung 44 ist der Aufbau eines Prozessors dargestellt.

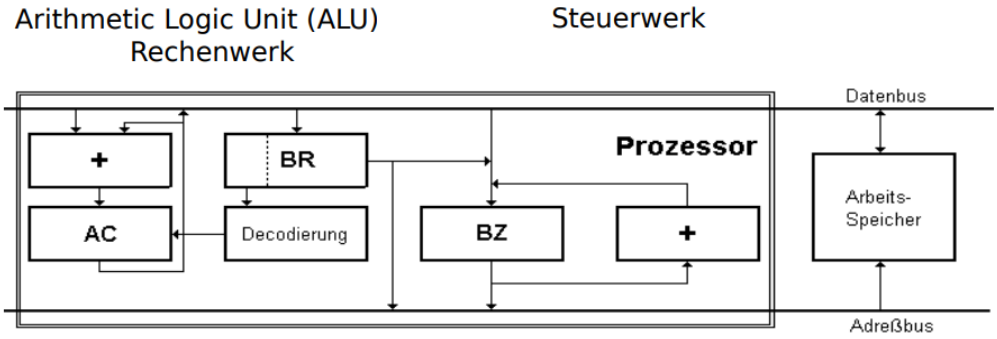


Abbildung 44: Aufbau eines Prozessors

In der Abbildung sind neben den angegebenen Komponenten noch der Akkumulator (AC) für kumulative Additionen im Rechenwerk, der Befehlszähler (BZ) und das Befehlsregister (BR) aufgeführt.

Ein Prozessor hat einen bestimmten Befehlssatz. Dieser ist die Menge der für ihn verständlichen Maschinenbefehle. Typische Maschinebefehle sind:

- Arithmetische Operationen (Addition, Subtraktion, Multiplikation, Division, ...)
- Logische Operationen (AND, OR, NOT, ...)
- Transport zwischen Speicherplätzen
- Ein- und Ausgabeoperationen
- Testen, Setzen, Löschen einzelner Bits in Operanden
- Adressoperationen: Sprünge zu anderen Befehlen

Für Prozessoren wurden im Laufe der Zeit verschiedene Methoden zur Leistungssteigerung entwickelt. Dazu zählen die Umsetzung durch mehrere Kerne und Hyperthreading. Mehrere Kerne realisieren die Multitasking-Fähigkeit des Prozessors. Ein Kern kann immer nur einen Befehl verarbeiten. Je mehr Kerne eingesetzt werden, desto mehr Befehle können zeitgleich verarbeitet werden. Während dies die physische Form der Leistungssteigerung darstellt, befasst sich das Hyperthreading mit der Aufteilung des Prozessors in logische, virtuelle Kerne (nicht physisch). Dies erhöht ebenfalls die Leistung. Auch die Kombination von Kernen und Hyperthreading möglich. Beispielsweise arbeiten 8 Kerne mit aktiviertem Hyperthreading wie 16 Kerne (virtuell).

2.4.3 Bussystem und Arbeitsspeicher

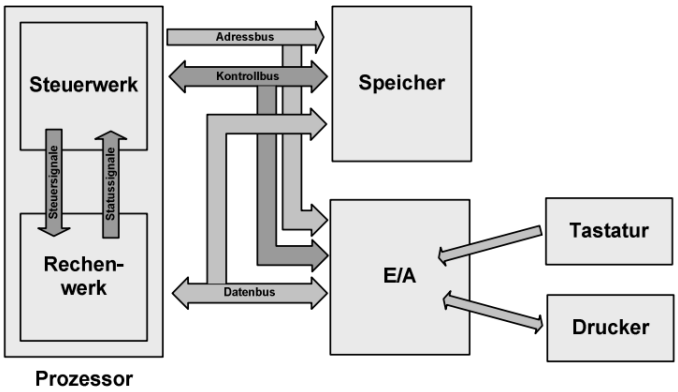


Abbildung 45: Allgemeiner Aufbau eines Computersystems

In Abbildung 45 ist der allgemeine Aufbau eines Computersystems dargestellt. Der Prozessor wurde bereits besprochen.

Bussystem

Das Bussystem ist ein Leitungsbündel zur Datenübertragung zwischen den Einheiten des Rechners. Speicherzugriff und die Datenübermittlung zwischen Speicher und Prozessor erfolgen über einen gemeinsamen Weg, den Datenbus (durchgängigen Adressierung). So entsteht hier eine Engstelle, der sogenannte „Flaschenhals“. Das Bussystem besteht aus drei Teilbusse: Datenbus, Adressbus, Steuerbus. Der Steuerbus bestimmt, ob Informationen gelesen oder geschrieben werden sollen. Der Adressbus übernimmt die Adresse einer Speicherzelle oder eines Ein- oder Ausgabegerätes, in der die Information abgelegt oder von der ausgelesen werden soll. Der Datenbus überträgt Daten zwischen den Teilsystemen des Prozessors und dem Arbeitsspeicher.

Arbeitsspeicher

Der Arbeitsspeicher ist deutlich kleiner als eine Festplatte oder ein Magnetband und verliert seine Informationen beim Ausschalten des Rechners. Dafür ist er schneller als permanente Speichermedien. Der Arbeitsspeicher besteht aus besteht aus Halbleiter-Speicherbausteinen, die RAM (Random Access Memory) genannt werden.

Zu startende Programme werden vom Prozessor zunächst automatisch von der Festplatte oder einem anderen Medium in den Arbeitsspeicher kopiert. Er ist Zwischenspeicher für alle Daten, die während des Programmlaufes erzeugt oder verarbeitet werden.

2.4.4 Ablauf des Bootvorgangs

Der Bootvorgang ist ein mehrstufiger, aufeinander aufbauender Vorgang und macht einen Computer arbeitsfähig. Hierbei gibt es verschiedene Firmware: das BIOS oder UEFI.

BIOS

Der erste Schritt nach dem Einschalten des Computers ist der Aufruf des BIOS (Basic Input Output System). Das BIOS stellt die klassische Variante dar. Es handelt sich hierbei um Computercode, der sich in einem nicht-volatilen Speicher auf dem Mainboard des Rechners befindet und unmittelbar nach dem Start des Computers ausgeführt. Das BIOS arbeitet zwischen Hardware und Betriebssystem (Schnittstelle zwischen Soft- und Hardware). Es führt eine Hardwareerkennung durch und initialisiert diese. Dabei beginnt das Testen der Komponenten CPU, RAM, ggf. Grafikkarte (Power-On self Test., POST). Danach erfolgt das Einbinden des Hardwarespeichers und die Initialisierung von Hardwareeinstellungen. Im Anschluss an die Hardwareerkennung werden die Einstellungen (Bootreinfolge, Partitionstabelle und Master Boot Record) geladen. Der MBR umfasst Bootprogramm, welches Betriebssystemeinträge und Partitionseinträge enthält. Auf die genauen Funktionsweisen der Komponenten wird in einem späteren Kapitel genauer eingegangen. Das BIOS übergibt den Vorgang schließlich an den Bootmanager, welcher den Kernel sucht und lädt Kernel. Danach erfolgt die Übergabe an den Kernel.

UEFI

Extensible Firmware Interface (EFI), bzw. Unified Extensible Firmware Interface (UEFI) als Nachfolger zum BIOS bietet mehr Möglichkeiten als BIOS. Es handelt sich um eine Firmware, die eigene Treiber zum Einbinden von Festplatten oder Netzwerkkarten besitzt, Partitionstabellen lesen und FAT-Systeme verstehen kann.

2.5 Datenträgertechnik

Ein Festplattenlaufwerk oder auch Hard-Drive ist ein magnetisches Speichermedium. Bei einer Festplatte werden die Daten auf rotierenden Scheiben abgelegt. Dazu Plattenoberfläche mit Hilfe eines Schreib- /Lesekopfes magnetisiert. Durch die Remanenz erfolgt die Speicherung der Information. Das Auslesen der Information erfolgt durch Abtastung der Magnetisierung der Plattenoberfläche. Weitere Datenträger, die mittels Magnetisierung Informationen ablegen sind.

Neben klassischen Festplatten-Laufwerken werden zunehmend so genannte Solid-State-Drives (SSDs) in IT-Systemen verbaut. Eines SSD, ist ein nichtflüchtiges elektronisches Speichermedium. Vorteile einer SSD gegenüber herkömmlichen Laufwerken sind mechanische Robustheit, sehr kurze Zugriffszeiten und keine Geräuschentwicklung aufgrund beweglicher Bauteile.

USB-Sticks, Memory-Cards in Mobil-Telefonen, SD-Karten nutzen genauso wie die zuvor genannten SSDs Flash-Speicher zur Speicherung. Bei einem Flash-EEPROM-Speicher wird Information (Bits) in einer Speichereinheit (Speicherzelle) in Form von elektrischen Ladungen gespeichert. Alle Flash-Speicher haben eine begrenzte Lebensdauer, die in einer maximalen Anzahl an Löschzyklen angegeben wird. Diese schwanken zwischen 10.000 und hin zu zwei Millionen Zyklen.

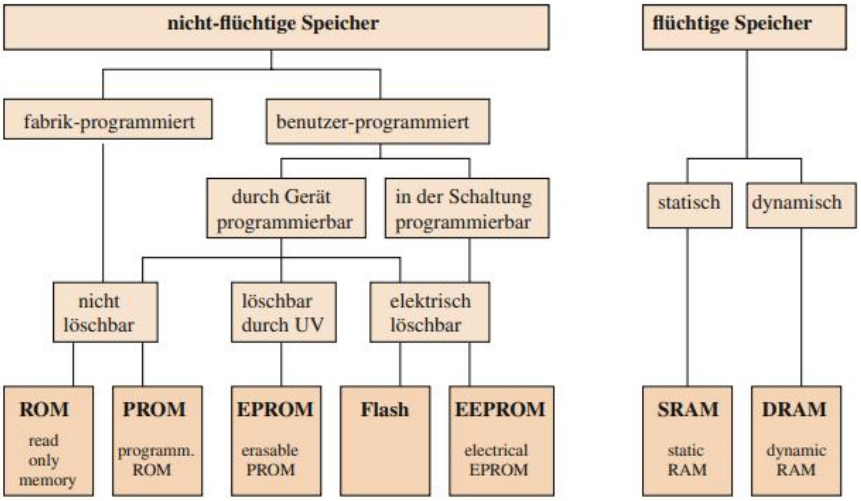


Abbildung 46: Übersicht über Speichertechnologien

Eine Übersicht über die verschiedenen Speichertechnologien und deren Einordnung ist in Abbildung 46 zu sehen. Der wichtigste Klassifikationsfaktor ist, ob es sich um flüchtige oder nicht-flüchtige Speicher handelt.

2.5.1 Technischer Aufbau von Festplatten

Moderne Festplatten nutzen das sogenannte Zone Bit Recording, bei dem die Platte in Spuren/Zonen aufgeteilt wird. In Abbildung 47 ist dieses Prinzip grafisch dargestellt. Die Festplatte an sich enthält mehrere genau übereinanderliegende Spuren, welche als Zylinder bezeichnet werden. Sie sind wie

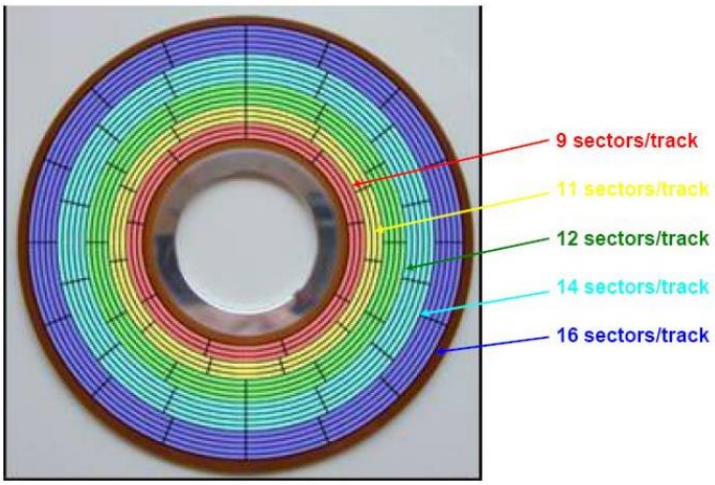


Abbildung 47: Zone Bit Recording auf einer Festplatte

einzelne Scheiben, die alle den gleichen Radius haben. Die Äußere Spuren jedes Zylinders sind dabei wesentlich länger und umfassen deshalb viele Sektoren. Das bedeutet, dass bei gleicher Datendichte mehr Daten speicherbar sind. Die inneren Spuren umfassen weniger Sektoren. Die Nummerierung erfolgt immer von außen nach innen.

Festplatten werden dann partitioniert. Die Erklärung dazu erfolgt in einem der folgenden Kapitel.

2.5.2 Aufbau von Flashspeichern

Flashspeicher sind aus mehreren Speicherzellen aufgebaut, welche jeweils einen Transistor zur Speicherung beinhalten. Die Technologie wird in Speicherkarten, USB-Sticks, SSDs (Solid State Disks) und als Speicher für das BIOS von Mainboards genutzt. Flashspeicher werden elektrisch gelöscht und beschrieben.

SSD

Eine SSD, ein Solid State Drive ist ein „Flash-only“ Speicher. In diesem Bereich unterscheidet man zwischen Single-level cell (SLC) und Multi-level cell (MLC), aber auch zwischen NAND vs. NOR-Zellen.

Vorteile von Flashspeichern:

- Keine mechanischen Teile (günstig & robust)
- Schnell (Datenrate & Latenz)
- Kapazität „nach oben offen“
- Strombedarf / Thermisches Verhalten
- (Dynamic) Wear Levelling
- kein Defragmentieren notwendig

Nachteile von Flashspeichern:

- Controller = SPOF (Single Point of Failure)
- Recovery extrem aufwendig bis unmöglich
- „sicheres Löschen“ nur im Enterprise Sektor
- Leistungsverluste (Trim / Garbage Collection)

2.5.3 RAID

Bei einem RAID (Redundant Array of Independent Disk) handelt es sich um eine Methode zur Speicherung von Daten auf Festplatten. Dabei liegt der Fokus auf dem Schutz vor Hardwareausfall. Dies wird mittels Redundanzen realisiert. Bei einem RAID-System werden Festplatten zu Gruppen, die unteranderem Datenkopien beinhalten, zusammengefasst. Umgesetzt wird dies durch drei verschiedene Techniken, die in Abbildung 48 kurz erläutert sind: Mirroring (Spiegelung), Striping, Parität.

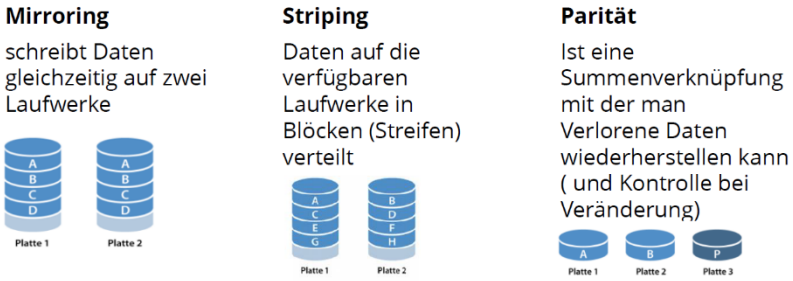


Abbildung 48: Techniken der RAID-Realisierung

Das Spiegeln und das Striping sind recht einfache Techniken. Das Bilden einer Parität ist etwas komplizierter, bietet dafür aber die Möglichkeit verlorene Daten wiederherzustellen. Man hat zwei Datensätze A und B auf zwei unterschiedlichen Platten und die Parität der beiden auf einer dritten. Fällt nun eine Platte aus, lassen sich die Daten mit dem übrigen Teil und dem Paritätsblock wiederherstellen. Die Parität wird mittels Summenverknüpfung berechnet/ermittelt. In Abbildung 49 ist die Vorgehensweise dargestellt.

```
Bits der Datenplatten → Summe → gerade oder ungerade → Summen-Bit der Paritätsplatte

0 + 0 + 0 → Summe ist 0 → Summe ist gerade   → Summen-Bit 0
1 + 0 + 0 → Summe ist 1 → Summe ist ungerade → Summen-Bit 1
1 + 1 + 0 → Summe ist 2 → Summe ist gerade   → Summen-Bit 0
1 + 1 + 1 → Summe ist 3 → Summe ist ungerade → Summen-Bit 1
0 + 1 + 0 → Summe ist 1 → Summe ist ungerade → Summen-Bit 1

Wenn beispielsweise das Bit der ersten Datenplatte verloren ginge,
könnte man es aus den Bits der anderen Datenplatten und dem Summen-Bit
der Paritätsplatte errechnen.

? + 0 + 0 → eine gerade Summe   → das erste Bit kann nicht 1 sein, nur 0
? + 0 + 0 → eine ungerade Summe → das erste Bit kann nicht 0 sein, nur 1
? + 1 + 0 → eine gerade Summe   → das erste Bit kann nicht 0 sein, nur 1
? + 1 + 1 → eine ungerade Summe → das erste Bit kann nicht 0 sein, nur 1
? + 1 + 0 → eine ungerade Summe → das erste Bit kann nicht 1 sein, nur 0
```

Abbildung 49: Berechnung der Bit-Weisen Parität

Durch die Kombination der verschiedenen Techniken können verschiedene RAID-Level zusammengestellt werden.

2.5.3.1 RAID 0

- Mindestens 2 Festplatten
- Daten werden auf Festplatten verteilt
- Keine Sicherheit (fällt eine Platte aus, sind alle Daten weg)
- Hohe Lese- und Schreibgeschwindigkeit
- Speicherkapazität 100 %

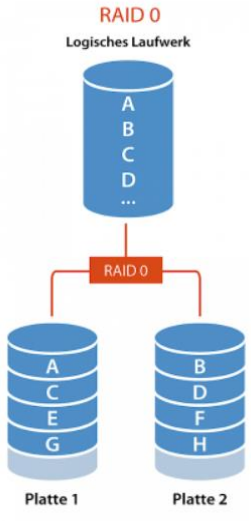


Abbildung 50: RAID 0

2.5.3.2 RAID 1

- Mindestens 2 Festplatten
- Alle Daten werden auf beide Festplatten geschrieben
- Hohe Ausfallsicherheit
- Hohe Lese- und Schreibgeschwindigkeit
- Speicherkapazität 50 %

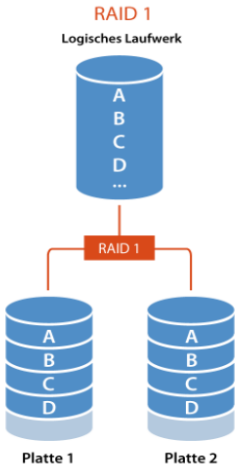


Abbildung 51: RAID 1

2.5.3.3 RAID 5

- Mindestens 3 Festplatten (max. 16)
- Daten auf Festplatten verteilt, Parität errechnet und gespeichert
- Bei Festplattenausfall können über Parität Daten gerettet werden
- Hohe Rechenleistung, aber Ausfallsicherheit
- Speicherkapazität: 67 % - 94 %

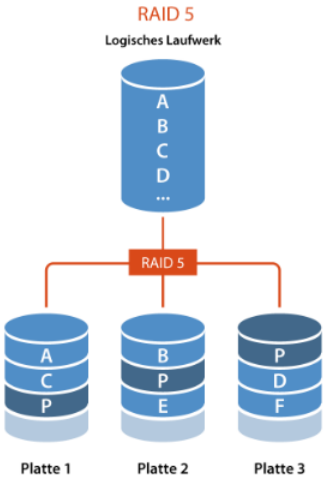


Abbildung 52: RAID 5

2.5.3.4 RAID 6

- Mindestens 4 Festplatten (max. 16)
- Daten auf Festplatten verteilt, zwei Paritäten (P und Q) errechnet und gespeichert
- Bei Festplattenausfall (maximal 2) können über Parität Daten gerettet werden
- Extrem hohe Rechenleistung, aber hohe Ausfallsicherheit
- Speicherkapazität: 50 % - 88 %

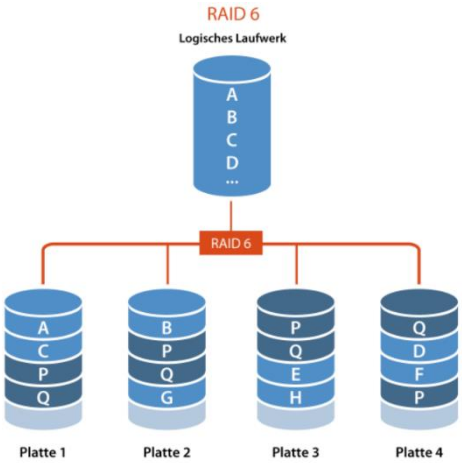


Abbildung 53: RAID 6

2.5.3.5 Kombination verschiedener RAID-Level

Die einzelnen RAID-Level lassen sich nun auch kombinieren. In Abbildung 54 sind drei kombinierte RAIRDs zu sehen: RAID 10, RAID 01 und RAID 50. Das Zusammenspiel verschiedener Level kann jeweils die Nachteile ausgleichen, allerdings werden auch die Vorteile etwas abgeschwächt.

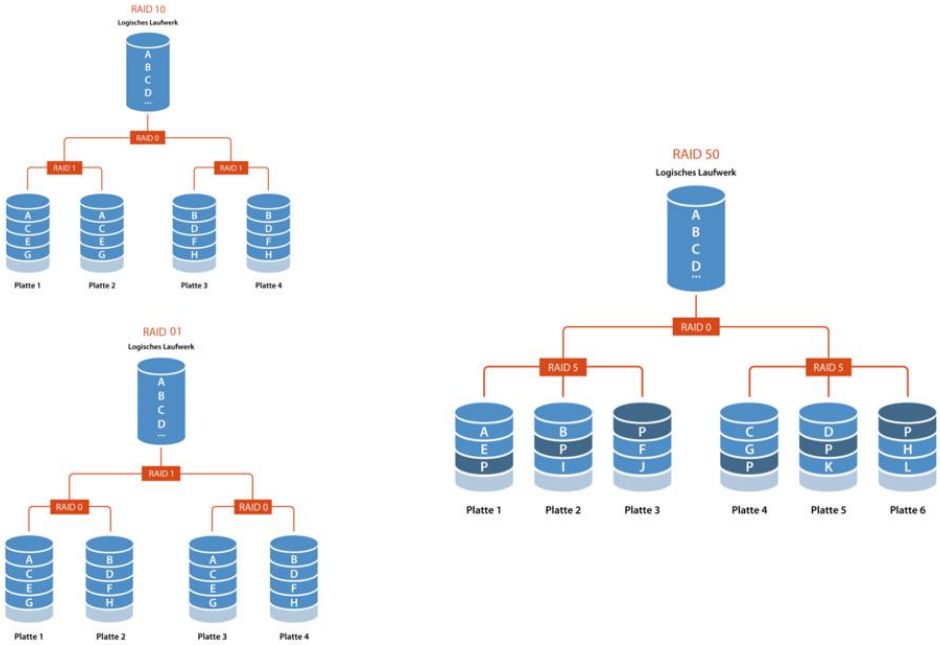


Abbildung 54: RAID 10, RAID 01, RAID 50

2.5.3.6 Hardware- und Software-RAID

Ein RAID-System kann entweder hardware- oder softwarebasierend realisiert werden. Beim Hardware-RAID sind die Platten physisch vorhanden, bei der Software-Lösung sind die Platten virtuell.

Das Hardware-RAID benötigt einen physischen Controller, der die Arbeit übernimmt. Dadurch wird die CPU nicht durch die Berechnungen belastet.

Vorteile Hardware-RAID:

- Steht bereits beim Booten zur Verfügung
- Unterstützt eine Vielzahl von Betriebssystemen
- Hohe Performance
- Niedrige CPU-Last am Host

Nachteile Hardware-RAID:

- Hohe Anschaffungskosten
- Betriebssystemabhängig

Vorteile Software-RAID:

- Kein separater RAID-Controller benötigt
- Preisgünstiger als ein Hardware-RAID
- Kann unter anderem direkt unter Windows erstellt werden

Nachteile Software-RAID:

- schlechtere Gesamtperformance durch höherer CPU-Belastung

2.6 Betriebssysteme und Dateisysteme

2.6.1 Dateisysteme Allgemein

Betriebssysteme und Datei- bzw. Filesysteme gehen Hand in Hand. Dateisysteme sind dabei die Grundlage zur Speicherung von Daten auf einem Datenträger und bilden somit die Schnittstelle zwischen den Betriebssystemen und der Hardware des Datenträgers. Dabei ist die wichtigste Aufgabe des Dateisystems die für den Nutzer nicht ersichtliche Speicherung bzw. Auslesung der Daten und die Möglichkeit der Organisation in Hierarchieebenen zu realisieren.

Das Dateisystem der Datenträger ist einer der bedeutsamsten Orte für digitale Spuren, da besonders nichtflüchtige Daten hier gespeichert werden. Ein Dateisystem muss eine Reihe von Informationen über die gespeicherten Daten enthalten, damit z.B. beim Mehrbenutzerbetrieb nur derjenige auf die Daten zugreifen kann, der auch die nötigen Rechte besitzt. Diese Details über Daten beinhalten u. a. das Erstellungsdatum einer Datei, das Datum des letzten Zugriffs, das Datum der letzten Modifikation, den Eigentümer und die Zugriffsrechte. Zu den Aufgaben eines Dateisystems gehören auch die Verwaltung des Dateinamens (bzw. des Verzeichnisnamens), Verwaltung des Dateianfangs, Verwaltung der Dateilänge zusammen mit Metadaten (z. B. Dateirechte, Zeitstempel), Verwaltung der von der Datei benutzten Speichereinheiten (Cluster) und die Verwaltung der belegten und freien Cluster.

2.6.1.1 Speicherung von Daten

Es existiert eine Vielzahl verschiedener Dateisysteme, welche vom Betriebssystem erkannt und die Daten zugänglich gemacht werden müssen. Dabei könnten Daten einfach aneinander folgend auf einen Datenträger geschrieben werden. Das wäre die einfachste Variante einer Speicherung. In Abbildung 55 ist dies dargestellt.

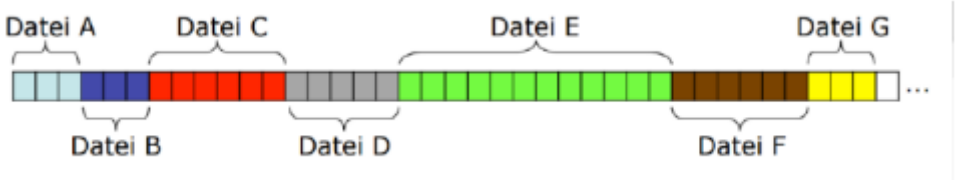


Abbildung 55: Einfaches Hintereinander Schreiben von Dateiblöcken

Der Vorteil hierbei wäre ein schnelles Lesen von Daten mit wenigen Leseoperationen. Das Finden wiederum gestaltet sich schwer, weil das Speichermedium jeden Mal von ausgelesen werden muss, bis die gesuchte Datei gefunden wird. Deshalb ist es besser, wenn man eine Struktur einbaut, die die Daten logisch organisiert und auch adressiert. Ein weiterer Nachteil dieser Variante wäre z.B. das Szenario, dass in Datei C etwas ergänzt werden muss. Dafür ist kein Platz, da sich Datei D direkt anschließt. Auch beim Löschen einer Datei, wäre ungenutzter Speicherplatz als Folge sehr ineffizient. Das Speichermedium wäre einer Fragmentierung ausgesetzt, welche das Auslesen verschlechtert und ineffizient bezüglich des genutzten Speicherplatzes ist. Für Read-Only-Memories ist das kein Problem, da diese Speichermedien nur gelesen werden, aber nicht ergänzt oder beschrieben werden können,

wie beispielsweise CD-ROMs oder DVD-ROMs. Für Dateisysteme, die dynamisch in Verbindung mit einem Betriebssystem laufen, ist diese Variante der Datenspeicherung nicht effizient.

Um dieser Problematik entgegenzuwirken, können verkettete Listen integriert werden, welche sich ähnlich zu Indexdateien verhalten. Dabei erfolgt die Speicherung von Dateien in Datenblöcken mit fester Blockgröße.

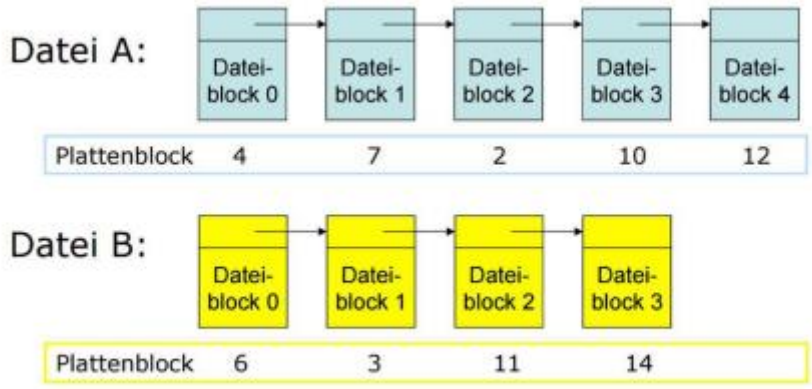


Abbildung 56: Verkettete Listen

In Abbildung 56 sind solche Listen für Datei A und B dargestellt. Vor der Aufteilung der Datei wird diese in gleichgroße Blöcke unterteilt. Jeder Block verweist auf den nächstfolgenden Block. Deshalb können die Blöcke über den gesamten Datenträger verteilt sein. Sollten Dateien gelöscht werden, können die frei gewordenen Blöcke neu besetzt werden. Die Fragmentierung führt also nicht zum Speicherplatzverlust. Allerdings ist das Auffinden eines bestimmten Blocks immer noch sehr zeitintensiv.

Als Verbesserung gilt hier dann die verkettete Liste in einer Tabelle. Informationen über die Verkettung der Blöcke wird zentral außerhalb der Blöcke in einer Tabelle realisiert. Die Informationen werden dann im Hauptspeicher (RAM) gehalten, wodurch man gezielt zwischen Blöcken hin und her springen kann. Durch diese Blockadressierung kann jede einzelne Speicherstelle über ihre fest zugeordnete Adresse beliebig oft gelesen oder beschrieben (und damit auch gelöscht) werden. Dabei werden also

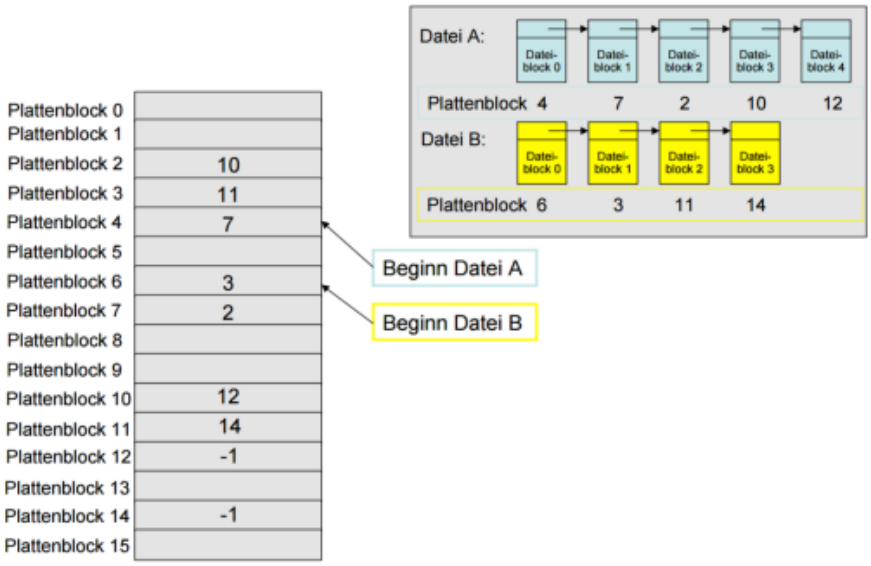


Abbildung 57: verkettete Liste mit Tabelle

langsame Plattenzugriffe durch schnellere Hauptspeicherzugriffe ersetzt. In Abbildung 57 ist das Prinzip der Datenspeicherung nochmal grafisch dargestellt. Man spricht bei diesem Prinzip von einer Datei-Allokationstabelle oder auch File Allocation Table (FAT).

Nachdem das Grundprinzip der Speicherung verstanden ist, folgt die Klärung einiger wichtiger Begrifflichkeiten, der Grundbegriffe im Zusammenhang mit Dateisystemen: Sektor und Cluster.

Als Sektor bezeichnet man die Zusammenfassung einzelner Bytes zu einem Block. Die Zusammenfassung wird auf Ebene der Festplattenfirmware realisiert. Die gebräuchlichste Sektorgröße sind 512 Bytes. Es ist auch möglich, Festplatten mit Sektorgrößen von 1024 – 4096 Bytes vorzufinden.

Die Zusammenfassung einzelner Sektoren zu einem Block bezeichnet man als Cluster. Sie wird auf Ebene der Betriebssysteme realisiert. Die Clustergröße ist direkt abhängig vom Dateisystem.

Durch die Zusammenfassung zu logischen Einheiten und Übereinheiten wird die Geschwindigkeit optimiert und der Verwaltungsaufwand verringert. Dabei ist wichtig zu wissen, dass die Adressierung im Dateisystem immer über die Clusternummer erfolgt, nicht über die Sektornummer! Cluster und Sektoren müssen gegebenenfalls ineinander umgerechnet werden!

2.6.1.2 Festplattenpartitionierung

Die Festplattenpartitionierung ist die Voraussetzung für die Realisierung bzw. Einrichtung eines Dateisystems. Eine Partition ist der zusammenhängende Speicher eines physischen bzw. virtuellen Datenträgers, wobei die Partition unter die logischen Datenträger einzuordnen ist. Von Betriebssystemen werden Partitionen wie eigenständige Speichereinheiten behandelt. Befinden sich auf einem Datenträger mehrere Partitionen, so sind die Speicherbereiche der einzelnen Partitionen voneinander getrennt und unabhängig, was bedeutet, dass eine Datei nicht über die Partitionsgrenzen hinweg in einer zweiten Partition gespeichert werden kann.

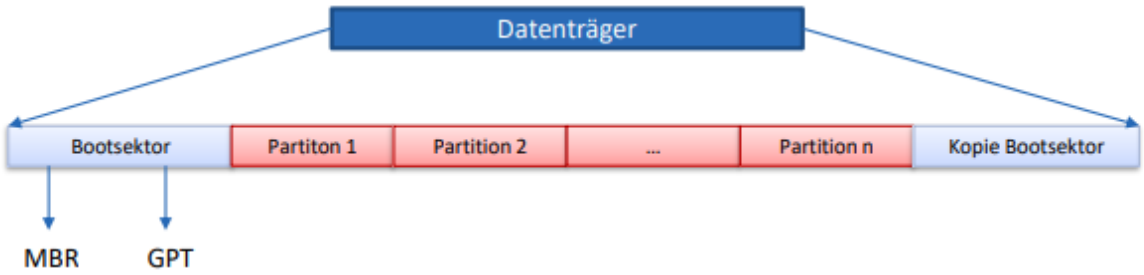


Abbildung 58: Festplattenpartitionierung eines Datenträgers

In Abbildung 58 ist die grundlegende Partitionierung eines Datenträgers zu sehen. Am Anfang eines Datenträgers befindet sich der Bootsektor (MBR/GPT), der die Partitionstabelle mit den Eintragungen zu den einzelnen Partitionen des Datenträgers enthält. Am Ende eines Datenträgers kann sich eine Kopie des Bootsektors befinden. Dazwischen befinden sich die einzelnen Partitionen.

Der **Master Boot Record (MBR)** enthält ein Startprogramm für BIOS basierte Rechner. Er liegt immer im ersten Sektor eines partitionierbaren Speichermediums, hat eine Größe von 512 Byte und besteht aus vier Komponenten:

- Startprogramm (Bootloader)
- Datenträger-, Disk-Signatur (ab Windows 2000)
- Master-Partitionstabelle

- MBR- oder Boot-Signatur (Magic Number/Magic Byte)

Adresse		Funktion / Inhalt		Größe (Bytes)
hex	dez			
0x0000	0	Startprogramm (Master Boot Code / Bootloader)		440
0x01B8	440	Datenträgersignatur		4
0x01BC	444	Null (0x0000)		2
0x01BE	446	Partitionstabelle		64
0x01FE	510	55_{hex}	Bootsektor-Signatur (wird vom BIOS für den ersten Bootloader geprüft)	2
0x01FF	511	AA_{hex}		

Abbildung 59: Aufbau MBR

Abbildung 59 zeigt nochmal den Aufbau eines MBRs mit allen Komponenten und den entsprechenden Größen. Einer der wichtigsten Teile ist die Partitionstabelle, welche die dezimale Adresse 446 besitzt. Sie ist 64 Bytes groß und beinhaltet immer 4 Einträge. Jeder Eintrag hat dabei eine feste Struktur und gibt Informationen über die einzelnen Partitionen. Erste Hinweise für Ermittlungen kann man bereits in der Partitionstabelle finden, beispielsweise ob das System bootfähig oder nicht.

Offset	Länge	Beschreibung
0x00	1	Bootindikator (0x80 für bootfähig)
0x01	3	Startsektor der Partition in CHS Notation
0x04	1	Partitionstyp
0x05	3	Partitionsende in CHS Notation
0x08	4	Startsektor der Partition in LBA Notation
0x0C	4	Größe der Partition in Sektoren

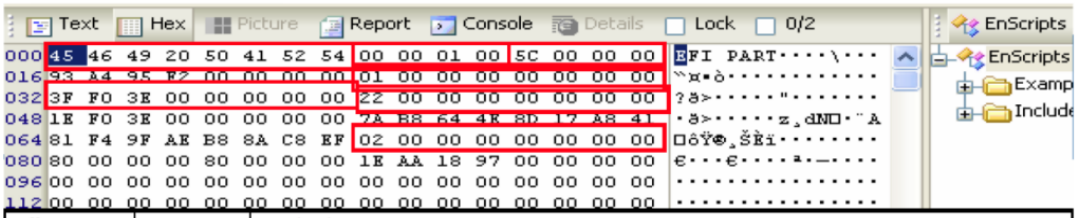
Abbildung 60: Aufbau eines Eintrags der Partitionstabelle

In Abbildung 60 ist diese Struktur sichtbar. Informationen, die entnommen werden können, sind hierbei der Startsektor der Partition, der Partitionstyp (hierfür gibt es Tabellen, welche die Typen aufschlüsseln), das Partitionsende, den Startsektor der Partition und die Größe der Partition in Sektoren. Durch die Begrenzung auf vier Einträge ist auch die maximale Partitionsanzahl vier. Für die

Lösung dieses Problems wurde das EFI (Extensible Firmware Interface) mit einer neuen Datenträgerverwaltung benannt als GUID Partition Table- GPT entwickelt.

EFI bietet mehr Möglichkeiten als das normale BIOS und ist eine Firmware, die eigene Treiber zum Einbinden von Festplatten oder Netzwerkkarten besitzt. Computer, die EFI basiert sind, können auf GPT-Festplatten zugreifen. Bei BIOS basierten Systemen ist dies nur optional einrichtbar.

GPT, die Global Unique Identifier Partition Table, ist in Abbildung 61 dargestellt.



Offset	Länge	Beschreibung
0x0	8	Signatur immer „EFI PART"
0x8	4	Revision, derzeit V.1.0 => 00 00 01 00
0x0C	4	Headersize
0x10	4	CRC 32 Checksumme
0x14	4	Reserviert – immer 0
0x18	8	Primary LBA, Adresse des primary GPT headers
0x20	8	Backup LBA, Adresse des backup GPT headers
0x28	8	1. Benutzbare LBA Sektor
0x30	8	Letzter benutzbarer LBA Sektor
0x38	16	Disk GUID, ID über die Disk und die Partitionstabelle
0x48	8	Partition entry LBA, Beginn der Partitionseinträge
0x50	4	Anzahl der Partitionseinträge (bei Windows 128)
0x54	4	Größe der einzelnen Partitionseinträge (128 Bytes)
0x58	4	CRC 32 Checksumme über die Partitionseinträge

Abbildung 61: Aufbau der Global Unique Identifier Partition Table

In der Abbildung sieht man den Aufbau mit allen Komponenten und Partitionierungsinformationen, also den GPT-Header. Die GPT schließt sich an den MBR an und schafft die Möglichkeit bis zu 128 bootfähige Partitionen einzurichten. Nach dem Header folgen 32 Sektoren für Partitionseinträge und daraufhin die Partitionen. Am Ende schließt sich eine Sicherheitskopie der ersten 33 Sektoren an, welche als Backup gilt. Diese Information ist nützlich, falls ein beschädigter Datenträger vorliegt, bei dem die GPT verändert wurde und somit unbrauchbar ist. Die Backup-GPT kann dann an den Anfang kopiert werden.

2.6.1.3 File Allocation Table (FAT)

Das FAT-Dateisystem baut auf der bereits beschriebenen Speicherungsidee mit verketteten Listen und einer Adressierungstabelle auf. FAT benötigt nur die File-Allocation-Table und die Verzeichniseinträge. Es ist eines der verbreitetsten und einfachsten Dateisysteme, da es eine geringe Anzahl an Datenstrukturen benötigt, um eine Datenverwaltung zu realisieren. Viele Hardwaresysteme wie USB-Sticks oder externe Festplatten unterstützen dieses Dateisystem. Wir unterscheiden die verschiedenen Versionen hauptsächlich anhand der Größe der Datenfelder, in die die FAT-Tabelle unterteilt ist. FAT 12 hat beispielsweise 12-bit große Datenfelder. Zusätzlich wurden noch einige Erweiterungen entwickelt, wie exFAT oder TFAT.

FAT 12

- FAT 12 ist für DOS-Disketten oder Festplatten von einer Größe von bis zu 32 MB
- 12 Bit Clusternummern -> die max. Anzahl der Cluster: 2^12 = 4.096 Byte
- Die max. Clustergröße auf Disketten: 2 KB - auf Festplatten: 4 KB
- Die max. Partitionsgröße auf Disketten: 8 MB - auf Festplatten: 16 MB
- Namenslänge von Einträgen: 8+3 (8 Zeichen für den Dateinamen, 3 für die Endung)
- Root Directory auf 14 Cluster beschränkt -> maximal 224 Einträge (VZ und/oder Dateien)
- Die Variante der Partitionsgröße von 32 MB mit einer Clustergröße von 8 KB ist möglich, wird jedoch per Default durch Verwendung von FAT 16 erzielt

FAT 16

- FAT 16 ist für Festplatten mit mehr als 32 MB Speicher geeignet.
- 16 Bit Clusternummern, d.h. die max. Anzahl der Cluster: (2^16)-12 = 65.524!
- 12 Cluster werden von FAT 16 reserviert, daher nicht 65.536
- Die max. Clustergröße: 32 KB. Bei Win NT 64 KB.
- Die max. Partitionsgröße: 2 GB. Bei Win NT 4GB (nicht kompatibel mit DOS)
- Max. Einträge in das Root-Verzeichnis: 256 (Größe wird festgelegt, kann nicht wachsen)
- Max. Einträge pro Volume: 65.536
- Max. Dateigröße: 2GB
- Namenslänge von Einträgen: 8+3

VFAT

- VFAT, Virtual File Allocation Table, ist eine Erweiterung von FAT zur Verwendung von längeren Dateinamen.
- Dies geschieht durch einen Trick im Layout der Verzeichniseinträge des FAT-Dateisystems.
- Der Name im Verzeichniseintrag wird regulär mit der Länge von 8+3 gespeichert. Ist der Name länger, so wird ein Alias in Form von xxxxxx~1.xxx verwendet.
- Dabei wird die Ziffer für jedes Alias, das verwendet wird, um eins inkrementiert. Bei FAT 12 und FAT 16, welches dieses System nicht unterstützt, werden die Alias nicht gelesen und der Dateiname wird als die ersten 8+3 gewertet.
- Somit abwärtskompatibel für zu anderen FAT-Anwendungen.

FAT 32

- 32 Bit Clusternummern, von denen 4 Bit reserviert sind (32 - 4 = 28 Bit).
- max. Clusternummer: 2^28 = 268.435.456 Cluster.
- Die max. Clustergröße: 32 KB. Die max. Partitionsgröße: 32 GB unter Win OS. (Tools von Drittherstellern 127 GB, theoretisch sind auch 8 TB möglich)
- Max. Einträge pro Verzeichnis: 65.536
- Max. Einträge in das Root-Verzeichnis: 4.177.920
- Max Dateigröße: 4 GB
- Namenslängen von Einträgen: 255 Zeichen
- Nicht kompatibel zu FAT-16 Anwendungen.

2.6.1.4 NTFS

NTFS - das New Technologie File System (NTFS) - wurde das erste Mal im Juli 1993 mit Windows NT 3.1 veröffentlicht und ist das Standarddateisystem für Windows-Betriebssysteme.

Ein Vorteil von NTFS ist, dass die Dateigröße nicht auf 4 GiB beschränkt ist, wie es bei FAT der Fall ist.

- Die max. Anzahl der Cluster: Bei Win-OS: 2^32, theoretisch aber 2^64 möglich.
- Die max. Clustergröße: 64 KB, per Default 4 KB.
- Die max. Partitionsgröße: Bei Win-OS: 256 TB.
- Theoretische max. Größe: 1YB -> 1 Yotabyte = 1.024 Zetabyte = 1.048.576 EB
- Die max. Dateigröße: Bei Win-OS: 16 TB. Theoretische max. Größe: 16 EB. 1 Exabyte = 1.048.576 TB = 1.073.741.824 GB
- Namenslänge von Einträgen: 255, nicht kompatibel zu FAT16- Anwendungen

NTFS bietet im Gegensatz zu FAT-Transaktionsverfolgungen, einen gezielten Zugriffschutz auf Dateiebene durch Dateirechte, eine höhere Datensicherheit durch Journaling und die Möglichkeit der Daten Komprimierung.

Wichtiger Hinweis: Es existiert keine offizielle Dokumentation für NTFS von Microsoft, die den genauen Aufbau des Dateisystems beschreibt. Aus diesem Grund tun sich Dritthersteller sehr schwer Treiber für schreibenden Zugriff auf NTFS bereitzustellen.

Das Dateisystem ist so aufgebaut, das Änderungen in der äußeren Datenstruktur vorgenommen werden können, ohne die vorhandenen Datenstrukturen zu verändern. Damit wird eine Abwärtskompatibilität gewährleistet!

NTFS arbeitet nach dem „Everything is a file“-Konzept. Bei NTFS wird alles als Datei behandelt. Das bedeutet, dass der gesamte Dateisystem als EIN Datenbereich eingerichtet ist. Der einzige konsistente Bereich ist der Boot-Sektor. In Abbildung 62 ist der Vergleich zwischen NTFS und FAT in Bezug auf deren Konzepte und Umsetzung dargestellt.

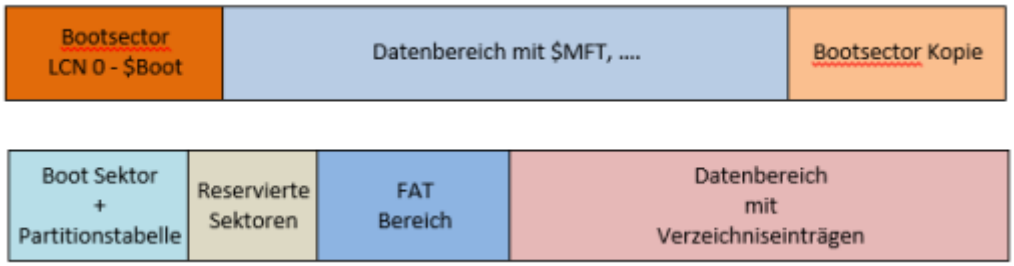


Abbildung 62: Vergleich NTFS und FAT

Die für die Dateiverwaltung zuständigen Strukturen sind ebenfalls nur Dateien und können sich überall auf dem Datenträger befinden. Die Verwaltungsstrukturen besitzen jedoch ein bestimmtes Dateilayout, so dass diese vom Betriebssystem als NTFS-internen Verwaltungsstrukturen erkannt und ausgeblendet werden. Erkennbar an dem Präfix $ vor dem Dateinamen. Die für die Datei und Verzeichnisverwaltung zuständige Datenstruktur wird als Master File Table (MFT) bezeichnet und ist eine Datei die sich als $MFT auf dem Datenträger befindet. Jede auf dem NTFS-Datenträger vorhandene Datei oder jedes vorhandene Verzeichnis besitzt zumindest einen Eintrag im MFT, welcher dann als MFT-Eintrag (File Entry/MFT Entry/MFT Record) bezeichnet wird.

Vergleicht man FAT32 und das NFTS kann man eine deutliche Verbesserung sehen. Das FAT32-Dateisystem weist diverse Beschränkungen auf: die Unterstützung von nicht mehr als 32 GB Speicherkapazität als Standard, fehlende Unterstützung für SDXC-Karten mit höherer Größe als 127GB oder auch den Punkt, dass es nicht für Flash Speicher konzipiert ist. NTFS bietet neben der Unterstützung größerer Speicherkapazitäten weitere Sicherheitsfunktionen, Optionen für Wechselspeichergeräte, einen Metadaten-Overhead für Dateien oder Verzeichnisse und einen

Schreib-Caching-Mechanismus für die Leistungsoptimierung. Der Schreib-Caching-Mechanismus verursacht jedoch eine Datenbeschädigung, wenn der Wechseldatenträger einfach abgesteckt wird.

Da die Technologieentwicklung die Grenzen von Wechselmedien sprengte, wurde ein neues Dateisystem benötigt, um die größeren Kapazitäten und schnelleren Zugriffsgeschwindigkeiten zu unterstützen. Die Antwort von Microsoft darauf ist das Extended FAT File System (exFAT) welches 2006 entwickelt wurde für Windows CE, das auf seinen neueren Betriebssystemen seit 2010 verfügbar gemacht wurde und auf neuen SDXC-Speichermedien (Secure Digital Extended Capacity) die 2009 eingeführt wurden, unterstützt wird. Zusätzlich zum ExFAT Dateisystem existiert eine transaktionsbasierte Erweiterung, das transaktionssichere Extended FAT-Dateisystem (TexFAT). Dieses ist eine Variante des ExFAT-Dateisystems mit Stromausfallsicherheit. Das TexFAT-Dateisystem ist in Windows CE (Compact Embedded) Version 6.0 und höheren Betriebssystemen (OS) nutzbar. Die Desktop Betriebssysteme unterstützen kein TexFAT! Die aktuelle ExFAT Version ist die Version 1.0, welche das transaktionsbasierte TexFAT Dateisystem nicht unterstützt.

2.6.2 Kompatibilität zwischen Dateisystemen und Betriebssystemen

Abbildung 63: Kompatibilität

In Abbildung 63 sind die Kompatibilitäten zwischen den Betriebssystemen (allgemein) Linux, iOS, Windows und der Dateigrößen von über 4 GB zu den Dateisystemen NTFS, exFAT und FAT bzw. FAT32 aufgezeigt.

2.6.3 Betriebssysteme und ihre Dateisysteme

Die Hardware eines Computers allein reicht nicht! Das Betriebssystem ist das Bindeglied zwischen der Hardware und dem Anwender bzw. dessen Anwendungsprogramm(en). Gleichzeitig bietet es dem Benutzer zahlreiche Dienste (Programme, Kommandos) an, die zusammen mit den Eigenschaften des Computers die „Grundlage der möglichen Betriebsarten dieses Systems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen“ (DIN 44300).

Generell bietet das Betriebssystem umfangreiche Möglichkeiten forensisch wertvolle Informationen zu liefern z.B. verwaltet Netzwerk (z.B. Netzwerkverbindungen, Konfigurationsvorgaben), Sitzungsdaten, Nutzerinformationen, Daten über geöffnete Dateien, Daten über laufende Prozesse uvm. Um in Betriebssystemen die forensisch wichtigen Spuren zu finden, muss der Ermittler die Betriebssysteme verstehen.

2.6.3.1 Betriebssystem Windows

Seit der Einführung von Windows 3.1 im Jahre 1990 hat Microsoft seine Marktstellung als führender Betriebssystemhersteller sukzessive ausgebaut. Seither gab es immer wieder neue Versionen des Betriebssystems Windows.

Allgemein unterstützt Windows die Dateisysteme FAT12/16/32, NTFS, ExFAT und CDFS/UDF. Die interne Datenaufteilung erfolgt in drei unterschiedlichen Kategorien, welche in Abbildung 64 zu sehen sind.

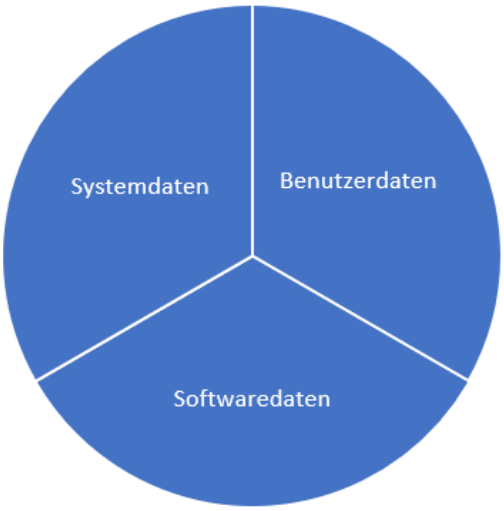


Abbildung 64: Kategorien der internen Datenaufteilung

Die logische Trennung dieser Daten findet sich dabei an verschiedenen Stellen im Betriebssystemaufbau wieder:

- **Systemdaten** findet man im Windows Verzeichnis, je nach Betriebssystemversion als „WINDOWS“, „WIN“ oder „WINNT“ benannt
- **Softwaredateien** befinden sich im Programm Verzeichnis je nach Betriebssystemversion als „Programme“ oder „Program Files“ benannt
- **Benutzerdaten** befinden sich im Benutzerdaten-Verzeichnis. Für die Windows Versionen Windows 95,98 und ME im Verzeichnis „Eigene Dateien“. Unter Windows NT, 2000 und XP im Verzeichnis „Dokumente und Einstellungen“ und unter Windows Vista, Windows 7, 8 und 10 im Verzeichnis „Users“ in einem Benutzerverzeichnis benannt nach dem Benutzerkontonamen

Einstellungen und Anwenderspezifische Daten zu einzelnen installierten Softwareanwendungen werden in Unterverzeichnissen gespeichert.

Unter Windows NT, 2000 und XP in: „\Anwendungsdaten“ und „\Lokale Einstellungen\Anwendungsdaten“.

Unter Windows Vista, 2003, 2008, 2012, 2013, 7, 8 und 10 in: „\AppData\Local“, „\AppData\LocalLow“ und „\AppData\Roaming“.

Windows (64 Bit) Besonderheiten

Seit der Einführung von 64Bit Windows Betriebssystemen wird 32Bit und 64Bit-Software in unterschiedlichen Verzeichnissen installiert. Dazu werden alle 32Bit-Programme auf 64Bit-Betriebssystemen in ein Programmverzeichnis mit dem Präfix „(x86)“ installiert.

Auch auf Systemebene wurde eine solche Trennung vollzogen. Im Windows Verzeichnis befindet sich auf 64Bit-Betriebssystemen das Verzeichnis „**SysWOW64**“ in dem sich die 32 Bit Systemkomponenten des Betriebssystems befinden. Bei der forensischen Untersuchung sind je nach Sachverhalt daher auch diese Verzeichnisse von Bedeutung.

Windows Benutzerverwaltung mittels SID

Die Benutzerverwaltung auf Windows Betriebssystemen wird mit Hilfe eines Security Identifier, kurz SID realisiert. Die SID ist geeignet um jedes System, jeden Benutzer und jede Gruppe dauerhaft zu identifizieren. An die SID sind die in Access Control Lists festgelegten Zugriffsrechte und Eigentümer gebunden, die auf NTFS-Dateisystemen die Benutzerzugriffsverwaltung realisieren. Werden Benutzernamen geändert oder gelöscht bleiben deren SID unverändert derjenigen Datei oder demjenigen Verzeichnis zugeordnet.

Spurenarten und Fundstellen in Windows

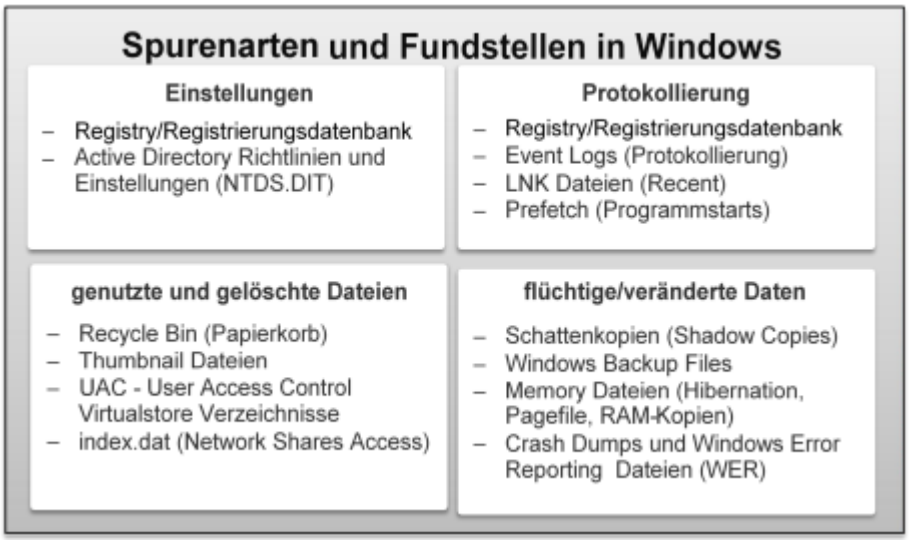


Abbildung 65: Spurenarten und Fundstellen (Quelle: Professor Ronny Bodach)

Speicherung von Einstellungen in der Registrierungsdatenbank

Die gespeicherten Daten werden in sogenannte Registrierungshives aufgeteilt und in Schlüsseln (Keys) mit Name Wert Paaren (Values) abgelegt. Ein Hive speichert damit einen Teilbaum der Registry. Alle Daten sind in einem Binärformat abgelegt. Bei Windows NT4, Windows 2000 und spätere haben die Dateien das Windows NT Registry File (REGF) Format. Für Windows 95, 98 und Me sind die Dateien im Windows 9x Registry File (CREG) Format organisiert. Ein Hive ist dabei nicht zwangsweise mit einem Haupt- oder Wurzelschlüssel identisch. So gibt es Wurzelschlüssel, die aus mehreren einzelnen Hives bestehen.

Die Trennung der drei Datenformen ist auch auf Ebene der Registrierung vorhanden. Die Datenbanken existieren in Form von Dateien im Verzeichnis:

„[Root-Laufwerk]/[Windows Verzeichnis]/System32/Config“.

Die Registrierungsdatei für die Benutzereinstellungen befindet sich im jeweiligen Benutzerdaten Verzeichnis unter:

„[Root-Laufwerk]/[Benutzerdaten Verzeichnis]/[Benutzername]/“.

Die Registrierungsdatei für die Benutzerkontenverwaltung wurde mit Windows NT eingeführt. In ihr werden die Einstellungen zu vorhandenen Benutzern des Betriebssystems gespeichert.

Seit Windows 7 werden einige der Benutzerinformationen auch in einem weiteren Benutzerspezifischen Schlüssel gespeichert:

„\AppData\Local\Microsoft\Windows\usrclass.dat“

Eine Auflistung der verwendeten Registrierungsdateien und ihren korrespondierenden Hauptschlüssel findet sich in Abbildung 66.

Typ	Windows 95,98 und ME	Windows NT, XP und höher	korrespondierende Hauptschlüssel
Systemeinstellungen	SYSTEM.DAT	SYSTEM	HKEY_LOCAL_MACHINE/SYSTEM
Softwareeinstellungen	SOFTWARE.DAT	SOFTWARE	HKEY_LOCAL_MACHINE/SOFTWARE
Benutzereinstellungen	USER.DAT	NTUSER.DAT USRCLASS.DAT	HKEY_CURRENT_USER/HKEY_USERS
Benutzerkonten - verwaltung	-	SAM	HKEY_LOCAL_MACHINE/SAM
Benutzerrechte und Richtlinien	-	SECURITY	HKEY_LOCAL_MACHINE/SECURITY

Abbildung 66: Registrierungsdateien und Hauptschlüssel

2.6.3.2 Linux Betriebssystem – Linux Dateisysteme

Linux nutzt als Standard die File System Hierarchy (FSH). Moderne Linux Systeme erlauben Datenträger in mehrere unterschiedlichen unabhängigen Einheiten zu partitionieren, wobei jede physikalische Einheit ein unterschiedliches Dateisystem unterstützen kann. Sie sind Virtual File Systems (VFS) und wurden designt, um verschiedene unterliegende Dateisysteme zu unterstützen. Der Aufbau eines VFSs ist in Abbildung 67 aufgezeigt. Das VFS ist somit die Brücke zwischen den „System Calls“ und den verschiedenen Dateisystemen.

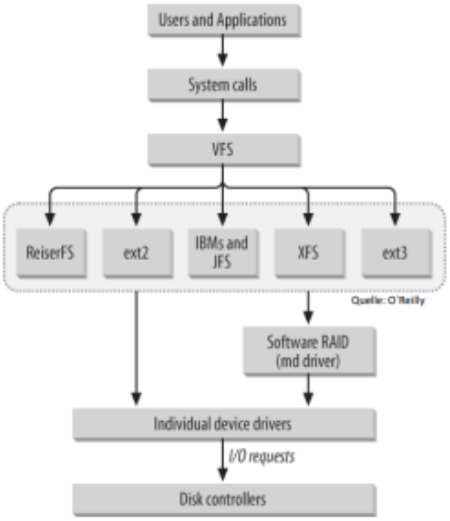


Abbildung 67: Aufbau Virtual File System in Linux

Filesystem Hierarchy Standard

Das im Linux wie im Unix eingesetzte Filesystem Hierarchy Standard (FHS) ist in allen bekannten Distributionen von Linux gleich aufgebaut. In FHS befinden sich alle Dateien und Verzeichnisse unterhalb des Root Directory "/" eingeordnet, auch wenn diese physisch oder virtuell an anderer Stelle abgelegt sind.

Besonderheiten im Dateisystem unter Linux sind dabei, dass Einträge maximal 255 Zeichen groß sind und das System eine Unterscheidung in Groß- und Kleinschreibung unternimmt. Das Hierarchy System stellt dabei auch eine Art Laufplan dar. In Abbildung 68 ist das sichtbar. Wenn man ins Homeverzeichnis des ersten Nutzers möchte, navigiert man sich horizontal durch die Verzeichnisstruktur.

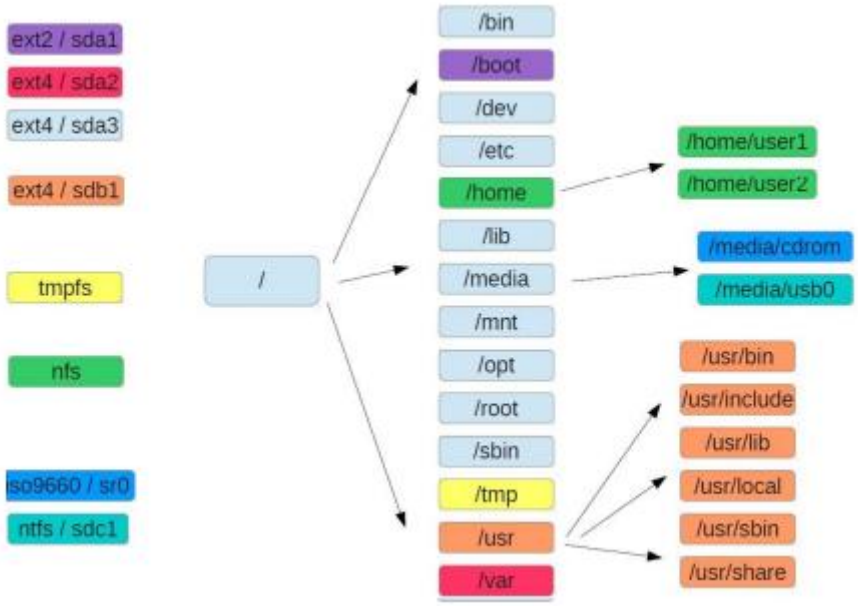


Abbildung 68: File Hierarchy Standard

FHS Für die forensische Untersuchung sind einige der Verzeichnisse von Interesse:

/

- Wurzelverzeichnis
- Soll außer den Verzeichnissen des FHS keine weiteren Dateien enthalten.
- Ausnahme: Kernel und Initrd (kann auch Symlink nach /boot sein)

/boot

- Dateien notwendig für den Bootvorgang:
- /boot/vmlinuz-<version> Linux-Kernel
- /boot/initrd.img-<version> Boot-Ramdisk
- /boot/System.map-<version> Kernel Einsprungtabelle
- /boot/config-<version> Kernel Konfiguration
- /boot/grub/ Konfiguration des grub-Bootloaders

/etc

- /etc/passwd Benutzerkonfiguration
- /etc/group Gruppen Konfiguration
- /etc/shadow Passwortdatei
- /etc/fstab statische Konfiguration der Dateisysteme
- /etc/sysctl.conf Konfiguration Kernelparameter
- /etc/hosts Statische Tabelle Auflösung Rechnernamen
- /etc/inittab Init Konfiguration (System V Init)
- /etc/init.d/ Kontrollskripte für Systemdienste
- /etc/issue OS-Version und Hinweise

/home

- Benutzerverzeichnisse, organisiert in /home/<unsername>
- Bei sehr großen Organisationen auch /home/<division>/<username>
- Nur wenig standardisiert; Benutzer darf frei mit seinem Home-Verzeichnis arbeiten
- Ablageort für Benutzereigene Konfigurationsdateien; verborgen mit <conffile>
- Vorlage für neue Benutzerverzeichnisse in /etc/skel
- /home/<user>/.bashrc Startupbefehle für eine "interactive non-login shell"
- /home/<user>/.profile Startupbefehle für eine "interactive login shell"

/media bzw. /mnt

- /media Mountpunkt für Wechselmedien
- /media/cdrom
- /media/usb0
- /media/floppy
- /mnt Temporärer Mountpunkt (meist von root genutzt)

/root

- Home-Verzeichnis für den Superuser
- relevant bei unberechtigten Rootzugriff

/srv

- Daten, die von System als Server angeboten werden.
- Achtung: Konkurriert je nach Distribution mit /var (Webserver mitunter unter/var/www)
- /srv/www Webseiten
- /srv/ftp FTP-Verzeichnis
- /srv/samba Samba-Share

/var

- Zweck: Trennung variabler Daten von /usr.
- Enthält Logging-Daten, Print / Mail-Spool, Caches, etc.
- /var/cache Cachedaten
- /var/lib Statusdaten
- /var/spool Spooldaten (Printjobs etc.)
- /var/tmp Temporäre Daten, bleibt bei Reboot erhalten
- /var/log Logfiles
- /var/mail Mailboxen
- /var/local Variable Daten für /usr/local
- /var/opt Variable Daten für /opt
- /var/lock Lockfiles (Dateisperren, die gleichzeitiges Bearbeiten verhindern)
- /var/run Runtime data
- /var/www Webseiten

Das Extended File System

Das Extended File System, kurz ext, ist das Standarddateisystem in vielen Linux Distributionen und der Nachfolger des Unix File Systems, UFS. Das grundlegende Designprinzip von ext ist Geschwindigkeit und Zuverlässigkeit. Dafür wurden Kopien zentraler Datenstrukturen mehrfach auf dem Datenträger verteilt. Zudem werden die Datenblöcke einer Datei nahe beieinander gehalten, um so die Wege des Lesekopfes zu minimieren.

Das Extended File System existiert in vier Versionen, mit unterschiedlichen Bestandteilen:

- ext: wurde im April 1992 als Nachfolger von UFS (UnixFileSystem) eingeführt und quasi sofort von ext2 abgelöst.
- ext2: wurde als Nachfolger von ext im Januar 1993 eingeführt und war viele Jahre das Standarddateisystem für Linux. Es ist heute noch weit verbreitet.
- ext3: wurde im November 2001 eingeführt und brachte Journaling in die Extended Filesystem Familie. Das Journal ist eine Dateistruktur, in die Metadaten (optional die Nutzdaten) geschrieben werden, bevor sie auf das tatsächliche Dateisystem geschrieben werden.
- ext4: Der Nachfolger von ext3 wurde im Oktober 2008 released, dieser führte Extends in die ext Reihe ein. Extends bringen Geschwindigkeitsvorteile bei der Verwaltung großer Dateien und beugt der Fragmentierung vor.

Die ext2,3,4 Dateisysteme sind nicht die einzigen Dateisysteme, welche für Linux Distributionen existieren. Jede Distribution und jeder Benutzer kann frei entscheiden, welches Dateisystem verwendet wird.

Ext ist ein offenes Dateisystem. Es gibt viele zusätzliche Features, die in drei Kategorien fallen:

- **Compatible Features**: Dateisysteme mit diesen Features lassen sich uneingeschränkt nutzen (Auf- und Abwärtskompatibel siehe Abbildung 69)
- **Incompatible Features**: Wenn das Betriebssystem das Feature nicht unterstützt, sollte das Dateisystem nicht gemountet werden (Beispiel: Kompression).
- **Read only Features**: Wenn ein Betriebssystem ein solches Feature nicht unterstützt, kann es das Dateisystem dennoch lesen, sollte es aber nichtschreiben (Beispiel: B-Baum Verzeichnissortierung).

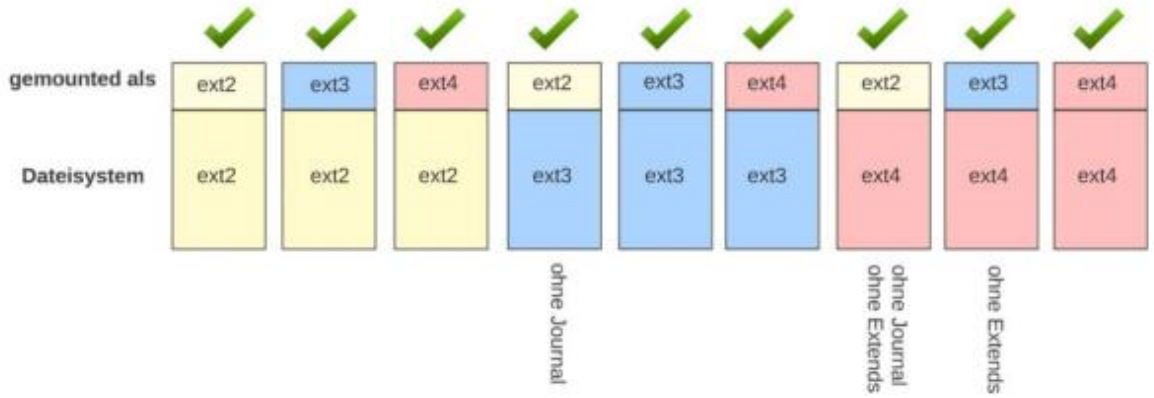


Abbildung 69: Auf- und Abwärtskompatibilität von ext

Das ext-Dateisystem besteht aus einem Bootblock und mehreren Blockgruppen in der die Partition mit dem ext-Dateisystem aufgeteilt wird. Der Bootblock ist immer 1024 Byte groß und enthält nur Boot-Code, dies aber auch nur selten. Insbesondere ist er aber ohne jeglichen forensischen Wert. Eine Partition ist aufgeteilt in einzelne Sektionen gleicher Größe, mit Ausnahme der letzten Sektion. Diese Sektionen heißen Blockgruppen. Jede Blockgruppe besitzt die gleiche Anzahl an Blöcken, welche für das Speichern der Verzeichniseinträge, Metadaten und Dateiinhalte zuständig sind. Blockgruppen sind vergleichbar mit Rängen in einem Theater. Ein Theater ist in mehrere Ränge aufgeteilt, die alle die gleiche Anzahl an Sitzplätzen aufweisen.

Linux Betriebssystemspezifika

Die Unix Familie, aus der Linux letztlich abstammt, ist breit gefächert. Auch Mac OS X hat seinen Ursprung im Unix Betriebssystem. Linux ist in der Lage fast jedes Dateisystem zu mounten (mit entsprechendem Treiber) und einzulesen. Neben den nativ verwendeten Dateisystem wie EXT und FAT, gibt etwa Module für NTFS, HFS+, VmwareFS 5, ReiserFS, NFS, UFS, XFS, YAFFS und ExFAT. Für das Mounten von diesen Dateisystem wird eine Technik genutzt die sich FUSE (Filesystem in Userspace) nennt.

FUSE ist ein Kernel-Modul für Unix- Systeme, das es ermöglicht, Dateisystem-Treiber aus dem Kernel-Mode in den User-Mode zu verlagern. FUSE ist das laufwerksspezifische Modul (für die angeschlossene Hardware) und benötigt zur Einbindung des darauf enthaltenen Dateisystems zusätzlich den jeweils passenden dateisystemspezifischen Treiber. Der wohl bekannteste ist NTFS-3G.

2.6.2.3 Mac OS Dateisystem – HFS/HFS+

Das Dateisystem HFS (Hierarchical File System) ist ein von Apple entwickeltes Dateisystem. Es wurde 1995 vorgestellt und ist seither um verschiedene Funktionen erweitert worden.

- Mac OS Standard
  - im September 1995 von Apple veröffentlicht als proprietäres Format
  - sehr gut dokumentiert deshalb für die meisten modernen Betriebssysteme lesbar
- Mac OS Extended
  - 1998 Nachfolger HFS+
  - effiziente Zuweisungen von Speicherplatz in HFS
  - weitere Verbesserungen und zusätzliche Features

- Mac OS Extended (Journaled)
    - OSX 10.3 Panther wurde 2003 wurde Journaling eingeführt abgekürzt als HFSJ
    - das Journal ist nicht Teil des Dateisystems, sondern ein virtuelles Dateisystem (VFS)in Form zweier Dateien .journal und .journal_info_block
    - ältere Versionen von Mac OS/Mac OS X können das Dateisystem verwenden ohne das Journal
- Mac OS Extended (Journaled, Groß-/Kleinschreibung)
    - HFS+ auf Mac-Rechnern standardmäßig kein Unterschied in Groß und Kleinschreibung
    - auf iOS-Geräten erweiterte Dateisystem-Variante (Abkürzung HFSX) Unterscheidung von Groß- und Kleinbuchstaben (NFD-Normalisierung bei Unicode)
    - Kein HFS-Wrapper mehr unterstüzt
- FileVault
    - 2010 in OSX 10.7 wurde die Logical Volume Encryption FileVault2 eingeführt
- APFS (Apple File System)
    - 2017 eingeführt als Nachfolger von HFS+ mit Mac OS X 10.13 und iOS 10.3
    - vom Aufbau an HFS angelehnt mit vielen Extras und Erweiterungen versehen

Die forensische Untersuchung vom Apple Filesystem APFS beruhte im Wesentlichen auf Reverse Engineering des Dateisystems. Eine offizielle Technical Note (TN) wie von HFS+ existierte lange Zeit nicht. Mittlerweile veröffentlichte Apple eine Developer Information zu APFS:

https://developer.apple.com/support/downloads/Apple-File-System-Reference.pdf

Die tatsächliche Funktionsweise des APFS ist aus dieser Developer Information jedoch auch nicht umfassend feststellbar.

Das neue APFS-Dateisystem wartet mit einer Reihe von Veränderungen auf, die es vom HFS+ Dateisystem unterscheiden. Unabhängig davon sind bekannte Strukturen aus dem HFS+ Dateisystem übernommen wurden, weil sie funktionieren, gut dokumentiert und auch bereits implementiert sind und eine Konvertierung von HFS+ in APFS effizienter gestaltet werden kann.

Betriebssystem Mac OS X

Das auf Unix basierende Mac OS X ist die zehnte Ausgabe des Apple eigenen Betriebssystems für Macintosh Computer. Die ursprünglich auf Motorola Chipsätzen basierten Apple Computer werden heute ausschließlich mit Intel Chipsätzen hergestellt. Im September 2000 wurde die erste OSX-Beta (Kodiak) an die Entwickler verteilt. Bis einschließlich Version 10.7 hieß das Betriebssystem Mac OS X ab 10.8 wurde es nur noch OS X genannt mit der Einführung von 10.12 wurde es erneut umbenannt und heißt nun macOS.

OSX ist in vier Schichten aufgebaut (siehe Abbildung 70):

1. Benutzerebene - Aqua, die grafische Benutzerschnittstelle (GUI)

2. Anwendungsprogrammierebene - Programmierschnittstellen (APIs) wie Cocoa (und früher Carbon), Java

3. Bereitstellungsebene - Grafik-Subsystem (Quartz mit Quartz Compositor, OpenGL), Audio/Video (QuickTime) etc.

4. Basisebene - Darwin, das Kern-Betriebssystem

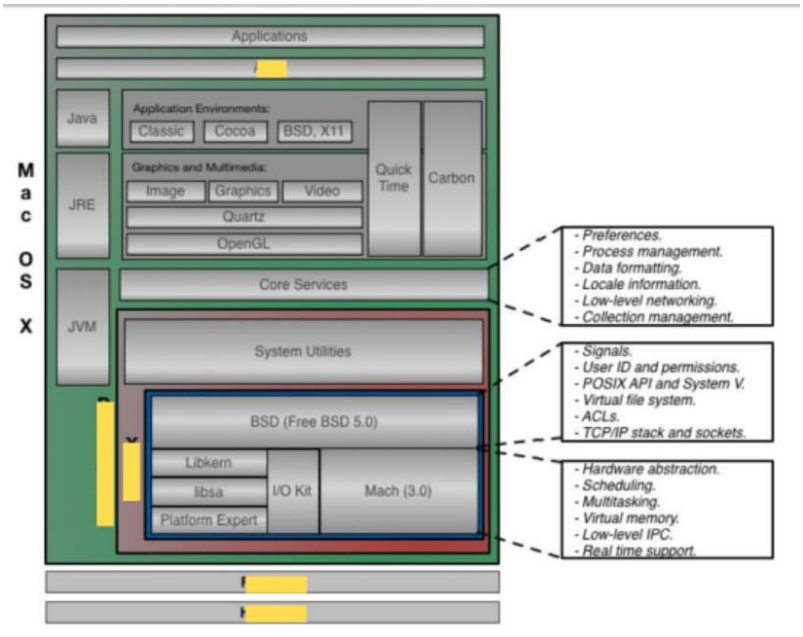


Abbildung 70: Aufbau Mac OS X

OSX ist ein Nachkomme von NeXTSTEP und genau genommen eine (proprietäre) Software-Distribution, wobei Darwin, die Basisebene von BSD abgeleitet ist, und damit ein (freies) Unix, das eigentliche Betriebssystem ist. Durch Darwin (vererbt aus BSD) verfügt OS X über Fähigkeiten wie Speicherplatzschutz, präemptives Multitasking, Mehrbenutzerfähigkeit, erweitertes Speichermanagement und symmetrisches Multiprocessing (SMP). Darwin wurde unter die quelloffene Lizenz Apple Public Source License gestellt. Der Kernel wurde gegenüber NeXTStep vollkommen überarbeitet - während NeXTStep noch einen reinen Mach-Mikrokernel verwendete, setzt OS X bzw. Darwin auf einen sogenannten Hybridkernel: Dabei werden einige Funktionen in den Kernel integriert, allerdings nicht so viele wie bei einem monolithischen Kernel. Als Basis Kernel wurde weiterhin Mach verwendet und mit Teilen des monolithischen FreeBSDKernel ergänzt. Der Kernel heißt XNU (X is Not Unix).

Unterstützte Dateisysteme: Mac OS X nutzt das Dateisystem HFS und dessen Erweiterung HFS+. Dieses von Apple entwickelte Dateisystem wird auch für externe Datenträger verwendet und kann mit einem Windows basierten System nicht gelesen werden. Mac OS X kann auch das FAT12/16/32 Dateisystem lesen und schreiben. Damit ist es möglich externe Datenträger, wie Speicherkarten und USB-Sticks für den Multibetriebssystembetrieb einzurichten. Seit der Einführung von macOS X 10.12 wurde das Apple Dateisystem HFS+ durch APFS (Apple File System) ersetzt. OS X unterstützt verschiedene weitere lokale Dateisysteme wie NTFS, exFAT, UFS, UDF, sowie ZFS (die beiden letztgenannten nur lesend). Der Schreibzugriff auf NTFS wurde in Mac OS X 10.6 hinzugefügt, ist standardmäßig jedoch abgeschaltet und muss durch einen Eintrag in fstab aktiviert werden. Unterstützte Netzwerkdateisysteme sind AFP, FTP, NFS, SMB/CIFS und Web-DAV. Mit der Zusatzsoftware MacFUSE und entsprechenden Plugins wie NTFS-3G (für Schreib/Lesezugriff auf NTFS-Datenträger bis OS X 10.6) sind weitere Dateisystemtypen unter OS X verfügbar. Hierbei werden zusätzlich eine Menge für die Forensik relevante Dateisysteme nutzbar, wie durch das Mounten von EWF-Images und BDE- Volumes, etc.

Benutzerverwaltung: Dem Ursprung von Mac OS X angelehnt ist das Betriebssystem Multiuserfähig und bietet eine entsprechende Benutzerverwaltung mit Benutzern und Gruppen an. OSX

unterscheidet zwischen normalen Benutzern (user), Systemverwalter (admin) und dem Superuser (root). Normale Benutzer können keine Änderungen am System vornehmen oder Software außerhalb ihrer Benutzerordner installieren. Alle von Usern gestartete Programme werden mit den entsprechenden Nutzerrechten des Users ausgeführt. Die Benutzer der Gruppe admin verfügen über weitergehende Rechte, sie dürfen systemweite Einstellungen vornehmen, Software installieren und verfügen über Schreibzugriff auf diverse Systemverzeichnisse. Nur nach gesonderten Authentifizierungen können tiefergreifende Änderungen am System vorgenommen werden. Ein nutzbares Root- Benutzerkonto, das dauerhaft über Berechtigungen des Superusers verfügt, gibt es nach einer Systeminstallation nicht. Zwar gibt es einen Benutzer „root“, dieser ist jedoch standardmäßig deaktiviert. Kann jedoch explizit aktiviert werden.

OS X speichert jede Menge Informationen, die für den IT-Forensiker von Interesse sein können. Diese Informationen sind in einer ganzen Reihe verschiedener Formate abgelegt. Einige sind leicht zu interpretieren, wie Plain Text, XML oder Datenbanken. Andere haben aber proprietäre Binärformate. Einige Dateiformate sind gut dokumentiert, andere leider gar nicht und mussten Reverse Engineered werden. Für die meisten Binärformate bringt OSX aber eigene Viewer mit. Das ist ein Grund, dass sich Apple Rechner am besten auf einem Apple auswerten lassen.

3 Erster Angriff

Der erste Angriff im Bereich der IT-Forensik bedient sich den bereits behandelten Prozessen aus Kapitel 1.4. Die Prozessschritte strategische Vorbereitung, operative Vorbereitung und Datensammlung lassen sich als erster Angriff zusammenfassen. Im Fokus steht die Vorbereitung für eine IT-forensische Analyse. Nach dem ersten Angriff erfolgen äquivalent zu den Prozessen die Analyse-, Auswertungs- und Präsentationsschritte. Die größte Herausforderung ist hierbei die ständig wachsende Komplexität informationstechnischer Systeme. Aus diesem Grund ist der erste Angriff von höchster Bedeutung: Je strukturierter die Vorbereitung, desto einfacher die Analyse.

3.1 Strategische Vorbereitung

Die strategische Vorbereitung in der IT-Forensik umfasst sämtliche Maßnahmen, die im Vorfeld eines potenziellen Ereignisses geplant werden. Dies beinhaltet die Auswahl und gründliche Prüfung verschiedener Sicherungstools sowie die Entwicklung einer detaillierten Vorgehensplanung. Zusätzlich dazu werden Hardware- und Software-Ressourcen vorbereitet, darunter Werkzeuge und Computersysteme, um eine effiziente Durchführung der forensischen Untersuchung zu gewährleisten. Ein Beispiel hierfür ist die sorgfältige Auswahl und Konfiguration von Datenerfassungsgeräten und Analysewerkzeugen, um sicherzustellen, dass alle relevanten Informationen erfasst und ausgewertet werden können.

Der Analysecomputer bildet die Grundlage für forensische Untersuchungen und ist ein eigenständiges Gerät, das im Idealfall vom Standardbüronetzwerk und Internet getrennt ist. Seine Ausstattung umfasst einen Mehrkern-Prozessor sowie maximalen Hauptspeicher, um eine schnelle und effiziente Verarbeitung großer Datenmengen zu ermöglichen. Er verfügt über erweiterte Busanschlussmöglichkeiten wie USB 2.0, USB 3.0, SATA, Firewire, Floppy Disk, DVD/Blu-ray und Dual-Monitor-Unterstützung. Zusätzlich bietet er Einschübe für SATA-Laufwerke zur einfachen Datenspeicherung und -übertragung. Mit einem Dual-Betriebssystem ausgestattet, ermöglicht der Analysecomputer die Durchführung von Untersuchungen in verschiedenen Umgebungen und Betriebssystemen. Ein aktueller Virenscanner und eine Firewall sind installiert, um die Integrität des Systems zu gewährleisten, insbesondere wenn es mit Netzwerken verbunden ist.

Für Außeneinsätze sind geeignete transportable Datensicherungsworkstations unerlässlich. Diese Workstations sind darauf ausgelegt, forensische Untersuchungen vor Ort durchzuführen und Daten sicher zu erfassen, ohne die Integrität der Beweismittel zu beeinträchtigen. Ihr Zweck besteht darin, eine zuverlässige und effiziente Methode zur Datensicherung und Analyse zu bieten, selbst unter herausfordernden Umgebungsbedingungen.

Abbildung 71: Arbeitsmittel in Abhängigkeit zum Datensicherungsumfang (DSU)

Bei der Planung von Außeneinsätzen ist es entscheidend, den Zweck und den Datensicherungsumfang (DSU) der Beweiserhebung im Voraus abzuschätzen. Dies umfasst die Identifizierung potenziell relevanter Datenquellen sowie die Einschätzung der erforderlichen Ressourcen und Zeitrahmen für die Untersuchung. In Abbildung 71 sind verschiedene Datensicherungswerkzeuge in Abhängigkeit des Umfangs der zu sichernden Daten abgebildet. Durch eine gründliche Vorbereitung und Abschätzung können Forensikteams sicherstellen, dass sie über die geeigneten Werkzeuge und Strategien verfügen, um die gesteckten Ziele effektiv zu erreichen.

Die strategische Vorbereitung erfordert insbesondere die Erstellung eines Forensik-Handbuchs. Ein Forensik-Handbuch dient als Leitfaden für forensische Untersuchungen und enthält wichtige Richtlinien, Verfahren und Best Practices. Es bietet einen klaren Rahmen für die Durchführung von Untersuchungen und erleichtert die Konsistenz und Genauigkeit der Ergebnisse. Insbesondere Aspekte im Bereich der Risikobewertung und Priorisierung sollten hier bereits definiert sein, um einen Einsatz zu erleichtern. Eine gründliche Risikobewertung ermöglicht es, potenzielle Bedrohungen und Schwachstellen zu identifizieren und zu priorisieren. Dies hilft dabei, Ressourcen und Maßnahmen gezielt dort einzusetzen, wo sie am dringendsten benötigt werden. Zusätzlich ist es wichtig, sicherzustellen, dass alle forensischen Untersuchungen den geltenden rechtlichen und regulatorischen Anforderungen entsprechen. Dies kann die Einhaltung von Datenschutzbestimmungen, rechtlichen Richtlinien und internen Unternehmensrichtlinien umfassen. Das Handbuch umfasst weitere Anweisungen und Aspekte für die folgenden Schritte des forensischen Prozesses und bildet eine unverzichtbare Arbeitsgrundlage.

3.2 Operative Vorbereitung

Die operative Vorbereitung in der IT-Forensik umfasst sämtliche Maßnahmen, die nach dem Eintreten eines Vorfalls und vor der eigentlichen Datensammlung durchgeführt werden. Dies beinhaltet insbesondere die systematische Suche, Identifikation und Beschriftung potenziell relevanter Datenquellen. Zu diesen Quellen können Computer, Mobilgeräte, USB-Sticks, externe Festplatten, aber auch volatile Speicher wie RAM, Routerkonfigurationen, Netzwerkstatistiken und Logfiles gehören.

Die Suche am Ereignisort stellt stets eine Ausnahmesituation dar, da sie für den Betroffenen unerwartet ist und möglicherweise auf Widerstand oder Unwillen stößt. Zudem müssen Forensikteams in fremden privaten Räumlichkeiten arbeiten, was zusätzliche Sensibilität erfordert. Für die Forensiker vor Ort ist es entscheidend, einen schnellen Überblick über die erforderlichen Maßnahmen zu erhalten, um effektiv handeln zu können. Dies erfordert ein hohes Maß an Professionalität und Erfahrung, um die Situation angemessen zu bewerten und geeignete Schritte einzuleiten.

Obwohl jede Durchsuchung, Datensicherung und Beweiserhebung je nach Sachverhalt unterschiedlich ist, gibt es grundlegende Dinge, die beachtet werden müssen. Dazu gehören die Einhaltung rechtlicher und ethischer Standards, die Sicherstellung der Integrität der Beweismittel, die Dokumentation aller

durchgeführten Maßnahmen sowie die Minimierung möglicher Störungen oder Beeinträchtigungen des untersuchten Umfelds. Darüber hinaus ist es wichtig, die Privatsphäre und Rechte aller Beteiligten zu respektieren und sicherzustellen, dass die Untersuchung transparent und fair durchgeführt wird. Durch eine gründliche Planung, klare Kommunikation und Zusammenarbeit mit den Betroffenen kann eine effektive und gerechte forensische Untersuchung gewährleistet werden.

Das Augenmerk bei der Suche am Ereignisort liegt auf der sorgfältigen Überprüfung aller potenziellen Quellen und Hinweise auf verborgene Geräte oder Beweismittel. Dazu gehört die gründliche Inspektion aller angeschlossenen Geräte, wobei insbesondere auf lose Verkabelungen wie USB, Firewire oder Ethernet geachtet wird, da diese auf das Vorhandensein versteckter Geräte hinweisen können. Auch Netzteile ohne zugehörige Geräte sowie Verpackungen mit Hinweisen auf Geräte, wie Seriennummern oder PIN-Codes, werden genau untersucht. Besonderes Augenmerk wird auf USB-Speicher gelegt, da sie aufgrund ihrer geringen Größe und vielfältigen Formen praktisch überall versteckt werden können, beispielsweise als Schlüsselanhänger oder in anderen Alltagsgegenständen. Es werden auch Abdrücke von Geräten, Literatur zu bestimmten Sachgebieten und Zettel mit handschriftlichen Notizen im unmittelbaren Umfeld des Computers untersucht, da sie möglicherweise wichtige Informationen wie Passwörter oder Hinweise auf Tätigkeiten enthalten könnten.

3.2.1 Zu erhebende Informationen

Zur effektiven Durchführung einer forensischen Untersuchung ist es entscheidend, frühzeitig Informationen zu verschiedenen Punkten zu erheben:

- Zum Netzwerk: Es ist wichtig, Informationen über die Netzwerktopologie, die Konfiguration von Routern und Switches sowie die Verbindungen zu anderen Netzwerken zu sammeln. Dies umfasst auch Informationen über Firewalls, VPNs und andere Sicherheitsvorkehrungen, die das Netzwerk schützen.
- Zu den Geräten: Eine genaue Auflistung aller beteiligten Geräte, einschließlich Computer, Server, Router, Switches, Mobilgeräte und Speichergeräte, ist von entscheidender Bedeutung. Hierbei ist es wichtig, Angaben zu den Herstellern, Modellen, Seriennummern und Konfigurationen der Geräte zu erfassen.
- Zum Nutzerverhalten: Durch die Analyse von Protokollen, Logdateien und anderen Aufzeichnungen können Informationen über das Nutzerverhalten gesammelt werden. Dies kann Aufschluss über die Aktivitäten und Interaktionen der Benutzer mit den Systemen geben und dabei helfen, verdächtige Aktivitäten zu identifizieren.
- Mögliche Absicherungen durch den Betroffenen: Informationen über Zugangskennungen, Passwörter, Sperrcodes und andere Sicherheitsvorkehrungen, die vom Betroffenen implementiert wurden, sind von großer Bedeutung. Diese Informationen können dabei helfen, geschützte Bereiche zu entschlüsseln und auf potenzielle Beweismittel zuzugreifen.

Es ist auch wichtig, Personen getrennt zu befragen, um eventuelle Widersprüche in den Aussagen zu erkennen und eine umfassende Darstellung der Ereignisse zu erhalten. Dabei ist darauf zu achten, den Betroffenen nicht aufgrund von Kosten oder anderen Faktoren unter Druck zu setzen.

Im Unternehmensumfeld sind Absprachen mit den IT-Verantwortlichen unerlässlich, um wichtige Informationen zu erhalten, die für eine forensische Untersuchung relevant sind. Dazu gehören:

- Genutzte Betriebssystemarchitektur: Informationen über die verwendeten Betriebssysteme auf den verschiedenen Geräten im Unternehmensnetzwerk sind entscheidend, um die forensische Analyse entsprechend anzupassen.
- Genutzte Netzwerktechnologie: Kenntnisse über die Netzwerktopologie, verwendete Netzwerkprotokolle und -geräte sowie mögliche Sicherheitsvorkehrungen wie Firewalls und Intrusion Detection Systems (IDS) sind wichtig, um potenzielle Angriffsvektoren zu identifizieren.
- Servertechnologie: Informationen über die Serverinfrastruktur, einschließlich Servertypen, Betriebssysteme, Dienste und Konfigurationen, sind wesentlich für die Analyse von Netzwerkaktivitäten und -daten.
- Backuptechnologien: Ein Verständnis der eingesetzten Backup-Lösungen und -Verfahren ermöglicht es, potenzielle Sicherungskopien von Beweismitteln zu identifizieren und zu sichern.
- Spezielle Softwareanwendungen: Informationen über spezifische Unternehmensanwendungen wie Customer Relationship Management (CRM), Buchhaltungssoftware und andere geschäftsrelevante Programme sind wichtig für die Identifizierung und Analyse von relevanten Daten.
- Zugriffsschutzmanagement und IT-Sicherheitsmanagement: Kenntnisse über Zugriffssteuerungsmechanismen, Passwortrichtlinien, Verschlüsselungsverfahren und andere Sicherheitsmaßnahmen sind entscheidend für die Bewertung der Sicherheitslage und potenzieller Schwachstellen.
- Meldepflichten: Informationen über interne und externe Meldepflichten im Falle von Sicherheitsvorfällen sind wichtig, um rechtliche Anforderungen zu erfüllen und angemessen auf Vorfälle zu reagieren.

Zudem ist der Zugang zu verschiedenen Ressourcen im Netzwerk von Bedeutung, darunter Netzwerkressourcen, Datenablagen, Backups und Datenbanken. Der Zugriff auf diese Ressourcen ermöglicht es Forensikern, potenzielle Beweismittel zu identifizieren, zu sichern und zu analysieren, um den Umfang des Vorfalls zu verstehen und geeignete Gegenmaßnahmen zu ergreifen. Daher sind Absprachen mit den IT-Verantwortlichen unerlässlich, um diese Informationen zu erhalten.

3.2.2 Priorisierung

In forensischen Untersuchungen ist die Priorisierung von Daten von grundlegender Bedeutung, um effizient Ressourcen einzusetzen und wichtige Beweismittel zu identifizieren und zu sichern. Dabei ist es ratsam, eine umfassende Datensicherung durchzuführen, um sicherzustellen, dass potenziell relevante Beweismittel erfasst werden. Dies umfasst nicht nur Dateien und Ordner, sondern auch Protokolldateien, Systemeinstellungen, Metadaten und andere Informationen, die für die forensische Analyse von Bedeutung sein könnten. Die Datensicherung erfolgt oft in vielen einzelnen Schritten, da verschiedene Arten von Daten unterschiedliche Sicherungsverfahren erfordern können. Ein wichtiger Aspekt bei der Priorisierung ist die Flüchtigkeit von Daten, insbesondere in Bezug auf volatile Speicher wie RAM, die bei einem Neustart oder Herunterfahren des Systems verloren gehen können. Daher ist es wichtig, diese Daten frühzeitig zu sichern. Eine sorgfältige Priorisierung basierend auf der Dringlichkeit, der Relevanz für den Fall, der potenziellen Flüchtigkeit oder anderen Faktoren ist unerlässlich, um die wichtigsten Daten zu identifizieren und zu sichern und eine umfassende forensische Analyse zu ermöglichen.

Eine mögliche Sicherungsreihenfolge könnte wie folgt aussehen:

1. CPU-Register, Cache-Speicher
2. Routingtabellen, ARP-Cache, Prozessliste, Netzwerkstatus, Kerneldaten, Hauptspeicherinhalt
3. temporäre Dateisysteme, SWAP-Bereiche, andere temporäre Daten
4. Massenspeicherinhalte (logisch oder physikalisch)
5. Auf anderen Systemen verfügbare Log- und Monitoringdaten des untersuchten Systems
6. Physikalische Konfiguration, Netzwerkkonfiguration
7. Archivierte Medien (Datensicherungen)

Fehlerquellen bei forensischen Untersuchungen können zu erheblichen Problemen führen und die Integrität der Beweise beeinträchtigen. Einige der häufigsten Fehlerquellen sind:

- Herunterfahren des Rechners: Durch das Herunterfahren des Computers können potenziell wichtige Beweise verloren gehen, insbesondere volatile Daten im Arbeitsspeicher. Es ist wichtig, den Rechner nur dann herunterzufahren, wenn dies unbedingt erforderlich ist und geeignete Maßnahmen ergriffen wurden, um die Datenintegrität zu gewährleisten.
- Vertrauen in Programme und Tools auf dem untersuchten Computer: Das Vertrauen in Programme und Tools, die auf dem untersuchten Computer vorhanden sind, birgt das Risiko der Kontamination oder Manipulation von Beweismitteln. Forensiker sollten ihre benötigten Programme auf einem schreibgeschützten Medium mitbringen und ausschließlich diese nutzen, um Daten aus dem System zu extrahieren.
- Starten von Programmen, die Zugriffszeitstempel verändern können: Programme wie "tar" oder "xcopy" haben das Potenzial, Zugriffszeitstempel auf Dateien zu verändern, was die forensische Analyse erschweren kann. Daher ist Vorsicht geboten und es sollten geeignete Werkzeuge verwendet werden, die die Integrität der Daten bewahren.
- System vom Netz nehmen: Das Trennen des Systems vom Netzwerk kann dazu führen, dass potenziell wichtige Netzwerkdaten verloren gehen. Es ist wichtig, diese Maßnahme nur nach gründlicher Planung und unter Berücksichtigung der möglichen Auswirkungen durchzuführen.
- Wipe-Skripte oder Fernzugriff zur Datenlöschung: Die versehentliche Verwendung von Wipe-Skripten oder Fernzugriffsmöglichkeiten zur Datenlöschung kann zu irreparablen Datenverlusten führen und die forensische Untersuchung erheblich beeinträchtigen. Daher ist äußerste Vorsicht geboten und der Zugriff auf solche Werkzeuge sollte streng kontrolliert werden.

Ein Beispielhafter Ablaufplan zur forensischen Sicherung ist in Abbildung 72 dargestellt:

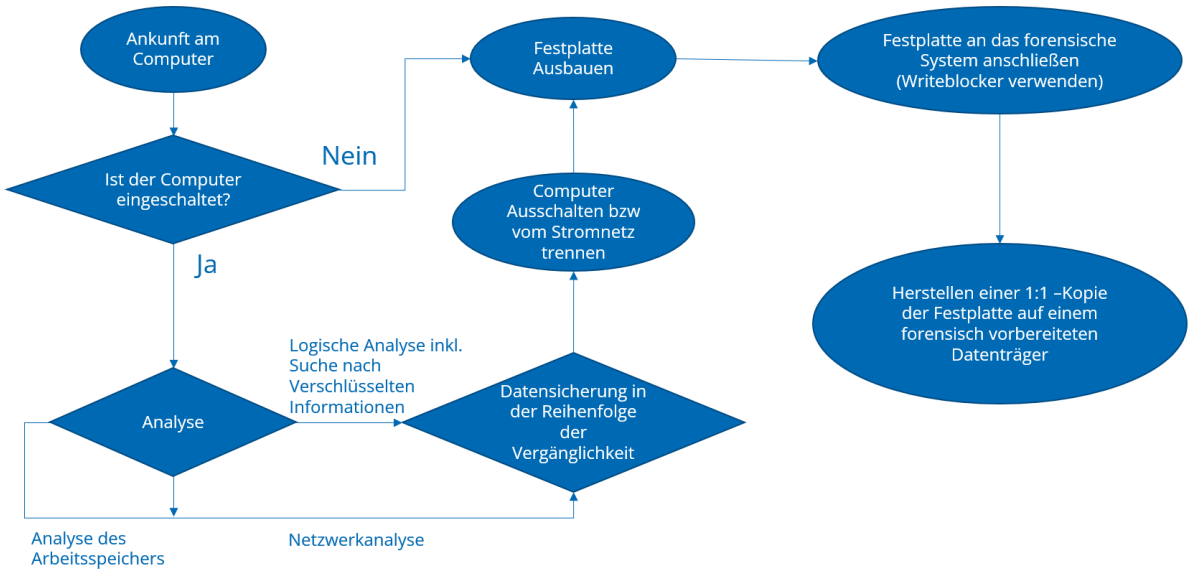


Abbildung 72: Ablaufplan der forensischen Sicherung

3.2.3 Triage-Forensik

Abbildung 73: Triage-Forensik als Methode der Priorisierung

Im medizinischen Kontext bezeichnet "Triage" die Selektion von Verletzten basierend auf ihren Überlebenschancen und der Schwere ihrer Verletzungen. Dies umfasst das Festlegen der Reihenfolge, in der die Verletzten behandelt werden sollen, um eine effiziente Nutzung der verfügbaren Ressourcen sicherzustellen und die bestmögliche Versorgung der Patienten zu gewährleisten.

Im Bereich der digitalen Forensik bezieht sich "Triage" auf die Selektion elektronischer Geräte und Internetquellen nach der Relevanz für eine systematische formale Untersuchung zur Beweisermittlung. Dabei werden potenziell relevante Quellen identifiziert und priorisiert, um Ressourcen effizient einzusetzen und die forensische Analyse auf die bedeutendsten Beweismittel zu konzentrieren. Dies ermöglicht es Forensikern, schnell eine erste Einschätzung vorzunehmen und die

Untersuchung auf die wichtigsten Bereiche zu fokussieren, um den Umfang des Falls zu verstehen und angemessen darauf zu reagieren.

Die Überlastung der Untersuchenden in der forensischen Analyse digitaler Beweise ist ein bekanntes Problem, das eine effiziente Vorgehensweise erfordert. Zur Bewältigung dieses Problems wird oft eine Triage durchgeführt, um zu bestimmen, welche Geräte von technischer Bedeutung sind und welche zunächst überprüft werden müssen. Diese Triage kann entweder direkt am Tatort oder im Labor durchgeführt werden und umfasst die Sammlung, Zusammenstellung, Identifizierung und Priorisierung relevanter digitaler Beweise, möglicherweise mit einer ersten Analyse.

Um eine schnelle Triage durchführen zu können, werden spezielle Tools verwendet, die einen schnellen Überblick über die vorhandenen Daten liefern, jedoch keine detaillierte Tiefenanalyse ermöglichen. Diese Tools basieren auf verschiedenen Quellen wie Cache-Dateien, Browserverlauf, Login-Daten, gespeicherten Zugangsdaten, Cloud-Speicher und Verbindungsprotokollen. Einige Beispiele für Tools, die in der forensischen Triage eingesetzt werden können, sind **Magnet Outrider**, **ADF Solutions Triage-G2**, **Cyan Forensics Rapid Digital Forensic Triage** oder **Spektor Forensics Triage** Tool. Diese Tools helfen dabei, die Arbeitslast der forensischen Analysten zu reduzieren, indem sie eine schnelle Vorprüfung der Daten durchführen und die Priorisierung für eine detailliertere Analyse erleichtern.

3.3 Bedeutung der Datenintegrität und Chain of Custody

Die Datenintegrität spielt im forensischen Prozess eine entscheidende Rolle, da technische Daten anfällig für Veränderungen und Manipulationen sind, die schwer nachweisbar sein können. Digitale Spuren können leicht verändert werden, was die Glaubwürdigkeit und Zuverlässigkeit der Beweise beeinträchtigen kann. Um die Datenintegrität zu gewährleisten, werden mehrere Kopien der Daten (Duplikationen) erstellt, wobei die Originalkopie archiviert wird. Dies ermöglicht es, die Integrität der Daten zu überprüfen und Veränderungen nachzuverfolgen. Anforderungen an die forensische Duplikation sind:

- Physische Kopie: Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben;
- Fehlerbehandlung: Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden;
- Vollständigkeit des Abbildes: Reservierte Bereiche von Massenspeichern müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;
- Unveränderheit Integrität: Die Erstellung des Abbildes muss mit der Berechnung einer kryptografischen Checksumme abgeschlossen werden, um die Unveränderheit (Integrität) des Abbildes nachweisen zu können.

Bei der Erstellung von Kopien ist es wichtig, einen Schreibschutzadapter zu verwenden, wo immer dies möglich ist. Ausnahmen hiervon sind beispielsweise laufende Systeme mit Vollverschlüsselung, Sicherungen aus Cloud-Speichern, großen Speichersystemen oder Rechenzentren. In diesen Fällen ist eine lückenlose Dokumentation und die Einhaltung eines Vier-Augen-Prinzips bei der Erstellung der Kopie ratsam, um sicherzustellen, dass die Integrität der Daten gewahrt bleibt und potenzielle Veränderungen nachvollziehbar sind.

Die Integrität hat einen wesentlichen Einfluss auf die Zuverlässigkeit von Untersuchungsergebnissen. Integrität von Daten befasst sich mit der Unveränderheit. Spuren, die während des Sicherungsprozesses gefunden oder ermittelt werden, sowie jegliche digitale Daten dürfen nicht unbemerkt verändert werden. Die Integrität soll dies sicherstellen und bedient sich dabei beispielsweise Prüfsummen, die mittels Hashverfahren erstellt werden. Hash-Funktionen sind im Kapitel 2.3 erklärt. Die Prüfsumme, also z.B. der Hashwert einer Datei oder eines Datenträgers wird nach der Sicherung erstellt. Im Verlauf der Analyse oder auch im Nachhinein können von den gleichen Medien die Hashwerte erneut erzeugt werden. Sollte die Datei oder der Datenträger in dieser Zeitspanne verändert wurden sein, so ist auch der Hashwert ein anderer. Deshalb wird er auch als Prüfsumme bezeichnet, weil er zur Überprüfung der Integrität genutzt wird. Wenn die Datenintegrität während der Ermittlungen nicht gegeben ist, hat dies starke Auswirkungen auf die Zuverlässigkeit der Daten und der daraus resultierenden Informationen. Durch das vorhanden sein von Prüfsummen, kann ein Ermittler oder eine dritte Person auch zu späteren Zeitpunkten die Zuverlässigkeit prüfen oder nachweisen. Das BSI formuliert dies wie folgt: ”Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein.” Somit sind alle Schritte jederzeit zu dokumentieren. Die Dokumentation hat einen erheblichen Einfluss auf die Beweismittelkette.

Die Beweismittelkette, die Chain of Custody, beinhaltet die Chronologie des Wegs der Beweismittel und ist im Verlauf von Untersuchungen von großer Bedeutung. Dazu gehören alle Informationen, die im Zusammenhang mit den Beweismitteln bestehen: die Sammlung, Analyseschritte, beteiligte Personen, Programme/Werkzeuge und Gegenstände (z.B. Writeblocker), Datum, Uhrzeiten und Orte etc. Ziel der Chain of Custody ist es einen lückenlosen Verlauf zu dokumentieren.

Beginnend mit der Erhaltung der digitalen Szene ist bereits ein wichtiger Punkt abgedeckt. Es ist unerlässlich von Anfang an Veränderungen an Daten und der Gesamtheit der Daten (Digitale Szene) zu vermeiden. Im Zuge der Befragung können dann weitere Details erlangt werden, welche im späteren Verlauf der Analyse von Bedeutung sein können. Im Zuge der Dokumentation werden Fakten wie Art, Fundort oder Zustand von Beweisdaten bzw. Beweisträgern gesammelt, um auch im späteren Verlauf die Szene bestmöglich rekonstruieren zu können und Fehler auszuschließen oder zu erklären. Dabei wird dann auf angefertigten Kopien (Images) von beispielsweise Datenträgern gearbeitet und nach Spuren/Informationen durchsucht. Diese extrahierten Informationen lassen im Idealfall Rückschlüsse auf einen Ablauf zu. Ob dieser Ablauf tatrelevant ist, ist zu prüfen. Sollten die gefundenen Spuren Tatbezug aufweisen, so kann man diese zur Rekonstruktion eines Tathergangs verwenden. Dabei ist zu beachten, dass der wahrscheinlichste Tathergang nachvollzogen werden kann.

Die Beweismittelkette ist im Ermittlungsszenario von Bedeutung, um den Weg der Beweismittel nachvollziehen und beweisen zu können. Ein anschauliches Beispiel wäre hierfür eine Autofahrt von Stadt A nach Stadt B. Es gibt immer verschiedene Strecken. Je mehr Informationen wie beispielsweise die befahrenen Straßen, die passierten Orte etc. vorliegen, umso genauer kann die gefahrene Route rekonstruiert werden. Dieser Präzisionsgedanke lässt sich auf digitale Daten und Asservate im Zusammenhang mit der Beweismittelkette übertragen. Dafür gibt es Vorschriften und Leitfäden, wie beispielsweise den Leitfaden für IT-Forensik, welcher eine Richtlinie vom BSI ist.

Auch Gesetze können einen Rahmen darstellen. Im Bereich der TKÜ ist im § 100a StPO Abs. 6 für eingesetzte technische Mittel folgendes festgelegt. „Bei jedem Einsatz des technischen Mittels sind zu protokollieren:

- die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
- die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
- die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
- die Organisationseinheit, die die Maßnahme durchführt.''

Auch diese Informationen sind ein wesentlicher Teil der Beweismittelkette, da sie den Ursprung der durch z.B. TKÜ erlangten Daten dokumentieren und somit verifizieren.

Es ist wichtig, dass alle Stationen, durch die das Beweismittel gegangen ist, nachvollziehbar sind. In Behörden wird dies oft durch ein Übergabeprotokoll sichergestellt, während in Laboren ein Asservatenausgabebuch verwendet wird. Beim Versand von forensischen Datenträgern ist eine Verschlüsselung der Daten unerlässlich, um die Vertraulichkeit und Integrität der Beweise während des Transports zu gewährleisten. Eine mangelhafte Chain of Custody kann zu erheblichen Problemen führen und sogar zur Unverwertbarkeit der gesamten Ergebnisse der forensischen Untersuchung führen. Daher ist eine sorgfältige Dokumentation und Nachverfolgung der Beweiskette von größter Bedeutung.

Ein weiterer wichtiger Punkt für die lückenlose Dokumentation im Bezug auf den Weg eines Beweismittels ist der generelle Umgang und die Aufbewahrung von Asservaten. Kleine Asservate werden oft in Plastikbeuteln aufbewahrt, die nach dem Verschließen nicht mehr ohne sichtbare Spuren oder Beschädigungen geöffnet werden können. Diese Beutel ermöglichen es, die Beweismittel sicher zu lagern, während eine Beschriftung für die Identifizierung der Asservate möglich ist. Größere Asservate hingegen werden häufig in Plastikboxen aufbewahrt, die entsprechend beschriftet und versiegelt sind. Diese Boxen bieten zusätzlichen Schutz für die Beweismittel und gewährleisten, dass sie während der Lagerung oder des Transports nicht beschädigt werden. Die Beschriftung ermöglicht eine einfache Identifizierung der Asservate, während die Versiegelung sicherstellt, dass keine unbefugte Manipulation erfolgt. Durch die Verwendung geeigneter Aufbewahrungsmethoden können Forensiker sicherstellen, dass die Integrität der Beweismittel gewahrt bleibt und sie jederzeit für eine forensische Untersuchung verfügbar sind.

4 Forensische Methoden und Sicherung

4.1 Überblick über forensische Tools

Tools unterstützen bei der Auswertung von Daten. Die meisten forensischen Softwaretools können Images unkomprimiert im Raw-Format und im Expert Witness Format (EWF) abspeichern. EWF unterstützt komprimiertes und unkomprimiertes Speichern in eine große oder mehrere kleine Dateien. Zusätzliche Informationen wie Beweisnummer, Ausführender, Datum und Uhrzeit können in der Imagedatei abgelegt werden.

Allgemein kann man Computerforensische Tools in verschiedene Kategorien einteilen:

- Festplatten- und Datenerfassungstools
- Dateibetrachter
- Datei-Analyse-Tools
- Tools zur Analyse der Registry
- Internet-Analyse-Tools
- E-Mail-Analyse-Tools
- Analyse-Tools für mobile Geräte
- Mac OS-Analyse-Tools
- Tools für die Netzwerk-Forensik
- Tools für die Datenbank-Forensik

4.1.1 Forensische Datensicherung

Die Aufgabe der forensischen Datensicherung ist die unverfälschte Sicherung des Datenträgers. Diese ist entscheidend für die Auswertbarkeit und Beweiskraft der Ermittlungserkenntnisse. Um diese Kriterien zu garantieren, folgt die Sicherung dem folgenden Schema:

1. Hash-Wertbildung des Quelllaufwerkes
2. Imageerstellung
3. Hash-Wertbildung des Images
4. Vergleich der beiden Hash-Werte

Stimmen die Hash-Werte überein, ist das der Beweis, dass das erstellte Image exakt dem gesicherten Bereich entspricht. Die Auswertung kann nun mittels des Images erfolgen, sodass die Integrität des Beweismittels nicht verletzt wird.

Es existieren verschiedene Tools, die eine forensische Datensicherung durchführen oder unterstützen können:

4.1.1.1 dd

dd ist ein Tool für die Kommandozeile unter Linux, dass für forensische Datensicherungen genutzt werden kann. Es ist in jeder Unix-Distribution enthalten und erstellt Images im Raw-Format. So können bit-genaue Kopien von Festplatten, Partitionen oder Distributionen erstellt werden. Eine Komprimierung ist dabei nicht möglich. Als Beispiel: der nachfolgende Befehl kopiert eine Festplatte (hda) auf eine andere. Zusätzlich wird die Blockgröße angegeben, um eine effizientere Arbeit zu ermöglichen.

```
dd if=/dev/hda of=/dev/hdb bs=512
```

Mit dd können z.B. auch Festplatten mit einer zufälligen Zeichenfolge überschrieben werden.

4.1.1.2 dcfldd

dcfldd ist ein erweitertes dd und wird ebenfalls zur Erstellung eines Datenträgerabbilds verwendet. Es bietet zusätzlich die Fähigkeit zur automatisierten Erstellung von Prüfsummen, um die Beweisintegrität zu gewährleisten oder auch eine integrierte Fortschrittsanzeige.

4.1.1.3 dd_rescue

dd_rescue ist eine dd-Erweiterung zur Wiederherstellung beschädigter Laufwerke und ermöglicht clusterhaftes Auslesen von hinten nach vorne. Das Tool dd wurde also in Bezug auf Datenrettung und Forensik erweitert. Ein weiterer Vorteil ist, dass dd_rescue auch mit Datenströmen umgehen kann. Man kann Daten also per Datenstrom übertragen.

4.1.1.4 guymager

Guymager ist ein frei verfügbares, open-source Programm, welches für die Imageerstellung genutzt werden kann. Es bietet eine Anwenderoberfläche in verschiedenen Sprachen und läuft unter Linux. Der guymager kann Abbilder im dd-Format, aber auch im EWF- oder AFF-Format erzeugen. Die interne Struktur basiert auf separaten Threads für das Lesen, die Hash-Berechnung (MD5 und SHA256), Schreiben und beinhaltet eine parallelisierte Kompressions-Möglichkeit, die die volle Nutzung von Multiprozessor- und Hyper-Threading-Maschinen.

4.1.2 EnCase Forensics

EnCase ist ein kommerzielles Windows-Tool zur Erstellung und Auswerten von Datenträger-Images, aber auch zur Extraktion von Dateien. Es handelt sich um eine gerichtsfeste Lösung für das Auffinden, Entschlüsseln, Sammeln und Bewahren forensischer Daten von einer Vielzahl von Geräten, wobei die Integrität der Beweise sichergestellt und Ermittlungsabläufe nahtlos integriert werden.

4.1.3 X-Ways

X-Ways Forensics ist eine hochintegrierte Arbeitsumgebung für Computerspezialisten bei der forensischen (kriminaltechnischen) Untersuchung von EDV (Computerforensik) für Windows. Das Tool beinhaltet viele Funktionen. Hier sind beispielhaft einige aufgeführt:

- Klonen von Datenträgern, Erstellen von Disk-Images
- Einlesen der Partitionierungs- und Dateisystemstruktur innerhalb von Roh-Image-Dateien („dd“-Images), ISO-, VHD-, VHDX-, VDI- und VMDK-Images
- vollständiger Zugriff auf Datenträger, RAIDs und Images größer als 2 TB (mit mehr als 2^{32} Sektoren) mit Sektorgrößen bis 8 KB
- native Interpretation von RAID-Systemen (JBOD, Level 0, 5, 5EE und 6), Linux Software-RAIDs, dynamischen Platten und LVM2
- automatische Identifikation von gelöschten/verlorenen Partitionen
- verschiedene Datenrettungs-Techniken, extrem schnelles und mächtiges Carving
- sorgfältig gepflegte Datei-Header-Signatur-Datenbank basierend auf GREP-Notation
- Daten-Dolmetscher für 20 Variablentypen
- verbesserte Funktionen für Datenträgersicherungen, mit intelligenter Kompression
- Einlesen und Erzeugen von .e01-Evidence-Files (sog. EnCase-Images)

- komplette Fall-Verwaltung und -Bearbeitung
- relevante Dateien markieren und Berichtstabellen hinzufügen, Hinterlegen von Kommentaren zu Dateien, zur Ausgabe im Bericht oder zum Filtern
- Unterstützung mehrerer Ermittler im selben Fall, wobei X-Ways Forensics zwischen Benutzern anhand ihrer Windows-Benutzerkonten unterscheidet und die Benutzer zu unterschiedlichen Zeiten oder auch zur gleichen Zeit mit demselben Fall arbeiten. Die Ergebnisse (Suchtreffer, Kommentare, Berichtstabellenverknüpfungen, Markierungen, eingesehene, ausgeblendete Dateien, angehängte Dateien) werden separat verwaltet und auf Wunsch geteilt.
- automatische Erstellung von Berichten, die von jeder Applikation importiert und weiterverarbeitet werden können, die HTML versteht, wie z. B. MS Word
- automatisches Protokollieren Ihrer Arbeitsschritte (Audit-Logs)
- Schreibschutz zur Wahrung der Datenintegrität

Wie man anhand der Funktionen erahnen kann, legt X-Ways großen Fokus auch auf die Dokumentation, was für Ermittler einen großen Vorteil bietet.

4.1.4 Windows Forensic Toolchest

Das Windows Forensic Toolchest ist eine kommerzielle Sammlung von Werkzeugen zur Sammlung und Analyse von flüchtigen Daten. Diese Toolchest wurde entwickelt, um eine strukturierte und wiederholbare automatisierte Live Forensic Response, Incident Response oder Audit auf einem Windows-System durchzuführen und dabei sicherheitsrelevante Informationen aus dem System zu sammeln. WFT ist im Wesentlichen eine forensisch erweiterte Stapelverarbeitungsshell, die in der Lage ist, andere Sicherheitstools auszuführen und HTML-basierte Berichte auf forensisch fundierte Weise zu erstellen.

Ein sachkundiger Sicherheitsexperte kann WFT verwenden, um nach Anzeichen für einen Vorfall oder ein Eindringen zu suchen oder um einen Computermissbrauch oder eine Konfiguration zu bestätigen. WFT erzeugt Ausgaben, die nicht nur für den Administrator nützlich sind, sondern sich auch für Gerichtsverfahren eignen. Es bietet eine ausführliche Protokollierung aller Aktionen sowie die Berechnung von MD5/SHA1-Prüfsummen, um sicherzustellen, dass die Ergebnisse überprüfbar sind. Der Hauptvorteil der Verwendung von WFT für die Durchführung von Reaktionen auf Vorfälle oder Audits besteht darin, dass es eine vereinfachte Methode zur Skripterstellung für solche Aktivitäten bietet, die eine solide Methodik für die Datenerfassung verwendet.

4.1.5 Oxygen Forensic

Oxygen Forensic Detective ist eine allumfassende forensische Softwareplattform zur Extraktion, Dekodierung und Analyse von Daten aus verschiedenen digitalen Quellen: Mobil- und IoT-Geräte, Geräte-Backups, UICC- und Medienkarten, Drohnen und Cloud-Dienste. Oxygen Forensic Detective kann außerdem eine Vielzahl von Artefakten, Systemdateien und Anmeldedaten von Windows-, macOS- und Linux-Rechnern finden und extrahieren.

Zu den innovativen Technologien von Oxygen Forensic Detective gehören unter anderem das Umgehen von Bildschirmsperren, das Auffinden von Passwörtern zu verschlüsselten Backups, das Extrahieren und Parsen von Daten aus sicheren Anwendungen sowie das Aufdecken gelöschter Daten.

Darüber hinaus können mehrere Extraktionen in einer einzigen Schnittstelle untersucht werden, um ein vollständiges Bild der Daten zu erhalten. Durch die Verwendung der integrierten, branchenführenden Analysetools zum Auffinden sozialer Verbindungen, zur Erstellung von Zeitleisten und zur Kategorisierung von Bildern können Strafverfolgungsbehörden, Unternehmensermittler und andere autorisierte Mitarbeiter dazu beitragen, die Welt sicherer zu machen.

Oxygen Forensic Detective wird in einem USB-Dongle geliefert und ist für einen einzelnen Benutzer gültig.

Die Softwareplattform bietet viele verschiedenen Funktionen. Einige sind unterhalb aufgeführt:

- **Konten und Passwörter**: Der Bereich "Konten und Passwörter" zeigt Logins, Passwörter und Token an, die von mobilen Geräten extrahiert wurden. Das Programm entschlüsselt Anmeldeinformationen aus dem iOS-Schlüsselbund und Android KeyStore, findet sie in Anwendungsdatenbanken und Webformularen. Die Ermittler können Passwörter und Token für verschiedene Anwendungen finden
- **Extraktion von Android-Dateien**: Diese Methoden ermöglichen die Umgehung des Sperrbildschirms und erfordern keine Root-Rechte. Darüber hinaus bietet die Software die Möglichkeit, Root-Rechte zu erhalten und eine vollständige physische Extraktion von Android-Geräten mit installiertem Android OS 7, 8, 9 und 10 durchzuführen
- **Backup- und Image-Import**: Die Software importiert und analysiert Dutzende verschiedener Geräte-Backups und Images, die mit offizieller Gerätesoftware, Drittanbieterprogrammen oder anderen forensischen Tools erstellt wurden. Ermittler können iTunes-, Android-ADB-Backups, JTAG/ISP-, CHIP-Off-Images, .dar-Archive, XRY- und UFED-Extraktionen, Warrant Returns und viele andere Dateien importieren
- **Bericht**: Das Programm ermöglicht den Export von Daten aus jedem Bereich in viele gängige Dateiformate, darunter: PDF, XLSX, XML, HTML, JSON-Project VIC. Ein Bericht kann so erstellt werden, dass er ein einzelnes Gerät, mehrere Geräte, mehrere Abschnitte oder sogar ausgewählte Datensätze enthält. Die Berichte sind in hohem Maße anpassbar, so dass für jede Art von Fall nur die erforderlichen Daten angezeigt werden. Unsere XML-Berichte können mit unserer integrierten XML-Export-Spezifikationsdokumentation in viele gängige Analysesoftware-Plattformen integriert werden. Der Export in Relativity-Software ist ebenfalls möglich
- **Datensuche**: Die Software verfügt über eine leistungsstarke integrierte Schnittstelle für die Datensuche. Die Suche kann auf allen Geräten, auf der Fall- und auf der Geräteebene durchgeführt werden. Die Ermittler können die Daten anhand der in das Eingabefeld eingegebenen Informationen, anhand von Schlüsselwortlisten, Hashes, regulären Ausdrücken oder nach jeder anderen verfügbaren Methode durchsuchen. Die Suche wird als separater Prozess gestartet, so dass die Ermittler während des Suchvorgangs frei mit der Software arbeiten können. Der Suchprozess kann innerhalb von Dateien suchen, um Daten aufzudecken, die noch nicht geparst wurden, und so oft wertvolle Daten in SQLite-Datenbanken, Protokolldateien und Eigenschaftslisten aufdecken

4.2 Linux als Forensisches Werkzeug

Die IT-Forensik wird ein immer wichtigeres Mittel, um Hackerangriffe oder sonstige Arten von Datendiebstählen aufzudecken und zurückzuverfolgen. Für so eine Beweismittelsicherung dienen meist Linux Distributionen für forensische Zwecke. Davon gibt es inzwischen einige freie Lösungen, welche sich nicht nur der Beweissicherung verschrieben haben, sondern ebenfalls Tools zu Systemanalyse, Datenrettung oder Penetrationstests mitbringen. Alle Distributionen können von CD/DVD/VMware gebootet werden (Live-Linux). Jede Linux Distribution bietet seine Vor- und Nachteile. Es ist allerdings Vorsicht geboten: einige Werkzeuge bewegen sich am Rande der Legalität (Stichwort Hackerparagraf: Vorbereiten des Ausspähens und Abfangens von Daten → umgangssprachlich auch Hackerparagraf oder Hackertoolparagraf, ist ein Tatbestand, der in § 202c des deutschen Strafgesetzbuches (StGB) normiert ist).

Die bekannteste forensische Linux-Distribution ist KALI-Linux. Kali ist eine Penetrationstesting-Distribution und umfasst verschiedene Sicherheits- und Pentesting-Tools. Kali ist darauf optimiert, den Arbeitsaufwand zu reduzieren, so dass ein Profi sich einfach hinsetzen und loslegen kann. Es ist verfügbar für mobile Geräte, Docker, ARM, Amazon Web Services, Windows Subsystem für Linux, Virtual Machine, Bare Metal und andere. Einige Tools und Werkzeuge sind hier kurz aufgeführt:

- Wireshark: Netzwerksniffer
- Nmap: erkunden und analysieren eines Netzwerks durch z.B. Portscanns
- Maltego: Sammeln von Daten im Internet über Unternehmen oder Personen
- John the Ripper: Programm zum Testen und Knacken von Passwörtern
- Metasploit: Exploit-Framework (Durchführung verschiedenster Angriffsmethoden, um die Verwundbarkeit von Systemen per Exploits zu testen)

Neben den Werkzeugen in diesem Bereich, finden sich auch forensische Tools zur Analyse von Datenträgern oder zur Widerherstellung von gelöschten Daten wie z.B. Autopsy. Auch Arbeitsspeicherabbilder können mittels Kali-Werkzeugen erstellt werden.

4.3 Anti-Forensik

Wie bereits angesprochen lassen sich einzelne Programme unter Linux, aber auch separat, für Zwecke der Anti-Forensik nutzen. Anti-Forensik bezeichnet die negative Beeinflussung der Existenz oder Qualität von digitalen Beweisen und soll die Analyse von Beweismitteln bei forensischen Untersuchungen erschweren.

Methoden im Bereich der Anti-Forensik:

- Löschen/Verbergen von Daten (durch Rootkits, Kryptografie, Steganografie)
- Vernichten von (nebenläufigen) Informationen/ Artefakten (mittels sicherer Löschverfahren)
- Verwischen von Spuren (durch Spoofing, Desinformation anhand Dateimodifikation)

Literatur

[1] Wikipedia, *IT-Forensik.* [Online] Verfügbar unter: https://de.wikipedia.org/wiki/IT-Forensik (Zugriff am: 9. Mai 2022).

[2] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden IT-Forensik“, Bonn, 2011.

[3] A. Geschonneck, „Computer-Forensik“, *Systemeinbrüche erkennen, ermitteln, aufklären. dpunkt-Verlag*, 2006.

[4] A. Dewald und F. C. Freiling, *Forensische Informatik*. Norderstedt: Books on Demand, 2011.

[5] B. Carrier, *File system forensic analysis*. Boston, Mass, London: Addison-Wesley, 2005.

[6] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press, 2011.

[7] C. Paar und J. Pelzl, *Kryptografie verständlich*. Springer, 2016.

Anmerkung

Dieser Lehrbrief wurde für die Studierenden der Sachverständigenausbildung gemäß ADiF/AFOS im Rahmen des Moduls „Digitale Forensik – Grundlagen“ erstellt. Das Dokument darf nicht außerhalb dieses Rahmens verbreitet, verwendet oder veröffentlicht werden.

Dies liegt nicht zuletzt daran, dass die Quellenangaben nicht vollständig sind. Inhalte dieses Dokuments sind aus verschiedenen öffentlichen Quellen zusammengetragen.