

Einführung in Forensik und digitale Spuren

Martin Morgenstern

13.03.2023

Vorstellung Dozent

- Martin Morgenstern, Jahrgang 1985
- 3 Kinder
- Seit 2012 im polizeilichen IT-Umfeld tätig
- 2019 Master of Science in Digitaler Forensik an der Hochschule Albstadt Sigmaringen
- Für verschiedene Hochschulen als Lehrbeauftragter tätig in den Bereichen IT-Forensik, IT-Sicherheit und IT-Infrastruktur

Ziele

- Sie sollen ein Grundverständnis für die Arbeit eines IT-Forensikers erhalten
- Sie können digitale Spuren gerichtsfest sichern
- Sie sind in der Lage einfache Sachverhalte auszuwerten
- Sie können eigene Gutachten schreiben
- Auf Basis der in diesem Kurs erworbenen Kenntnisse können Sie ihr IT-forensisches Wissen vertiefen und zum Experten werden

Ihre Testumgebung

- Bitte installieren Sie VirtualBox
- Wir arbeiten mit der Forensik-Distribution CAINE
- Sie können CAINE unter folgenden Link herunterladen:
<https://cfitaly.net/caine/caine12.4.iso>
- Bitte installieren Sie auf Ihrem Hauptsystem Autopsy
<https://www.autopsy.com/download/>
- Bitte laden Sie die Dateien nps-2009-domexusers.redacted.E01 bis E03 herunter
<https://downloads.digitalcorpora.org/corpora/drives/nps-2009-domexusers>

Gliederung

- Definition und Ziele von IT-Forensik
- Vorgehensmodelle
- Gutachtenerstellung
- Traditionelle Sicherung und Auswertung digitaler Beweismittel
- Live-Analyse

Ihre Vorerfahrungen

- Hatten Sie schon etwas mit Computerkriminalität/Cybercrime zu tun?
- Welche IT-Forensikerfahrung haben Sie?

Prüfung

- Die Prüfung wird aus 2 Teilen bestehen
- Testat und Abgabe praktische Aufgabe
- Siehe Moodle
- Die Prüfungsaufgaben werden morgen vorgestellt:
 - Teamaufgaben zwischen 2 und 4 Leuten

Wozu dient dieser Kurs nicht

- In fremde Systeme eindringen (klassisches Hacking)
- Daten manipulieren (wir sind die Guten!)

Einführung in Forensik und digitale Spuren

Wissenschaftliche Beantwortung von Fragen des Rechts

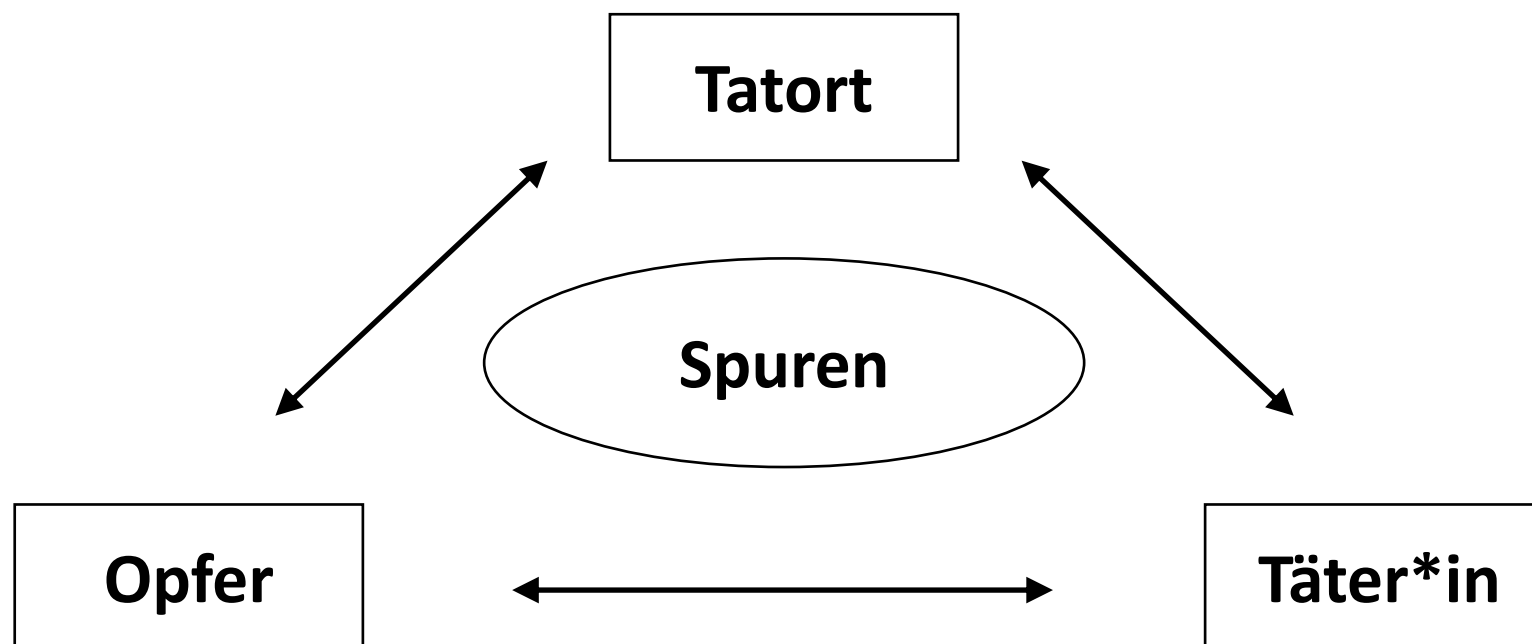
- Forum = Marktplatz (im antiken Rom)
- Auf dem Forum fanden Gerichtsverhandlungen statt
- Beantwortung der Rechtsfragen im öffentlichen Raum

Kontext: strafbare bzw. anderweitig rechtswidrige oder sozialschädliche Handlungen nachzuweisen und aufzuklären

Es ist keine Interaktion zwischen Gegenständen möglich, ohne Spuren zu erzeugen. Die eigentliche Frage ist lediglich, ob es im Rahmen der Ermittlungen möglich ist, die Spuren zu finden.

Edmond Locard (1930)

Lorcardsches Austauschprinzip



Spur

- **Materialübertragung**
- **Musterübertragung**



Dewald, Freiling (2011): Forensische Informatik

Vom Indiz zum Beweis

Indiz

- Als relevant erscheinende Spur
- Spur, die auf das Vorliegen eines Sachverhalts schließen lässt
- Beispiel: dieser Fußabdruck gehört mutmaßlich zum Schuh des Verdächtigen

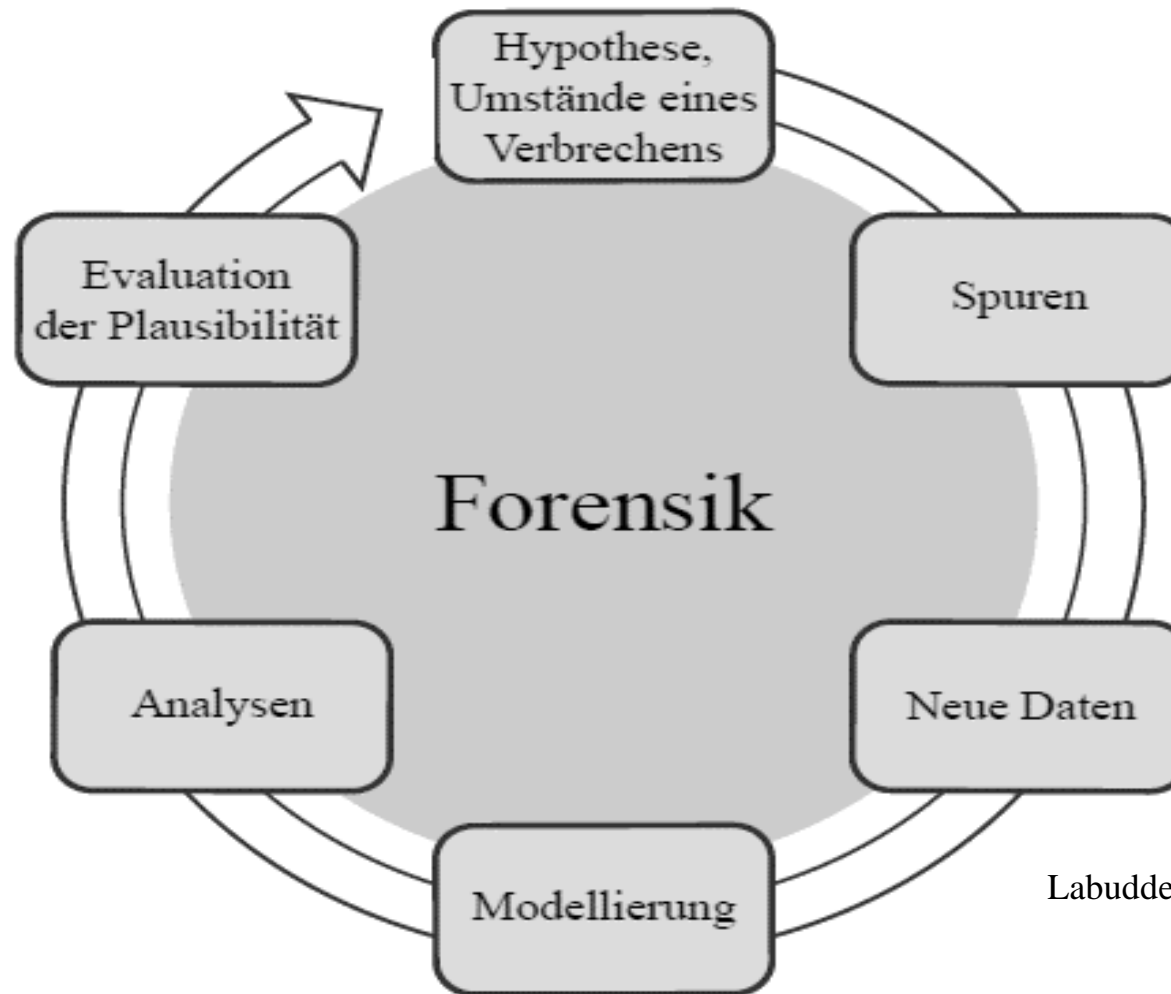
Vom Indiz zum Beweis

Beweis

Feststellung eines Sachverhalts als Tatsache in einem Gerichtsverfahren aufgrund richterlicher Überzeugung.

- Juristische Wahrheit
- Beispiel: dieser Fußabdruck gehört zum Schuh des Verdächtigen

Hypothesen Cycle



Labudde/Spranger 2017

Die W-Fragen der Forensik

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?
- Wer hat es getan?

Anforderungen an die Forensik

- Akzeptanz
- Glaubwürdigkeit
- Wiederholbarkeit
- Integrität
- Ursache und Wirkungen
- Dokumentation
- Lückenlosigkeit (chain of custody)

Checkliste

- Ist der Untersuchungsweg mit gleichen Ergebnissen wiederholbar?
- Sind die eingesetzten Werkzeuge und Methoden allgemein anerkannt?
- Ist die Wahl der eingesetzten Werkzeuge und Methoden nachvollziehbar?
- Waren die Untersuchenden mit diesen ausreichend vertraut, um potentielle Hinweise zu erkennen?

Teilgebiete der Forensik

- Forensische Medizin/Rechtsmedizin
- Forensische Toxikologie
- Forensische Ballistik
- IT-Forensik
- ...

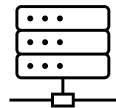
Teilgebiete der IT-Forensik

- Bisher werden Teilgebiete der IT-Forensik nach der Datenherkunft eingeteilt
- Beispiele
 - Datenträgerforensik
 - Netzwerkforensik
 - Cloudforensik
 - ...
- Nach Meinung von Experten sollte die Einteilung geändert werden

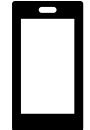
Teilgebiete der IT-Forensik



Cloud-Forensic




Network-Forensic



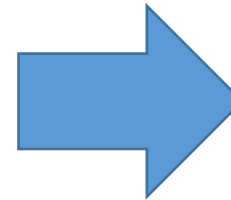
Smartphone-Forensic



App-Forensic

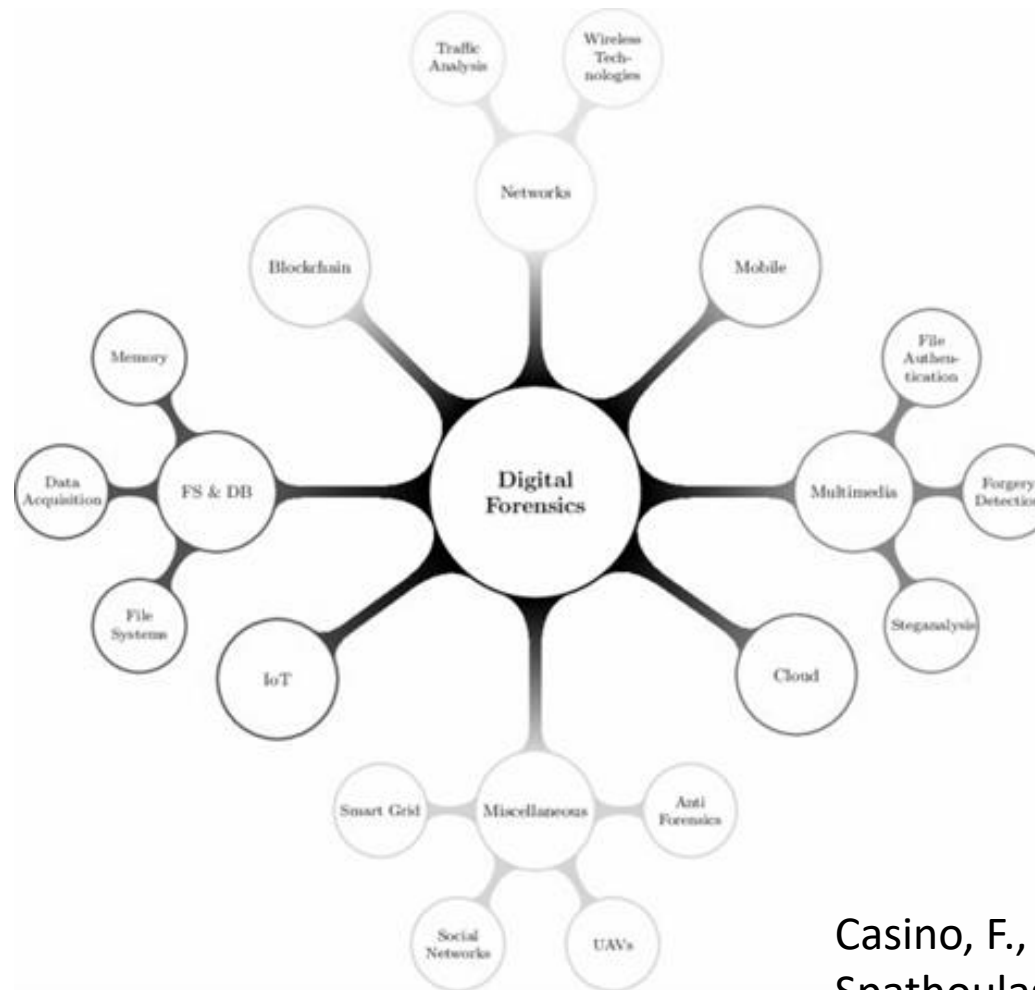


Unlimited kinds of forensic sources



Unstructured Data to Analyze

Teilgebiete der IT-Forensik



Casino, F., Dasaklis, T.,
Spathoulas, G. 2021

Was tut der Forensiker NICHT (1)

Forensiker...

- KEINE Entscheidung über Schuld oder Unterschuld
→ das tun Richter
- KEINE strafrechtliche Bewertung von Inhalten (z.B. Entscheidung ob Inhalte KiPo, verfassungsfeindlich...) → das tun die jeweiligen Spezialisten, wir bringen diesen unsere Verdachtsfälle

Was tut der Forensiker NICHT (2)

Forensiker...

- KEINE Bevorzugung vom Auftraggeber → bei persönlicher Befangenheit ist der Auftrag abzulehnen
- KEINE eigene Interpretation ohne Validierung (z.B. eine KiPo-Datei auf einem System kann durch Schadsoftware statt dem Nutzer selbst heruntergeladen sein)

IT-Forensik

- Streng methodisch vorgenommene,
- wissenschaftlich fundierte und
- gerichtssicher dokumentierte
- Datenanalyse
- auf Datenträgern und
- in Netzwerken

In der Privatwirtschaft kann von der Zielstellung abgewichen werden, wenn Strafverfolgung nicht das Ziel der Forensik ist

BSI-Leitfaden IT-Forensik 2011
Dewald, Freiling (2011): Forensische Informatik

Digitale Spur

Spuren, die auf Daten basieren, welche

- in IT-Systemen gespeichert sind oder
- zwischen IT-Systemen übertragen werden / wurden

BSI-Leitfaden IT-Forensik 2011
Dewald, Freiling (2011): Forensische
Informatik

Einteilung von digitalen Spuren

- Vermeidbare Spuren
 - Werden für die Funktion eines Systems bzw. einer Anwendung nicht benötigt
 - Leichter zu Fälschen
 - Bsp.: Log-Daten, Browser-History
 - Unvermeidbare Spuren
 - Sind für den Betrieb einer Anwendung / eines Systems notwendig
 - Höherer Manipulationsaufwand
 - Bsp.: Magic-Numbers, Partitionstabellen,...
- Unvermeidbare Spuren sind vertrauenswürdiger.

Rechtliche Grundlagen der IT-Forensik

Warum sollten Sie Forensiker rechtliche Grundlagen im groben kennen?

- Nicht alles was technisch möglich ist, ist erlaubt!
- Häufig haben Sie mit Daten zu tun, deren Besitz eigentlich verboten ist
- Durch Fehler können Sie sich selbst strafbar machen.
- Diese Vorlesung stellt keine Rechtsberatung dar. Wenn Sie IT-forensisch tätig werden liegt es in Ihrer eigenen Verantwortung die individuell relevanten rechtlichen Regelungen zu kennen!

Hoheitliche Aufgaben

- Wenn Sie hoheitliche Aufgaben erfüllen haben Sie besondere Berechtigungen
- Hoheitliche Aufgaben werden durch Behörden oder von Ihnen beauftragte Organisationen / Personen durchgeführt
- Strafverfolgung und damit deren Aufklärung ist eine hoheitliche Aufgabe
- Keine Hoheitliche Aufgabe wird übernommen, wenn interne Forensiker einer Firma auf eigene Faust tätig werden!
 - Hier gelten weiterhin alle Regeln, insbesondere auch die der DSGVO

Wie können Forensiker sich vor eigener Strafbarkeit schützen?

- Niemals ohne schriftlichen Auftrag hoheitlich tätig werden
- Zum Üben / Testen nur eigene Systeme und Daten verwenden oder frei verfügbare Trainingsdaten nutzen
- Keine Untersuchung von Mitarbeitergeräten ohne Zustimmung des Personalrats / Betriebsrats und dem Datenschutzverantwortlichen
- Bei Zweifeln an der Rechtmäßigkeit einer Untersuchung diese pausieren und fachkundigen Rat (z. B: Justiziar, Anwalt, ...) einholen.
- Gerade in kleineren privatgeführten Firmen kommen unrechtmäßige Aufträge vor. Der Klassiker ist es den Browserverlauf eines Mitarbeiters ohne dessen Wissen auswerten zu lassen.

Gutachtenerstellung

Möglichkeiten zur Dokumentation

- Fotodokumentation
 - Videomitschnitt
 - Screencasting/Screenshots
 - Dokumentation in den All-in-One-Auswertetools
 - (Standardisierte) Protokolle
(auf Papier oder in Dateien)
 - (Standardisierter) Auswertebericht
-
- → In der Praxis wird eine Kombination verschiedener Möglichkeiten genutzt

Dokumentation der Vorgehensweise

- Name und Versionsnummer des verwendeten Programms
- Kommandozeilenparameter des Aufrufs
- Forensische Absicherung dieses Werkzeugs, notfalls durch externe Schutzmechanismen wie Prüfsummen, Verschlüsselung, Signierung, Hardware-Schreibblocker oder andere Maßnahmen, die geeignet sind, Authentizität, Integrität oder Vertraulichkeit sicherzustellen
- Erfahrung des Untersuchenden mit diesem Werkzeug
- Motivation zur Auswahl dieses Werkzeugs

Bericht

- Der Bericht muss den Sachverhalt ohne wesentliche Lücken darstellen.
- Schlussfolgerungen sind deutlich als solche gekennzeichnet und begründet.
- Technische (forensische) Fachleute müssen in die Lage versetzt werden, die Vorgehensweise, die Feststellungen und Schlussfolgerungen zu prüfen und zu bewerten.

Rittelmeier 2015

Bericht

- Anhand der technischen Beschreibungen muss ein fachkundiger Leser in der Lage sein, die Untersuchungen zu wiederholen und dabei (idealerweise) zu denselben Ergebnissen kommen.
- Die Managementebene und technisch eher unkundige Leser mit juristischem Hintergrund (Anwalt, Staatsanwalt, Richter,...) müssen verstehen, was passiert ist und in der Lage sein, die Informationen im Bericht auf juristische Normen zu übertragen.

Rittelmeier 2015

Berichtsgliederung

- Deckblatt
- Auftraggeber, Auftragnehmer, Verteilung der tatsächlichen Arbeit, Versionshistorie
- Konkreter Auftrag
falls gegeben: Erweiterungen/Änderungen des ursprünglichen Auftrags
- Zusammenfassung der Ergebnisse auf einer, maximal zwei Seiten
- Ausführlicher Untersuchungsbericht
- Anlagen, technische Unterlagen, Skripte, Listen, ...

Rittelmeier 2015

Berichtsgliederung

De Wold/Freiling 2011

- Titel
- Prolog
- Zusammenfassung für Nicht-Techniker
- Zusammenfassung für Techniker
- Details für Techniker

Untersuchungsverlauf

FALL-ID: 00001

Zeit	Aktion	Kommentar
0:04	Snapshot erstellen... & md5-x64 ct103.vmem	Erstellung des Hauptspeicherabbilds mit „Snapshot erstellen...“, Berechnung der Prüfsumme mit MD5 1.1.18 (MD5-Hash: 5582970b95a6fdac27ca070e83db970e)
0:09	vol.py -f ct103.vmem pstree	Anzeige aller aktiven Prozesse in der Baumansicht (Volatility 2.1_alpha), unbekanntes Prozess 580846.exe entdeckt (pid 1464), Ergebnis gespeichert in ct103_pstree.txt (MD5-Hash: b14496eaa5ace4cfe75668c72f957a4b)
0:11	vol.py -f ct103.vmem psscan	Auflistung aller aktiven, versteckten & beendeten Prozesse, bereits beendetes Prozess darkness_8.exe (Dropper?) entdeckt (pid 3560, exit time 2011-12-16 13:30:49), Ergebnis gespeichert in ct103_psscan.txt (MD5-Hash: f68641ef061d859dc2e45992c1238f05)
0:13	vol.py -f ct103.vmem procexedump -p 1464 -D dump/	Prozessdump zur Überprüfung mittels Virenscaan, Ergebnis gespeichert in executable.1464.ex_ (MD5-Hash: 4b47b5fe0e63c8192b8b6aafa80c34cb)
0:14	virustotal.com	Virusscan via virustotal.com, Datei identifiziert als Backdoor:Win32/Votwup.B, Ergebnis gespeichert in ct103_virustotal_1464.pdf (MD5-Hash: 020b455ac9692adfa780949d6fea53ce)

Weiterführende Informationen

FALL-ID: 00001

Darkness DDoS Malware (auch bekannt als Votwup) ist für seine hohe Effizienz bekannt: mit einer Handvoll infizierten Rechner können sogar größere Webseiten bzw. Server-Cluster mit fehlerhaften HTTP-Anfragen lahmlegen. Kompromittierte Systeme werden über mehrere C&C-Server im russischen Netzbereich kontrollieren und auf dem neuesten Stand gehalten².

Nach Angaben der Programmierer können 5000 Bots Server-Cluster, 15000-2000 beliebigen Server, unabhängig von verwendeten Schutzmaßnahmen in die Knie zwingen. Aktuelle Version der Malware ist 9H³.

Berichtsqualität

Was fällt Ihnen bei den folgenden
Berichtsausschnitten auf?

Beispielformulierung: Chain of Custody

Nachdem mir das Image, in Form einer CD, von Frau B. am 16.03.2010 übergeben wurde, habe ich es in meinem Rucksack sicher in meine Wohnung transportiert. In meiner Wohnung legte ich das Image in einen nur mir zugänglichen und verschlossenen Schrank. Am 08.03.2010 nahm ich das Image wieder aus dem Schrank, legte es in meinen Rucksack und transportierte es ins forensische Labor. Dort legte ich die CD in die forensische Workstation in Raum 123. Der Raum ist stets verschlossen und nur Arbeitern und anderen Forensikern zugänglich. Nach vollendeten forensischen Arbeiten transportierte ich die CD in meinem Rucksack wieder in meine Wohnung, wo sie in den verschließbaren, nur mir zugänglichen Schrank eingeschlossen wurde.

Dewald/Freiling 2011

Beispielformulierung: Bilder

Auf der Festplatte konnten acht Dateien mittels foremost wiederhergestellt werden. Es handelt sich um jpg- und pdf-Dateien. Die Bilddateien zeigen zweimal Dagobert Duck sowie zwei zubereitete Speisen und ein Bild eines winkenden Mannes (siehe 4.1 Bilder). Gravierender ist die Datei 12345.jpg, welche eine schematische Darstellung einer Bombe beinhaltet. [...] Zusammenfassend lässt sich sagen, dass die gefundenen Texte von Täterwissen zeugen, welches kein anderer in dieser Detaillierung haben könnte. In Kombination mit der Liste an Bauteilen für eine Zündungsvorrichtung und der schematischen Darstellung einer Bombe sowie der minutengenauen Angabe der Explosion lässt sich ein klarer Zusammenhang der Person XY mit den vorliegenden Erpressungen bestätigen.

Dewald/Freiling 2011

.

Vorgehensmodelle

Definition Vorgehensmodelle

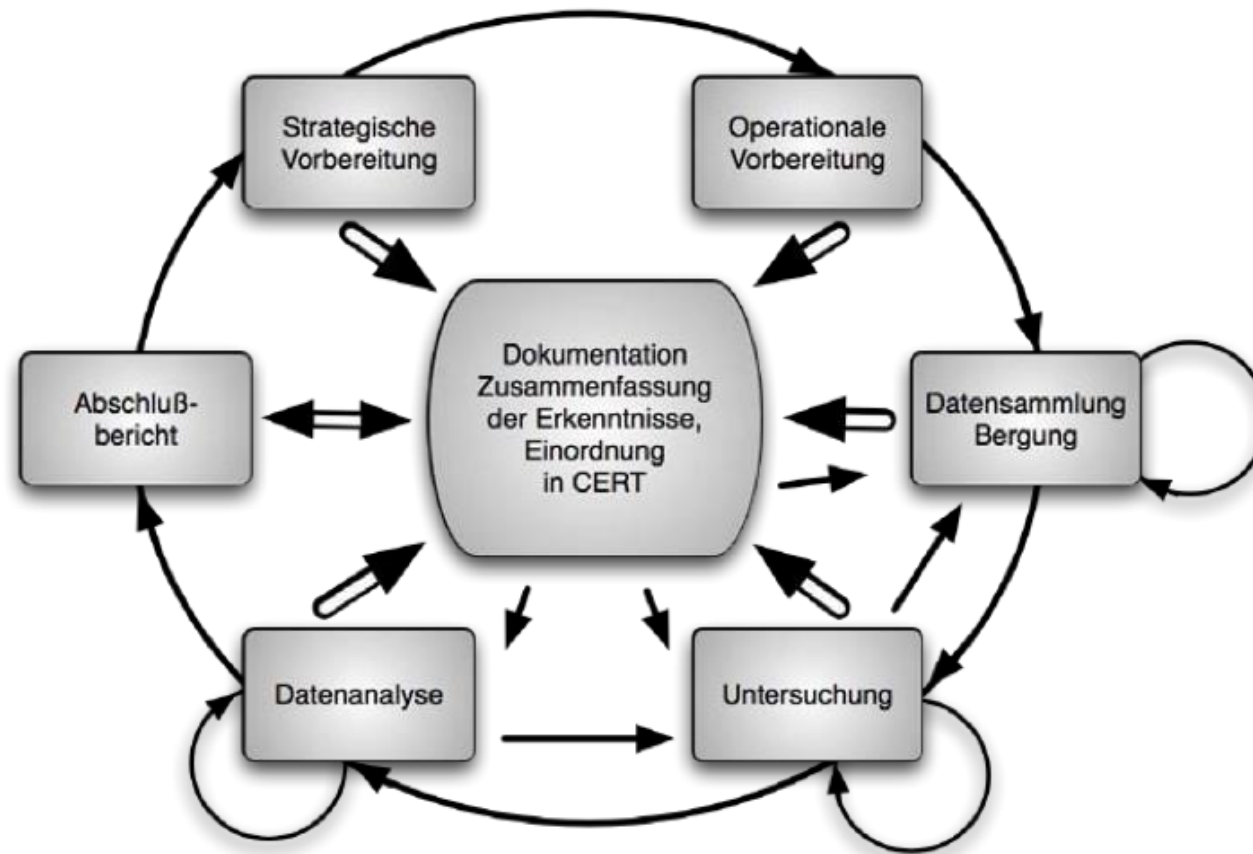
Modelle

- Beschreiben stark Vereinfacht den Untersuchungsablauf
- Es existieren ein Vielzahl an Modellen
- Bei der Wahl des Modells gibt es kein richtig oder falsch
- bedeutendste Modelle sind:
 - SAP-Modell
 - BSI-Modell
 - NIST-Modell

S-A-P Modell

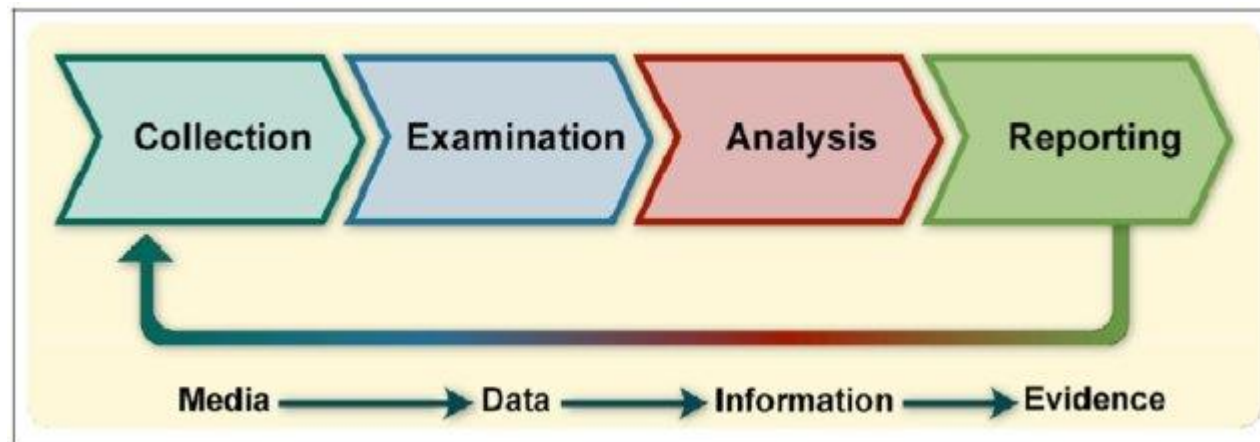
- **Secure Analyse Present**
- **Secure**
 - Alle vorhandenen Daten werden gesichert
 - Es erfolgt keine Vorprüfung der Relevanz
- **Analyse**
 - Sichtung der gesicherten Daten
 - Feststellung von Spuren
- **Present**
 - Zielgruppengerichte Aufarbeitung der Ergebnisse
 - Vervollständigung der Dokumentation

BSI-Modell



<https://it-forensik.fiw.hs-wismar.de/index.php/Datei:BSI-Vorgehensmodell.png> aufgerufen am 02.12.2022

NIST-Modell



Traditionelle Sicherung und Auswertung digitaler Beweismittel

Grundlagen Dateien

- „Menge von Daten, die nach einem Ordnungskriterium, das sie als zusammengehörend kennzeichnet, in maschinell lesbaren externen Speichern gespeichert sind.“ Lakes 2018
- Es existiert eine Vielfalt verschiedener Dateien
- Dateien können nach verschiedenen Kriterien kategorisiert werden (z. B. Ausführbarkeit oder Nutzungstyp)
- Verschiedene Möglichkeiten zur Kennzeichnung des Datentyps
 - Datei-Endung (leicht zu manipulieren)
 - Anfang des Dateiinhalts (siehe folgende Folien)
 - Auf Basis des Speicherorts
 - ...

Magic Numbers (Magische Nummern)

- Zur Identifizierung von Datentypen nutzen Betriebssysteme und Programme häufig die ersten Zeichen einer Datei (Magic Numbers)
- Forensiker können so leicht falsche bzw. fehlende Dateiendungen identifizieren
- Auf Basis der Suche nach Magic Numbers kann nach gelöschten Dateien bzw. Fragmenten von denen gecarvt werden → Carven suche nach Magic Numbers in einer großen Datenmenge

Übung: Carven

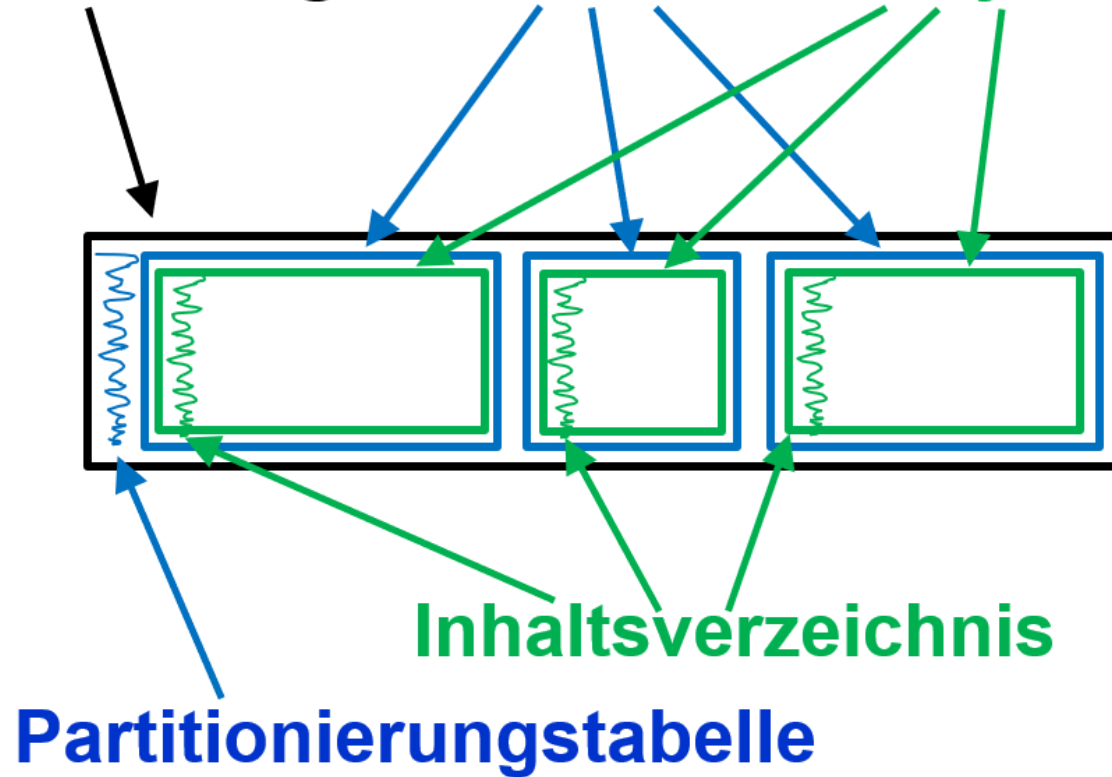
- Wir werden zuerst manuell Carven (mit einem Hex-Editor)
- anschließend lernen wir erste Tools für automatisiertes Carven kennen und nutzen

Grundlagen Dateisysteme

- Als Forensiker sollen Sie verstehen, wie Daten auf Dateisystem-Ebene wiederhergestellt werden können
- In dem Kurs lernen Sie die grundlegenden Funktionen eines Dateisystems, sowie Grundlagen zu verbreiteten Dateisystemen kennen

Zusammenhang Datenträger Partition Dateisystem

Datenträger **Partition** **Dateisystem**



Honekamp 2021

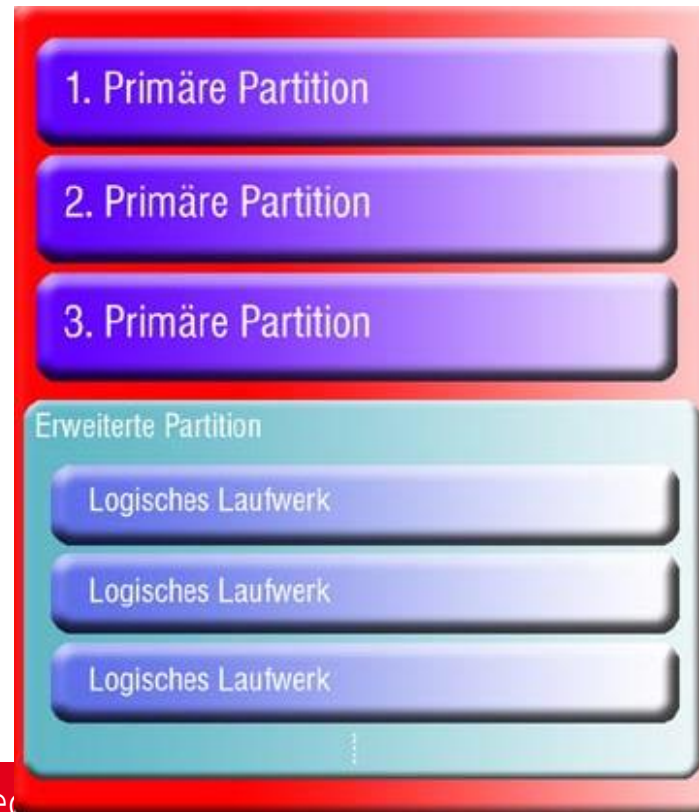
Master-Boot-Record (MBR)

- Enthält Startprogramm und Partitionstabelle
- Befindet sich am Anfang eines Datenträgers
- Ermöglicht das Booten eines Datenträgers
- Heute zunehmend durch GPT ersetzt

Master-Boot-Record (MBR)

Adresse		Funktion / Inhalt		Größe (Bytes)
hex	dez			
0x0000	0	Startprogramm (englisch <i>Bootloader</i>) (Programmcode)		440
0x01B8	440	Datenträgersignatur (seit Windows 2000)		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}		
Gesamt:				512

- maximal 4 (primäre) Partitionen
- eine Partition maximal 2 TB
- erweiterte Partitionen mit logischen Laufwerken



GUID Partition Table (GPT)

- Zählt als Nachfolger von MBR
- Enthält im ersten Sektor aus kompatibilitätsgründen eine klassische MBR-Partitionstabelle
- GPT wird seit ca. 2000 eingesetzt und hat diverse technische Vorteile, z.B. sind mehr Partitionen möglich
- Jede Partition hat eine weltweit eindeutige ID
- Partitionsgrößen bis 18 Exabyte möglich

GPT-Header

Offset	Länge	Inhalt
0	8 bytes	Signatur („EFI PART“, 45h 46h 49h 20h 50h 41h 52h 54h)
8	4 bytes	Revision (00h 00h 01h 00h)
12	4 bytes	Header-Größe – Little Endian (5Ch 00h 00h 00h entspricht 92 bytes)
16	4 bytes	Header-CRC32-Prüfsumme (von Offset 0 bis Header-Größe, dieses Feld selbst wird bei der Berechnung auf 0 gesetzt)
20	4 bytes	Reservierter Bereich – muss Null (0) sein
24	8 bytes	Position des eigenen LBA (dieses Headers)
32	8 bytes	Position des Backup-LBA (des anderen Headers)
40	8 bytes	Erster benutzbarer LBA für Partitionen (Letzter LBA der primären Partitionstabelle + 1, normalerweise 34)
48	8 bytes	Letzter benutzbarer LBA (Erster LBA der sekundären Partitionstabelle – 1, normalerweise Datenträgergröße – 34)
56	16 bytes	Datenträger- GUID (als Referenz siehe auch UUID bei UNIXe)
72	8 bytes	Start-LBA der Partitionstabelle
80	4 bytes	Anzahl der Partitionseinträge (Partitionen)
84	4 bytes	Größe eines Partitionseintrags (normalerweise 128)
88	4 bytes	Partitionstabellen-CRC32-Prüfsumme
92	*	Reservierter Bereich; muss mit Nullen, für den Rest des Blocks, belegt sein (420 Bytes bei einem 512-byte LBA)

https://de.wikipedia.org/wiki/GUID_Partition_Table

GPT-Partitionseintrag

Offset	Länge	Inhalt
0	16 Bytes	Partitionstyp-GUID
16	16 Bytes	Eindeutige Partitions-GUID
32	8 Bytes	Beginn der Partition (erster LBA – Little-Endian)
40	8 Bytes	Ende der Partition (letzter LBA – inklusive)
48	8 Bytes	Attribute (siehe folgende Tabelle)
56	72 Bytes	Partitionsname (36 UTF-16LE-Zeichen)
insg.	128 Bytes	

https://de.wikipedia.org/wiki/GUID_Partition_Table

NTFS

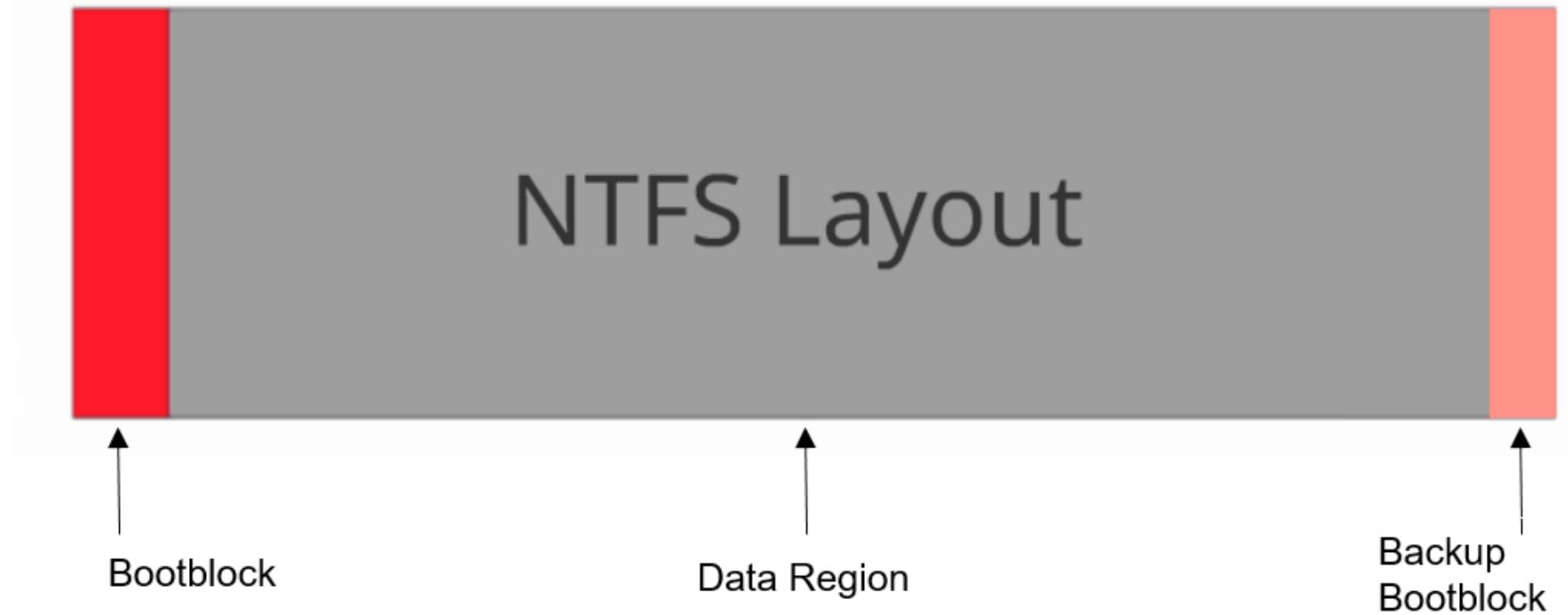
- Max. Clustergröße: 64 KiB, Default 4 KiB
- Max. Partitionsgröße: Win-OS: 256 TeBiB Theoretische max. Größe: 1Yobibyte
- Max. Dateigröße: Win-OS: 16 TiB Theoretische max. Größe: 16 Exbibyte
- Namenslänge: 255
- Alles ist eine Datei, selbst der Bootblock

NTFS-Versionen

- NTFS 1.0 – Microsoft Windows NT 3.1
- NTFS 1.1 – Microsoft Windows NT 3.5/3.51
- NTFS 2 – Microsoft Windows NT 4.0
- NTFS 3.0 – Microsoft Windows NT 4.0 ab SP 4 und Windows 2000 (NT 5.0)
- NTFS 3.1 – ab Microsoft Windows XP (NT 5.1)
- Die Datei NTFS.SYS zählt die Versionen einfach hoch. Derzeit Version 5.0.

- NTFS ist ein proprietäres Dateisystem von Microsoft, d.h. es existiert keine öffentliche Dokumentation, die den genauen Aufbau des Dateisystems beschreibt.
- Aus diesem Grund tun sich andere sehr schwer, Treiber für schreibenden Zugriff auf NTFS bereitzustellen.

NTFS



NTFS Bootblock

Offset	Länge	Beschreibung
0x000	3	EB 52 90 (Sprung zum Start des Bootprogramms + NOP)
0x003	8	System-ID: "NTFS"
0x00B	2	Anzahl Bytes pro Sektor
0x00D	1	Anzahl Sektoren pro Cluster
0x00E	7	reserviert (00 00 00 00 00 00 00)
0x015	1	Media Descriptor Byte (0xF8 für Hard Disk)
0x016	2	reserviert (00 00)
0x018	2	Anzahl Sektoren pro Spur
0x01A	2	Anzahl der Schreib-/Leseköpfe (Oberflächen)
0x01C	8	reserviert (00 00 00 00 00 00 00 00)
0x024	4	80 00 80 00 (immer?)
0x028	8	Gesamtzahl Sektoren im logischen Laufwerk
0x030	8	Logische Cluster-Nr. des ersten Clusters der MFT (Datenattribut von \$MFT)
0x038	8	Logische Cluster-Nr des ersten Clusters der Backup-MFT (\$MFTMirr)
0x040	4	Anzahl Cluster pro MFT-Record (0xF6 bedeutet 1/4) <small>neg: 2ⁿ Bytes</small>
0x044	4	Anzahl Cluster pro Index-Record
0x048	8	Seriennummer des logischen Laufwerks
0x050	4	reserviert (00 00 00 00)
0x054	426	Boot-Code (boot loader routine)
0x1FE	2	Kennung für Bootsektoren (55 AA)

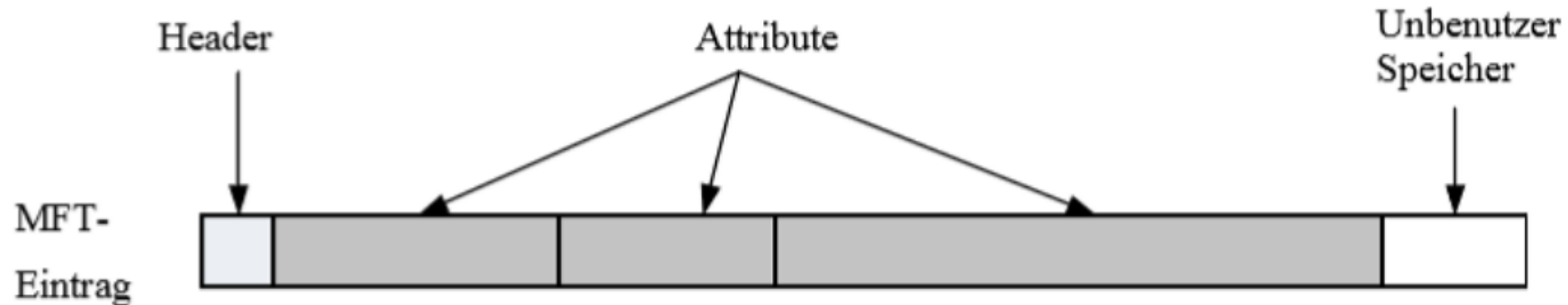
NTFS

Record-Nr

0
1
2
3
4
5
6
7
8
9
...
16
...
24

MFT (\$MFT)
Teilkopie der MFT (\$MFTMirr)
Log File (\$LogFile)
Volume File (\$Volume)
Attribute Definition File (\$AttrDef)
Root Directory (.)
Bitmap File (\$Bitmap)
Boot File (\$Boot)
BadCluster File (\$BadClus)
weitere NTFS Metadata Files
reserviert für <i>extension file records</i> der MFT
Anwender-Dateien und Directories
...
...
...

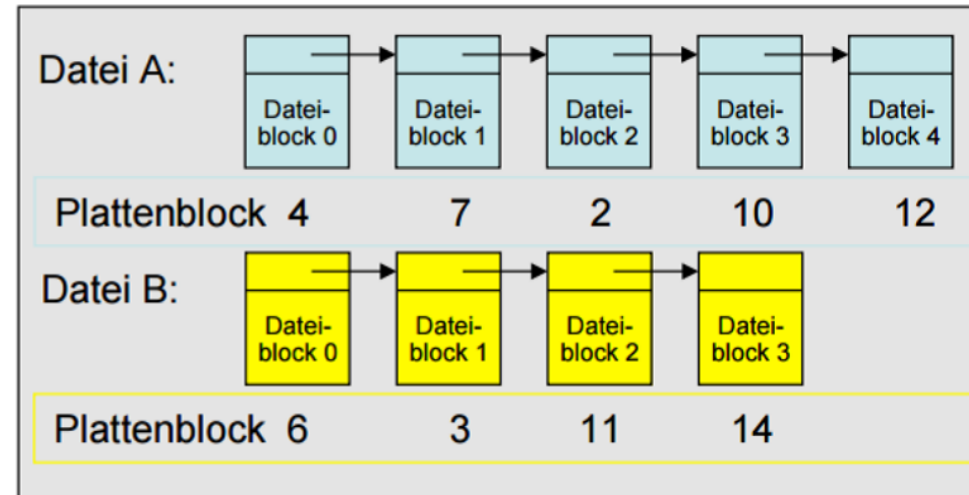
NTFS MFT



- Jede Datei und jedes Verzeichnis hat mindestens einen Eintrag in der MFT, Default 1024 Bytes
- Die ersten 42 Bytes eines MFT-Eintrages bestehen aus 12 definierten Feldern, die restlichen 982 Bytes besitzen keine Struktur und können mit sog. Attributen aufgefüllt werden
- Attribute: Dateiname, Dateigröße, MAC, Freigabe, Dateityp, Dateiinhalt
- Bei sehr kleinen Dateien wird auch der Dateiinhalt in der MFT abgelegt (residente Attribute)

File Allocation Table (FAT)

Plattenblock 0	
Plattenblock 1	
Plattenblock 2	10
Plattenblock 3	11
Plattenblock 4	7
Plattenblock 5	
Plattenblock 6	3
Plattenblock 7	2
Plattenblock 8	
Plattenblock 9	
Plattenblock 10	12
Plattenblock 11	14
Plattenblock 12	-1
Plattenblock 13	
Plattenblock 14	-1
Plattenblock 15	



Beginn Datei A

Beginn Datei B

FAT32

FAT32 für Festplatten über 2 GB

Max. Anzahl Cluster 2^{28} (4 Bit sind reserviert) =
268.435.456

Max. Clustergröße: 32 KB

Max. Partitionsgröße mit Win-OS: 32 GB, durch
Tools von Drittherstellern: 127 GB, theoretische
max. Größe: 8 TB

Max. 65.536 Einträge pro Verzeichnis

Max. 4.177.920 Einträge pro Volume

Max. Dateigröße: 4 GB

Namenslänge von Einträgen: 255

HOST Nicht kompatibel zu FAT16-Anwendungen

extFAT

exFAT erlaubt Dateien mit mehr als 4 GiB
Dateigröße (max. 64 ZiB, empfohlene maximale
Dateigröße 512 TB (maximale Partitionsgröße)

Die maximale Cluster-Größe beträgt 32 MiB, daher
auch für sehr große Datenträger geeignet
exFAT verwendet nur eine FAT-Tabelle. Das spart
Platz und Verwaltungsaufwand, reduziert aber die
Datensicherheit

exFAT verwendet Dateinamen in Unicode und bis
zu 255 Zeichen. Kurze 8.3-Namen gibt es nicht
mehr.

Definition forensisches Image

- Unterscheidet sich erheblich von einer reinen logischen Daten-Kopie
- Kopie aller Sektoren, also auch der scheinbar nicht genutzten, wird erstellt
- Attribute werden mitgesichert
- Gelöschte Daten werden mitgesichert

Formate für forensische Images

- RAW-Format
 - Keine Komprimierung
 - Kann mir Boardmitteln unter Linux schnell erstellt werden (z. B. dd-Befehl)
 - Endung oft .dd oder .raw
- Encase Image Format / Expert Witness Format
 - Datenkomprimierung ist Standard
 - Format ist Quasi-Standard in der Forensik
 - Splittung in mehrere Dateien üblich, Größe individuell anpassbar
 - Dateiendungen e01, e02,....en

Erstellung forensischer Datenträgerimages (klassisch)

- Sofortige Unterbrechung der Stromzufuhr bzw. sofortiges Ausschalten des Rechners
- Entfernen der Datenträger
- Erstellung des von Datenträger Images mit Nutzung eines Write-Blockers, alternativ auch Datenträger im Lesemodus mounten
- Alternativ zum Datenträgerausbau kann Zielsystem mit einer Forensik-Distribution gebootet werden. → Datenträgerimage kann dann z. B. auf USB- oder NAS erstellt werden.

Hindernisse für klassische Image-Erstellung

- Verschlüsselung
- Nicht entfernbare Datenträger (z. B. in Smartphones)
- Weitere Details in der Lerneinheit „Live-Forensik“

Auswertung forensischer Images

- Auswertung mit Forensik-Programmen; diese gibt es für Windows und Linux
- In diesem Kurs wird Autopsy verwendet
 - Autopsy kostenlos nutzbar
 - Für alle gängigen Betriebssysteme verfügbar
 - Relativ großer Funktionsumfang
- Bekannte weitere Tools sind u. a.: X-Ways, Encase, Oxygen Forensic...

Autopsy

