

HOCHSCHULE ...

STUDIENGANG ...

Masterthesis

**Aufbau einer Plattform zur
forensischen Analyse basierend auf dem
Apache Hadoop[®] Framework**

Zur Erlangung des akademischen Grades
Master of Science

vorgelegt im Sommersemester 2018

von
Johannes Busam

Erstbetreuung: ...

Zweitbetreuung: ...

Kurzfassung

Die digitale Forensik ist heutzutage ein wichtiger Teil bei der Aufklärung von Straftaten durch Ermittlungsbehörden. Nahezu in jedem Fall können digitale Beweismittel sichergestellt werden, weil informationstechnische Systeme im Alltag allgegenwärtig sind. Durch den rasanten Fortschritt von IT-Technologien, müssen auch die forensischen Methoden immer wieder neu adaptiert und verbessert werden. Allein die Datenmenge, welche aufgrund sichergestellter Mobiltelefone, Computer, Netzwerkspeicher und Server verarbeitet werden muss, kann durchaus mehrere Terabyte groß sein.

Um solche Datenmengen schnell und effizient bearbeiten zu können, wird in dieser Thesis eine forensische Analyseplattform entwickelt. Sie soll anfallende Daten verteilt in einem Computer-Cluster speichern und aufbereiten können. Zuerst soll geprüft werden, wie diese Daten verteilt gespeichert werden können. Im nächsten Schritt sollen neue Informationen aus dem gespeicherten Datenbestand extrahiert werden. Hierbei sollen auch forensische Aspekte, wie beispielsweise die Erstellung einer Beweismittelkette und die Sicherheit des Computer-Clusters, betrachtet werden.

Zur Datenspeicherung wird das Apache Hadoop®-Ökosystem genutzt. Es werden diverse Datenträgerabbilder erstellt, die als Grundlage zur Datenverarbeitung der Analyseplattform dienen sollen. Diese Abbilder können nicht ohne vorherige Datenaufbereitung in die Analyseplattform importiert werden, da sonst keine parallele Verarbeitung möglich wäre. Daher werden unterschiedliche Ansätze analysiert, wie diese Daten optimal im Hadoop-Cluster gespeichert werden können. In einer Variante werden die Daten auf logischer Dateiebene, Datei für Datei, in die Analyseplattform importiert. Dieser Ansatz ermöglicht eine parallele Datenverarbeitung. Allerdings können die Dateimetadaten nicht optimal gespeichert werden, was sich bei großen Datenmengen negativ auf die Geschwindigkeit der Datenverarbeitung auswirkt. Die finale Variante zur Datenspeicherung ist eine Mischung aus zwei Datenspeicherarten. So werden die Dateimetadaten und kleine Dateien in einer spaltenorientierten Datenbank gespeichert. Wohingegen große Dateien im verteilten Dateisystem der Hadoop-Plattform abgelegt werden. Damit ist es auch möglich, die bestehenden Daten aus der Datenbank mit neuen Informationen aus der Datenverarbeitung anzureichern.

Bei der Datenverarbeitung wird Apache Spark™ genutzt, welches die Daten auf der Hadoop-Plattform parallel prozessieren kann. Es werden beispielsweise Hashsummen berechnet und Medientypen ermittelt.

Ein weiterer Aspekt ist die Implementierung einer Volltextsuche für einen performanten Datenzugriff. Hierzu werden die Daten im Computer-Cluster verteilt indexiert, um sie schneller durchsuchen zu können. Derzeit können nur die Dateimetadaten indexiert werden. Eine Indexierung aller Dateinhalte kann in einer Weiterentwicklung des Systems implementiert werden.

Letztlich ist es möglich, beliebige Datenträger mit der hier entwickelten forensischen Analyseplattform zu verarbeiten. Auch ein performanter Zugriff auf die Daten ist realisierbar. Allerdings hat diese Plattform auch Schwächen, welche zukünftig behoben werden sollten. So benötigt schon das Importieren großer Datenträger sehr viel Zeit. Hier wäre es sinnvoll, die Datenverarbeitung so umzustellen, dass einzelne Daten sofort prozessiert und angezeigt werden, um damit schon auf Teilergebnisse zugreifen zu können.

Abstract

Digital forensics is an important part to resolve crime. Digital evidence may be found at almost every crime scene because information technology is pervasive. Apart from that, the forensic approach must be adapted and improved continuously. Merely the amount of data, collected from mobile phones, computers and network storages, can be very large (up to multiple tera bytes).

A new forensic analysis platform shall be developed in this thesis to handle such a huge amount of data as quickly as possible. Therefore the data shall be stored on multiple nodes within a computer cluster to speed up the data processing by parallelism. The first part of this work handles the persistence of the data within the computer cluster. The next step is to find suitable approaches for processing the data and extracting new information out of them. Also these new information must be stored in a technically correct manner. Cross-cutting concerns, like the creation of a chain of custody and the computer cluster security, shall be handled also in this work.

The forensic analysis platform will be based on the big data framework Apache Hadoop®. During the development of this platform several disk images will be created, that can be used for testing. These disk images can be very large and must be preprocessed before saving it on the analysis platform. Otherwise the data processing engine can't process the data parallelly. There are several approaches how to save the data in a suitable manner on the cluster. In the first approach the data, saved on disk images, will be imported file by file. With this approach the data processing engine can be executed in parallel because the files can be analysed independently from each other. On the downside, the file metadata will be saved in a way that doesn't allow parallelized data processing. To solve this issue the finally introduced approach for data persistence contains a mixture of two different data storage types. The metadata of all imported files will be stored on a column-oriented database. Additionally the file content of small files will be also saved on this database. Whereas large files will be saved on the distributed file system of Hadoop. With this approach it's also possible to persist new information, extracted by the data processing engine, directly on the database.

The open-source data analytics cluster computing framework Apache Spark™ will be used as data processing engine. Based on this engine some simple data processing jobs will be implemented, like calculating file hashes and extracting file media types based on the file content.

In addition, a full text search will be implemented to support an easy access to the metadata. To get the extracted metadata quickly, it will be indexed by an enterprise search platform. Currently it's only possible to access the file metadata in this way. In future it shall be also possible to index the file contents to allow a real full text search on every persisted data.

The results of this work approve the feasibility to do forensic data analysis with the Apache Hadoop framework on large data sets. The data can be also accessed efficiently. Nevertheless there are some weaknesses that must be improved in future. The primary disadvantage of this analysis platform belongs to the time-consuming data import. To improve this performance issue, the data should be processed directly after saving it. With this approach the user can already analyse partial results while the data import is ongoing.

Danksagung

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne Verwendung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten und nicht veröffentlichten Schriften entnommen sind, sind als solche kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch in keiner anderen Prüfungsbehörde vorgelegen. Alle eingereichten Versionen der Arbeit sind identisch.

Meersburg, den 10.10.2018

Johannes Busam

Inhaltsverzeichnis

| | |
|--|-----------|
| 1 Einleitung | 1 |
| 1.1 Problemstellung | 1 |
| 1.2 Zielsetzung | 2 |
| 1.3 Aufbau | 4 |
| 2 Vorgehen | 5 |
| 2.1 Projektplanung | 5 |
| 2.2 Entwicklungsumgebung | 10 |
| 2.3 Testdatengenerierung | 12 |
| 3 Grundlagen von Apache Hadoop® | 13 |
| 3.1 Apache Hadoop Framework | 13 |
| 3.2 Apache Hadoop HDFS | 15 |
| 3.3 Apache Hadoop YARN | 18 |
| 3.4 Apache Spark | 20 |
| 3.5 Apache HBase | 22 |
| 3.6 Apache ZooKeeper | 25 |
| 3.7 Apache Solr und Lucene | 26 |
| 4 Datenspeicherung | 30 |
| 4.1 Allgemeiner forensischer Analyseprozess | 30 |
| 4.2 Klassisches Analysevorgehen | 33 |
| 4.3 Umsetzung in der forensischen Analyseplattform | 36 |
| 4.4 Variante 1 - Speicherung der Datenträgerabbilder | 36 |
| 4.5 Variante 2 - Speicherung der logischen Dateien | 38 |
| 4.6 Variante 3 - Speicherung in Dateicontainer | 41 |
| 4.7 Variante 4 - Speicherung in HBase und HDFS | 44 |
| 4.7.1 Allgemeines | 44 |
| 4.7.2 Speicherung kleiner Dateien | 44 |
| 4.7.3 Anwendungsimplementierung | 48 |
| 4.7.4 Datenmodell | 51 |
| 4.7.5 Datenspezifische Aspekte | 53 |
| 4.7.6 Zugriffs- und Ausführungsrechte | 53 |
| 4.8 Fazit | 55 |
| 5 Datenverarbeitung | 56 |
| 5.1 Klassisches Analysevorgehen | 56 |
| 5.2 Umsetzung in der forensischen Analyseplattform | 58 |

| | | |
|----------|---|-----------|
| 5.3 | Anwendungsfälle der Datenverarbeitung | 60 |
| 5.3.1 | Berechnung von Hashsummen | 60 |
| 5.3.2 | Erkennung von Duplikaten | 60 |
| 5.3.3 | Ermittlung von Medientypen | 61 |
| 5.3.4 | Volltextsuche und Datenindexierung | 62 |
| 5.4 | Praxisbeispiele und deren Optimierungen | 64 |
| 5.5 | Leistungsanalyse | 67 |
| 6 | Datenvisualisierung | 70 |
| 7 | Weitere Aspekte | 73 |
| 7.1 | Plattform absichern | 73 |
| 7.1.1 | Allgemeines | 73 |
| 7.1.2 | Authentifizierung | 73 |
| 7.1.3 | Datenverschlüsselung | 75 |
| 7.2 | Datenlöschung | 76 |
| 8 | Zusammenfassung | 77 |
| 9 | Ausblick | 78 |
| A | Allgemeines | 88 |
| A.1 | Analyse ähnlicher Projekte und Produkte | 88 |
| A.2 | Lizenzierungen in dieser Arbeit | 89 |
| B | Datenimport | 90 |
| B.1 | Konfigurationsdateien | 90 |

1 Einleitung

1.1 Problemstellung

Die forensische Analyse von digitalen Beweismitteln ist in der heutigen Zeit ein wichtiger Aspekt, um in der Strafverfolgung rechtswidriges Verhalten aufzudecken oder nachzuweisen. In vielen Fällen werden informationstechnische Systeme am Tatort gefunden oder zur Tatbegehung genutzt. Einschlägig sind hierbei Angriffe auf kritische Infrastrukturen durch Computersabotage oder das Ausspähen von Daten. Aber auch Urheberrechtsverletzungen durch die Weitergabe von geschützten Medien oder Verstöße gegen das Wettbewerbsrecht werden mit Informationstechnik begangen. Je nach Dauer und Umfang der Strafhandlung werden gerade auch im Bereich der Wirtschaftskriminalität dutzende Asservate von informationstechnischen Systemen sichergestellt. Beispielsweise werden beteiligte Computer und Mobiltelefone beschlagnahmt. Oder es werden logische Sicherungen von Netzwerkspeichern durchgeführt.

Bei der Analyse dieser Asservate möchte ein forensischer Ermittler möglichst schnell einen Überblick über die sichergestellten Daten erhalten. Darauf aufbauend kann er entscheiden, welche Spuren in den Daten zum Nachweis konkreter Tathandlungen dienen und welche potentielle Beweismittel nicht weiter analysiert werden müssen.

Der kritischste Aspekt hierbei ist, in kürzester Zeit die richtigen Informationen aus allen Daten zu extrahieren. Denn gerade in der Strafverfolgung ist eine schnelle und zielgerichtete Aufarbeitung der Ermittlungsfälle erforderlich. Darüber hinaus werden während der Analyse oftmals weitere Indizien gefunden, welche wiederum zur Sicherung neuer Asservate führen können. Je mehr Zeit jedoch für die Analyse benötigt wird, desto höher ist die Gefahr, dass noch nicht sichergestellte Daten endgültig gelöscht werden. Beispielsweise werden Telekommunikationsverbindungsdaten nicht über längere Zeiträume gespeichert.

Zur Analyse stehen dem Forensiker etliche proprietäre und Open-Source Programme zur Auswahl. Allerdings sind im forensischen Open-Source Bereich viele Programme durch die Ressourcen des Analyserechners beschränkt. Sie bieten keine Möglichkeiten rechenintensive Aufgaben performant auf mehreren Computern zu skalieren.

Aus fachlicher Sicht wäre eine Plattform sinnvoll, die anfallende Analyseaufgaben automatisiert auf allen Daten durchführt. Das System sollte die Ergebnisse, unter Berücksichtigung verfügbarer Ressourcen, schnellstmöglich ermitteln und dem forensischen Ermittler in einer aufbereiteten Form darstellen. Auf Basis dieser Ergebnisse kann sich der Forensiker möglichst frühzeitig einen Überblick über alle Asservate verschaffen, um dann bestimmte Daten auch in anderen spezialisierten Analyseanwendungen weiterzuverarbeiten.

1.2 Zielsetzung

Zur Lösung der Problemstellung soll in dieser Masterthesis eine Plattform zur forensischen Analyse entwickelt werden. Diese Plattform soll durch eine automatisierte Analyse und Aufbereitung forensisch relevanter Informationen dem Forensiker helfen, sich einen Überblick zu verschaffen. Er soll dadurch effizient und zielgerichtet Datenanalysen durchführen können. Als Basis dieser Plattform soll das Apache Hadoop® Framework genutzt werden. Hierbei sollen Vor- und Nachteile dieser Art der Datenverarbeitung im forensischen Kontext herausgearbeitet werden.

Apache Hadoop ist ein etabliertes Open-Source Framework zur verteilten Speicherung und Verarbeitung von Daten. Durch die parallele Datenverarbeitung eignet sich ein Hadoop-Cluster auch zur Prozessierung von großen Datenmengen im Terabyte-Bereich. Ein zugrundeliegendes Paradigma ist hierbei, dass die Programmausführung dort stattfindet, wo auch die Daten liegen, um kostspielige Datentransporte weitgehend zu vermeiden. Aufgrund dieser Beschaffenheit kann diese Art der Datenverarbeitung auch Geschwindigkeitsvorteile bei forensischen Analysen bieten.

Ein wichtiger Aspekt der Masterthesis ist die Aufbereitung der Daten für die Analyse im Hadoop-Cluster. Hierbei sollen mehrere Möglichkeiten analysiert werden, wie diese Aufbereitung und Speicherung der Daten im Hadoop-Cluster gelingen kann. Dabei muss auch auf die Unversehrtheit der Dateiinhalte und Metadaten bei der Aufbereitung geachtet werden. Darauf aufbauend soll eine fachliche Verwaltungsstruktur entwickelt werden, die es auch erlaubt, mehrere Asservate von beliebigen Ermittlungen parallel zu verarbeiten. Dadurch können auch Zusammenhänge zwischen unterschiedlichen Asservaten identifiziert werden.

Im Rahmen der Thesis soll die Datenanalyse vorerst grundlegende Funktionen unterstützen. So sollen die Metadaten, wie beispielsweise Name, Dateipfad, Hashsumme, Dateityp, Größe und Zeitstempel ermittelt werden und zu weiteren Analysen zur Verfügung stehen. Es soll auch eine Volltextsuche auf den Daten möglich sein. Darauf aufbauend soll der Nutzer beispielsweise gleiche Dateien und Verbindungen zwischen den einzelnen Beweismitteln erkennen können. Optional könnte die Analyseplattform gezielt nach IP-Adressen, Web-Adressen, E-Mail-Adressen oder Positionsdaten¹ suchen.

Die Resultate durchgeföhrter Datenanalysen sollen dem Nutzer bereitgestellt werden. Hierzu wird eine grafische Oberfläche benötigt, welche die fachlichen Aspekte der forensischen Analyseplattform widerspiegelt. Im Rahmen der Thesis sollen Möglichkeiten analysiert werden, wie eine grafische Oberfläche aussehen könnte. In diesem Kontext soll auch geprüft werden, ob existierende Programme zur Datenvisualisierung im Hadoop-Umfeld wiederverwendet werden können. Die Implementierung einer grafischen Oberfläche ist im Rahmen dieser Thesis jedoch nicht angedacht.

Abbildung 1.1 skizziert das angestrebte Analysevorgehen mit dieser Analyseplattform. Der Forensiker soll digitale Asservate in das Hadoop-Cluster importieren können. Nachfolgend hat er die Möglichkeit, diverse Analysen auf den Daten durchzuführen. Die Ergebnisse könnten später über eine entsprechende Oberfläche visualisiert werden.

¹Beispielsweise könnten Geopositionen oder Ortsnamen aus Dateien extrahiert werden. Diese Daten könnten dann mit ihrem geografischen Bezug auf einer Karte dargestellt werden.

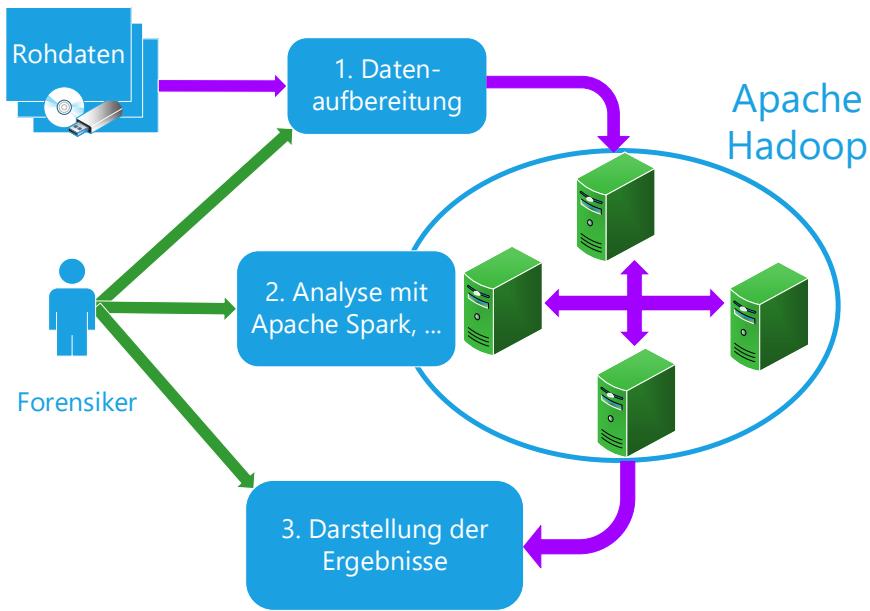


Abbildung 1.1: Analysevorgehen

Das Ziel dieser Masterthesis ist es, dem forensischen Ermittler schnellstmöglich einen Überblick zu den einzelnen Beweismitteln und deren Zusammenhänge im Kontext einer Fallanalyse zu liefern.

Bei einer realen forensischen Analyse gibt es weitere Anforderungen, die das Analysesystem erfüllen sollte. Da in vielen Fällen hochsensible personenbezogene Daten und Geschäftsgeheimnisse verarbeitet werden, müssen auch entsprechende Regelungen getroffen werden, wie nach der Analyse alle Daten restlos aus dem System gelöscht werden können.

Das System muss gegen fremden Zugriff gesichert sein. Es muss zu jeder Zeit ersichtlich sein, welche Personen zu welchem Zweck auf das System zugreifen.

Ein weiterer Aspekt in der Analyse ist die lückenlose Erstellung einer Beweismittelkette (Chain of Custody). Für jedes forensische Analyseergebnis müssen die Herkunft und die Verarbeitungsschritte transparent nachvollziehbar sein.

Im Rahmen der Masterthesis sollen diese Aspekte zumindest theoretisch und wenn möglich, auch praktisch analysiert werden.

Aus organisatorischer Sicht soll die Analyseplattform als Open Source Projekt bereitgestellt werden. Hierzu soll der Source-Code, die Konfiguration des Systems und die Dokumentation in einer öffentlich zugänglichen Versionsverwaltung verfügbar sein.

1.3 Aufbau

In Kapitel 1 wird das Eingangsproblem und die Ziele dieser Masterthesis beschrieben.

In Kapitel 2 folgt das allgemeine Entwicklungsvorgehen. Darin ist der aktuelle Projektplan enthalten, welcher die Arbeitspakete definiert. Zusätzlich wird die genutzte Entwicklungsumgebung skizziert.

In Kapitel 3 erfolgt eine Darstellung der Apache Hadoop Plattform, inklusive der theoretischen Grundlagen zur Arbeitsweise des Frameworks. Des Weiteren werden darauf aufbauende Projekte, wie beispielsweise Apache Spark und Apache HBase erklärt.

In Kapitel 4 werden unterschiedliche Varianten zur Datenspeicherung und Aufbereitung analysiert. Innerhalb dieses Kapitels wird ein Vorgehen entwickelt, wie die Daten eines Asservats im Hadoop-Cluster gespeichert werden können, um sie später parallelisiert verarbeiten zu können. Zu Beginn wird das herkömmliche Analysevorgehen in Verbindung mit der Analyseanwendung *Autopsy* beschrieben, um fachlich relevante Aspekte bei der Analyse herauszuarbeiten.

Die eigentliche Datenverarbeitung wird in Kapitel 5 beschrieben. Hier wird ein Ansatz vorgestellt, wie die Daten parallel verarbeitet werden können. Anhand dieses Ansatzes werden Hashsummen der Daten berechnet und die Medientypen der Dateien ermittelt. Zum Schluss wird eine Möglichkeit vorgestellt, wie die Informationen für eine Volltextsuche aufbereitet werden können.

Die Visualisierung der Informationen ist ein interessanter Aspekt der forensischen Analyseplattform, welcher in Kapitel 6 beschrieben wird. Dort werden einige Möglichkeiten erläutert, wie eine Visualisierung aussehen könnte.

In Kapitel 7 werden querschnittliche Aspekte zur Datensicherheit von forensischen Analysen und zum Löschen von Daten dargestellt.

Zuletzt erfolgt in Kapitel 8 eine Zusammenfassung der erarbeiteten Ergebnisse. Es wird auch aufgezeigt, ob das Apache Hadoop Framework überhaupt die Anforderungen einer forensischen Analyseplattform erfüllen kann.

Offene Punkte und Verbesserungen werden in Kapitel 9 beschrieben.

2 Vorgehen

2.1 Projektplanung

Zur Realisierung einer forensischen Analyseplattform wurde ein Projektplan erstellt, welcher die einzelnen Aufgaben im Rahmen der Masterthesis enthält. Abbildung 2.1 zeigt die Aufteilung in diese Arbeitspakete.

Das Ziel der Einarbeitungsphase ist es, ein grundlegendes Verständnis über die Datenverarbeitung im Hadoop-Framework zu erhalten. Zusätzlich soll eine Entwicklungsumgebung inklusive öffentlicher Versionsverwaltung eingerichtet werden. Danach erfolgt der Aufbau eines eigenen Hadoop-Clusters und die Beschaffung von Testdaten.¹ Für die Einarbeitung und den Aufbau sind vier Wochen eingeplant (siehe Abbildung 2.2).²

Der zweite Teil behandelt die Datenaufbereitung und Speicherung im Hadoop-Cluster. Es soll geprüft werden, welche Struktur der Daten für eine optimale Speicherung und Verarbeitung im Hadoop-Framework erforderlich ist. Für diesen Teil sind vier Wochen Bearbeitungszeit geplant.

Am Ende des Arbeitspaketes soll ein erster Zwischenbericht erstellt werden, welcher die bisherigen Ergebnisse enthält (siehe Abbildung 2.2).

Nach der Speicherung der Rohdaten erfolgt im dritten Arbeitspaket die Datenanalyse mit Apache Spark. Hier sollen die Daten nach anwendungsbezogenen Problemstellungen analysiert werden. Ein weiterer Aspekt der Datenanalyse beschäftigt sich mit den Möglichkeiten, wie die Ergebnisse persistiert werden können.³ Im Anschluss soll die Performanz der Algorithmen geprüft werden. Hier bietet sich der Vergleich zu herkömmlichen Analyseprogrammen an. Denn schließlich hat diese Thesis auch das Ziel, bei großen Datenmengen schneller Ergebnisse zu liefern als die herkömmlichen Analysewerkzeuge auf einem einzelnen Analyserechner. Für dieses Arbeitspaket sind sieben Wochen eingeplant (siehe Abbildung 2.3). Darauf folgt ein zweiter Zwischenbericht.

Im letzten Drittel der Masterthesis sollen querschnittliche Aspekte in die bestehende Analyseplattform integriert werden. Hierbei geht es um das Absichern der Plattform, die Dokumentation der Beweismittelkette und um das sichere Löschen von Asservaten. Für dieses Arbeitspaket sind vier Wochen eingeplant (siehe Abbildung 2.4).

¹Hierbei wird ein bestehendes Hadoop-Cluster genutzt und um zusätzliche Softwarepakete ergänzt.

²Die referenzierten Gantt-Diagramme wurden mit der JavaScript-Bibliothek *dhtmlxGantt* erstellt. Der Quellcode ist unter der *GNU GPLv2*-Lizenz lizenziert. Weitere Informationen können in Kapitel A.2 im Anhang nachgelesen werden.

³Hierfür soll Apache HBase zur Speicherung von strukturierten und unstrukturierten Daten untersucht werden.

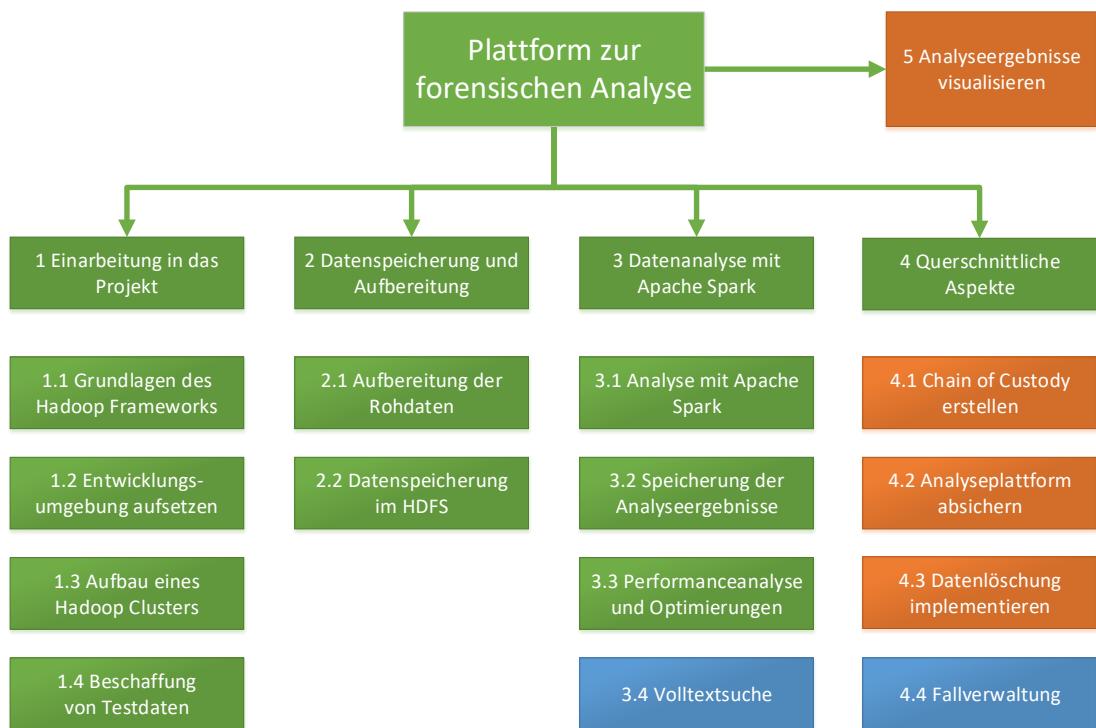


Abbildung 2.1: Arbeitspakete der Masterthesis

Das letzte Arbeitspaket enthält eine prototypische Visualisierung der Analyseergebnisse. Hierbei soll geprüft werden, welche Möglichkeiten zur Darstellung der Ergebnisse existieren. Für diese Arbeit sind drei Wochen eingeplant (siehe Abbildung 2.4).

Projektverlauf

Während dem Projektverlauf wurde die Planung teilweise angepasst. Es wurden einige Aspekte aus der Planung entfernt (orange hinterlegt in Abbildung 2.1). So werden die Visualisierung der Ergebnisse, die Erstellung der Beweismittelkette, das Absichern der Analyseplattform und die forensisch korrekte Datenlöschung nicht implementiert, sondern nur theoretisch erläutert. Der Hauptgrund dafür ist eine verlängerte Analyse- und Implementierungsphase zum Importieren und Speichern von Asservaten im Hadoop-Framework. Es wurden mehrere Ansätze entwickelt und getestet. Dadurch verlängerte sich die ursprünglich angedachte Bearbeitungszeit.

Andererseits sind auch neue Arbeitspakete hinzugekommen (blau hinterlegt in Abbildung 2.1). So wurde bei der Datenanalyse mit Apache Spark sichtbar, dass die Informationen und Analyseergebnisse performant durchsuchbar sein müssen. Daher wurde untersucht, wie eine Volltextsuche aller gespeicherten Daten im Hadoop-Cluster realisiert werden könnte. Ein anderer Aspekt ist die Implementierung einer Fallverwaltung. Denn damit können nun mehrere Asservate in das System importiert werden, um Zusammenhänge identifizieren zu können.

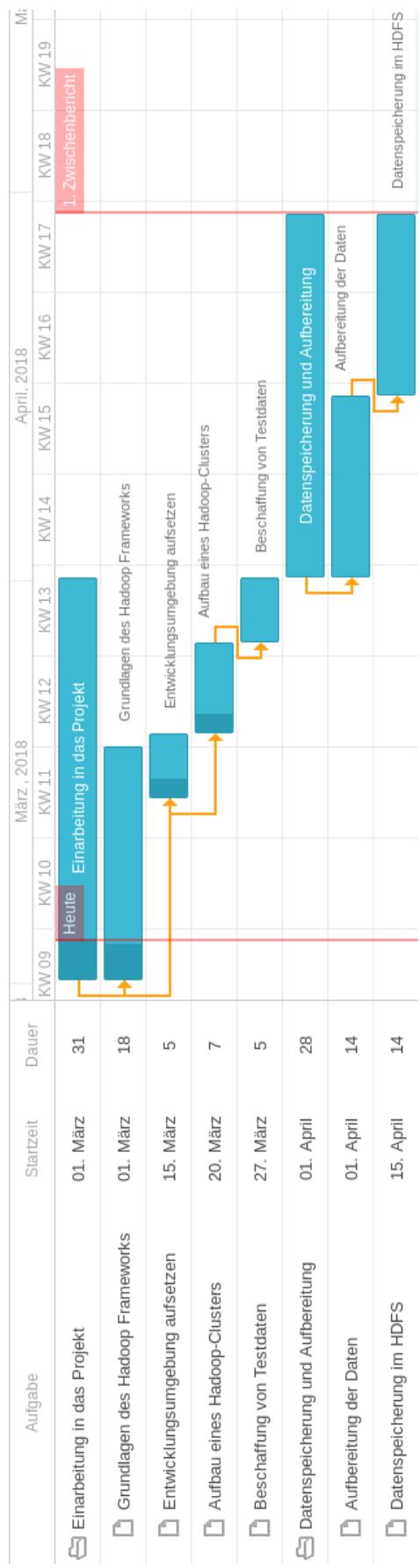


Abbildung 2.2: Projektplan Teil A - Einarbeitung und Rohdatenspeicherung (siehe Kapitel A.2)

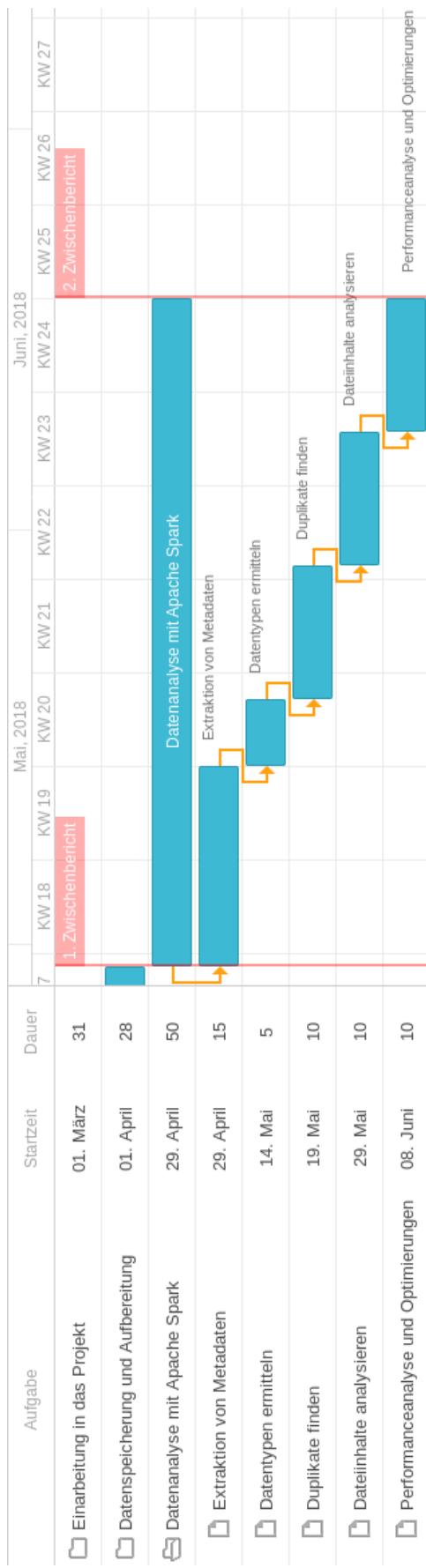


Abbildung 2.3: Projektplan Teil B - Datenanalyse (siehe Kapitel A.2)



Abbildung 2.4: Projektplan Teil C - Querschnittliche Aspekte und Visualisierung (siehe Kapitel A.2)

2.2 Entwicklungsumgebung

Der Aufbau einer Test- und Entwicklungsumgebung ist ein wichtiger Bestandteil dieser Thesis. Einerseits sollen Anwendungsprogramme zur Datenverarbeitung schnell und lokal ausführbar sein. Andererseits soll die Testumgebung auf einem realen Apache Hadoop Cluster basieren, um mögliche Infrastrukturprobleme identifizieren zu können und die Performance zu testen.

Abbildung 2.5 skizziert die Komponenten der Entwicklungsumgebung. Zentraler Bestandteil ist ein Entwicklungsrechner mit der Linux-Distribution *Fedora* in der Version 28 64-bit.

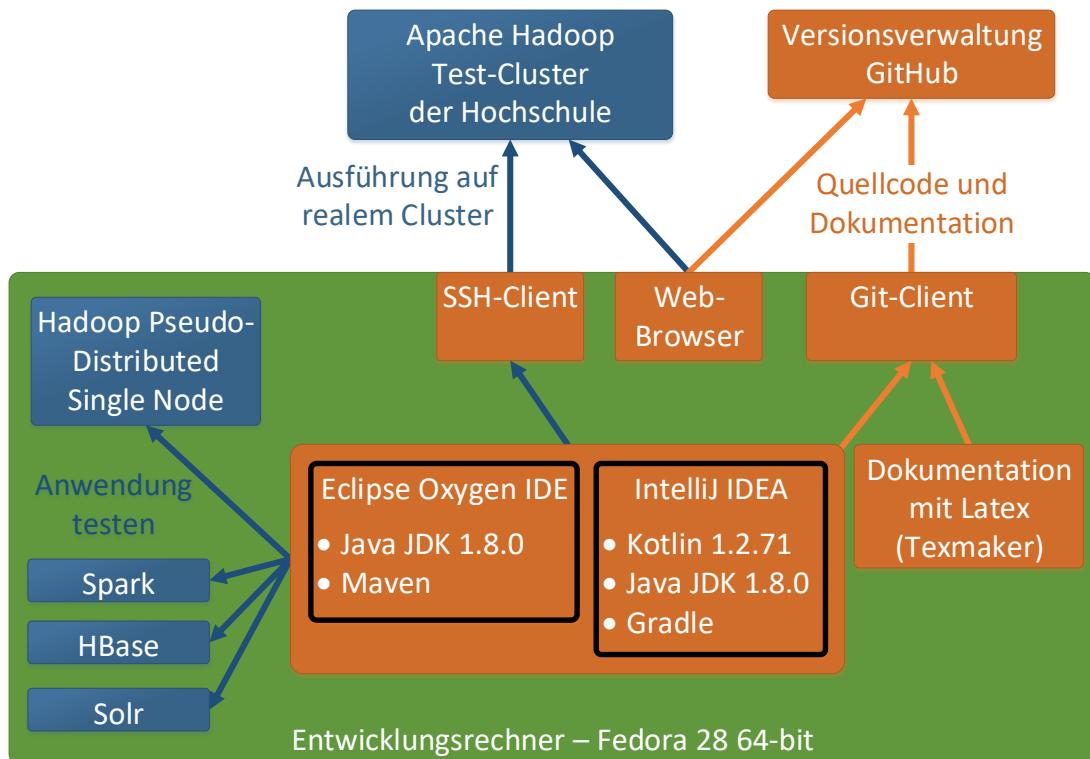


Abbildung 2.5: Komponenten der Entwicklungsumgebung

Zur Entwicklung der forensischen Analyseprogramme wird *Eclipse Oxygen* genutzt. Die Anwendungen selbst werden in Java geschrieben.⁴ Zum Bauen der ausführbaren Java Archive (JAR) wird *Maven* verwendet. Mit Maven können weitere Java-Bibliotheken in eigenen Programmen auf einfache Weise wiederverwendet werden.⁵

Zusätzlich befindet sich die Entwicklungsumgebung *IntelliJ IDEA* in der kostenlosen Community Variante auf dem Entwicklungsrechner. Mit der IntelliJ IDEA wird die Datenimport-Anwendung in *Kotlin* entwickelt. Kotlin ist eine statisch typisierte Programmiersprache zur Anwendungsentwicklung auf verschiedenen Plattformen.⁶ Sie ist interoperabel mit Java. Die Anwendungen können in der *Java Virtual Machine* (JVM) ausgeführt werden.

⁴Wobei auch Python oder Scala als Programmiersprache genutzt werden kann.

⁵Diese können über ein zentrales Repository, dem sogenannten *Maven Central Repository* aus dem Internet geladen werden (siehe Link <https://search.maven.org/>. Letzter Zugriff 26.8.2018).

⁶Siehe Link <https://kotlinlang.org/>. Letzter Zugriff: 24.8.2018.

Gegenüber Java bietet sie diverse Sprachkonstrukte zur Optimierung des Programmcodes an. Darüber hinaus können alle Bibliotheken aus dem Java-Umfeld auch in Kotlin genutzt werden. Zum Bauen der Kotlin-Anwendungen wird *Gradle* genutzt, welches analog zu Maven Abhängigkeiten zu Drittbibliotheken und deren Versionen verwaltet.⁷

Um die gebauten Java- und Kotlin-Programme schnell zu testen, können alle notwendigen Komponenten auch lokal auf dem Entwicklungsrechner gestartet werden. Hierzu gehört ein Hadoop-Knoten im sogenannten *Pseudo-Distributed* Modus, eine lokale Spark-Instanz, eine HBase-Instanz und eine Solr-Instanz zur Datenindexierung.⁸

Mithilfe dieser Komponenten können auch spezifische Konfigurationen getestet werden.⁹ Letztendlich kommen die lokalen Instanzen schnell an ihre Grenzen, gerade wenn größere Datenmengen analysiert werden sollen. Daher werden spezifische Konfigurationen und fertiggestellte Analyseprogramme auch auf einem realen Apache Hadoop-Cluster durchgeführt. Dort kann das Zusammenspiel zwischen den Komponenten nachvollzogen werden. Auch entsprechende Last-Tests sind nur auf dem Hadoop Test-Cluster möglich. Um mit dem Test-Cluster arbeiten zu können, wird ein SSH-Client benötigt. Zusätzlich gibt es eine Web-Oberfläche, basierend auf Apache Ambari, zur Konfiguration und Anzeige des aktuellen Systemzustandes.

Alle selbst erstellten Anwendungsprogramme, Konfigurationsdateien und die Dokumentation dieser Thesis sollen als Open-Source Projekte in einem öffentlichen Repository zugänglich sein. Gerade in der Forensik ist es sehr wichtig, dem Nutzer die Möglichkeit zu geben, den Quellcode der Analyseprogramme einsehen zu können und notfalls auf spezielle Bedürfnisse anzupassen. Darüber hinaus kann die Datenverarbeitung transparent nachvollzogen werden. Daher werden die einzelne Projekte mithilfe eines Git-Clients auf GitHub versioniert.

Nachfolgende Auflistung zeigt die Aufteilung der Projekte:

- Das Projekt *foam-thesis*¹⁰ enthält die schriftliche Ausarbeitung der Thesis und den Quellcode als Latex-Projekt. Als Entwicklungsumgebung wird *Texmaker* genutzt. Über den Link <https://github.com/jobusam/foam-thesis> ist der aktuelle Stand der Arbeit jederzeit einsehbar.¹¹
- Das Projekt *foam-data-import* enthält den Quellcode zum Importieren von Asservaten in das Hadoop-Cluster. Unter <https://github.com/jobusam/foam-data-import> befindet sich die Kotlin-Anwendung, welche wiederum mit Gradle gebaut werden kann.
- Das Projekt *foam-processing-spark* enthält den Quellcode zur Auswertung mit Apache SparkTM. Unter <https://github.com/jobusam/foam-processing-spark> befindet sich ein Maven-Projekt, welches wiederum die Java-Anwendung baut. Es werden

⁷Siehe auch Kapitel 4.7.3 für weitere Informationen zur Datenimportanwendung.

⁸Siehe Kapitel 3 für eine detaillierte Erklärung der Komponenten.

⁹Hierfür muss der Entwicklungsrechner entsprechende Ressourcen bereitstellen. Es sollte mindestens eine Quad-Core-CPU, 16 GB Arbeitsspeicher und eine SSD zur Verfügung stehen, um performant arbeiten zu können.

¹⁰Die Abkürzung *foam* oder auch *FoAm* steht für *forensische Analyseplattform*.

¹¹Das erstellte PDF-Dokument zum jeweiligen Stand wird im gleichen Projekt versioniert und ist unter dem Link <https://github.com/jobusam/foam-thesis/blob/master/main.pdf> verfügbar (Letzter Zugriff: 6.10.2018).

auch entsprechende Skripte zum Starten von Spark-Anwendungen für lokale Installationen und Hadoop-Cluster bereitgestellt.

- Das Projekt *foam-storage-hadoop* enthält alle Konfigurationsdateien zum Aufsetzen eines Hadoop-Clusters auf einem einzelnen Knoten im *Pseudo-Distributed Mode*.¹² Zusätzlich existieren Shell-Skripte zum Starten des Hadoop-Clusters auf einem einzelnen Knoten.¹³ Mithilfe der Skripte aus dem *foam-processing-spark* Projekt können damit Spark-Anwendungen ausgeführt werden. In diesem Projekt sind auch weitere Konfigurationen zur Installation von HBase und Solr enthalten.

Die Dokumentation der Thesis und alle erstellten Diagramme sind unter der Lizenz *Creative Commons Attribution Share Alike 4.0 (CC-BY-SA-4.0)* lizenziert. Der Quellcode der forensischen Analyseplattform und die erstellten Konfigurationen sind unter der Apache Lizenz 2.0 lizenziert. Dadurch ist der Quellcode frei zugänglich und kann von jedem genutzt und verändert werden.

2.3 Testdatengenerierung

Für den Aufbau einer forensischen Analyseplattform sollen entsprechende Testdaten generiert werden. Hierzu werden zwei unterschiedliche Falldaten erzeugt. Der erste Fall ist ein kleines Datenträgerabbild mit knapp 10 GB Gesamtgröße. Dieses Image soll für lokale Tests genutzt werden, um die entwickelten Implementierungen zur Datenspeicherung und Verarbeitung schnell auf ihre Korrektheit prüfen zu können. Der Datenträger enthält eine Partitionen mit dem ext4-Dateisystem. Darauf ist ein Ubuntu 16.04 LTS installiert. Zusätzlich sind auch noch einige Testdaten darauf gespeichert.

Im zweiten Fall wird ein 155 GB großes Image erzeugt. Der Datenträger besteht wiederum aus einer Partition mit einem NTFS-Dateisystem. Darauf ist Windows 10 installiert. Zusätzlich sind größere Datensätze von Bildern und Musik aus dem Internet darauf gespeichert. Die Datensätze werden kostenfrei als Trainingsdaten zum maschinellen Lernen angeboten. Dieses größere Datenträgerabbild kann zur Verarbeitung im Testcluster genutzt werden, um die Skalierbarkeit bei großen Datenmengen zu testen. Beide Datenträgerabilder werden in Kapitel 5.5 für Leistungstests verwendet. Hierzu befinden sich einige sehr große und auch viele kleine Dateien auf den Datenträgern, um möglichst realitätsnahe Testergebnisse zu erhalten.

¹²Siehe Link: <https://github.com/jobusam/foam-storage-hadoop/tree/master/hadoop.standalone.configuration>. Letzter Zugriff: 6.10.2018.

¹³Siehe Link: <https://github.com/jobusam/foam-storage-hadoop/tree/master/hadoop.standalone.setup>. Letzter Zugriff: 6.10.2018.

3 Grundlagen von Apache Hadoop[®]

3.1 Apache Hadoop Framework

Apache Hadoop[®] ist ein etabliertes Java-Framework zur verteilten Speicherung und Verarbeitung von Daten. Durch die parallele Ausführung von Algorithmen, eignet sich ein Hadoop-Cluster für rechenaufwendige Datenanalysen. Ein primäres Paradigma ist das Konzept der *Datenlokalität*. Die auszuführenden Programme werden auf die Knoten verteilt, auf welchen auch die Daten liegen. Ressourcenintensive Datentransporte sollen weitgehend vermieden werden.[5, S. 20 ff.]

Das Framework ist für die Ausführung auf Standardhardware konzipiert. Es wird also keine verhältnismäßig teure Spezialhardware benötigt. Das Cluster besteht aus vielen einzelnen Knoten mit Standardcomputern, welche im Verhältnis zu Spezialservern günstiger und leicht ersetzbar sind. Der Ausfall einzelner Knoten wird bei der Datenhaltung entsprechend berücksichtigt.

Hadoop selbst besteht aus mehreren Komponenten, welche spezifische Aufgaben übernehmen. Abbildung 3.1 stellt eine grobe Skizzierung der Komponentenlandschaft der Plattform dar.¹

Die Basis bildet das *Hadoop Distributed File System (HDFS)*, welches die Daten redundant auf allen Knoten des Computer-Clusters speichert. Hierbei besteht das Computer-Cluster selbst aus mehreren Knoten, auf welchen vorzugsweise ein Linux-Betriebssystem, wie beispielsweise CentOS, läuft.

Der Ressourcenmanager *YARN (Yet Another Resource Negotiator)* ist für die Verteilung und Bereitstellung von verfügbarer Rechenleistung verantwortlich.

Die dritte Komponente ist das *Hadoop Map-Reduce Framework*. Hadoop Map-Reduce kann zur Datenverarbeitung genutzt werden. Hierbei werden Algorithmen parallel auf den Knoten prozessiert und die Ergebnisse im Anschluss zusammengetragen. Die einzelnen Zwischenergebnisse werden alle im HDFS abgelegt.²

Das verteilte Dateisystem HDFS und der Ressourcenmanager YARN bilden den Kern des Hadoop-Clusters. Darauf aufbauend können andere Komponenten die Daten verarbeiten

¹In der Abbildung 3.1 werden Logos der einzelnen Apache Projekte verwendet. Diese sind Handelsmarken der *Apache Source Foundation* (siehe Link: <https://www.apache.org/>. Letzter Zugriff: 6.10.2018). In Kapitel A.2 im Anhang werden die Logos und deren Herkunft nochmals aufgelistet.

²Sogenannte Map-Reduce Jobs bildeten in den Anfängen von Hadoop den primären Weg, Daten verteilt zu verarbeiten. Mittlerweile wurde diese Art der Datenverarbeitung in den Hintergrund verdrängt, da andere Projekte, wie beispielsweise Apache Spark, die Daten schneller verarbeiten können oder andere Ansätze zur Verarbeitung nutzen. Dies ist beispielsweise auch der Grund, weshalb Hadoop Map-Reduce in dieser Masterthesis nicht genutzt wird.

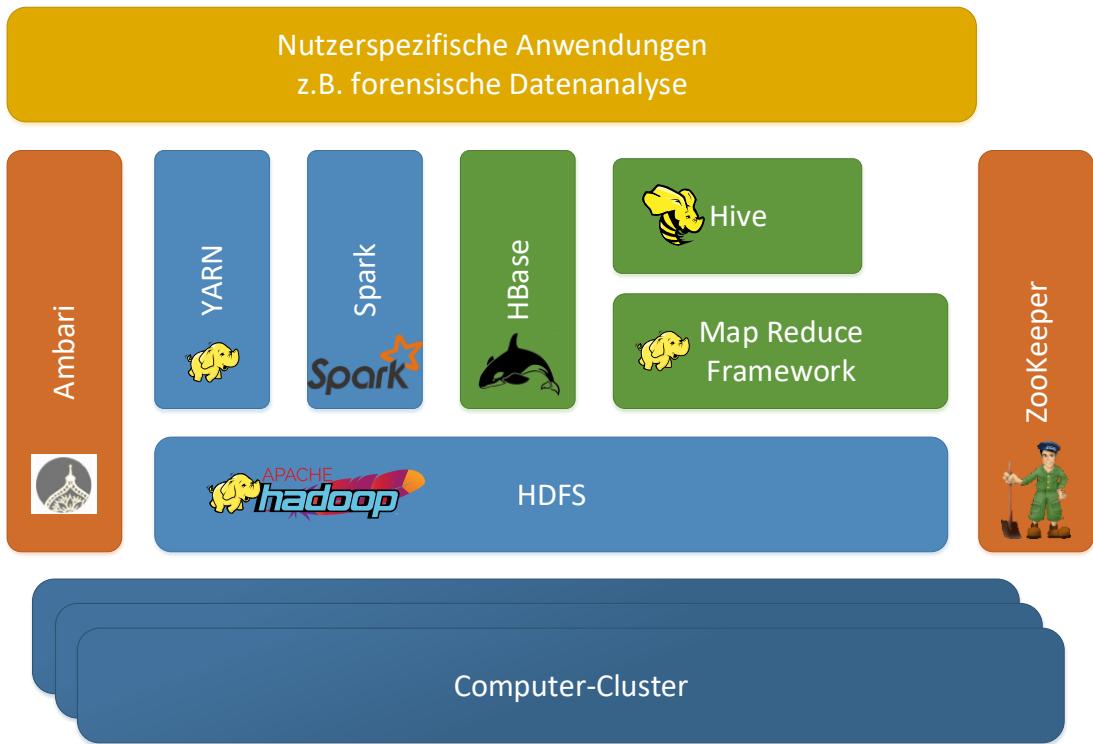


Abbildung 3.1: Apache Hadoop Ökosystem (Vgl. [5],[13]. Siehe Kapitel A.2)

oder weitere Funktionen anbieten. So wird beispielsweise in dieser Thesis *Apache SparkTM* bei der Prozessierung und Analyse der Daten genutzt. Der Vorteil von Apache Spark ist eine performante Datenverarbeitung, da einerseits die Daten verteilt verarbeitet werden und andererseits Zwischenergebnisse und temporäre Daten im Arbeitsspeicher der einzelnen Rechenknoten gehalten werden.³

Des Weiteren bietet *Apache HiveTM* eine Möglichkeit, Dateien im HDFS mithilfe einer SQL ähnlichen Syntax (HiveQL) abzufragen. Die Komponente nutzt wiederum das Map-Reduce Framework von Hadoop. Apache Hive ist jedoch keine reine Datenbank, sondern arbeitet auf den Dateien im HDFS.

Apache HBase[®] hingegen ist eine spaltenorientierte Key-Value Datenbank. Sie wurde eigens für Apache Hadoop implementiert, um große Datenmengen performant zu speichern.

Das Hadoop-Ökosystem als Ganzes muss auch konfiguriert und überwacht werden. Um die Verfügbarkeit einzelner Instanzen zu gewährleisten und gegebenenfalls redundante Verarbeitungswägen anzubieten, wird *Apache ZooKeeperTM* genutzt. Mit ZooKeeper ist es auch möglich, Konfigurationen und Änderungen im Cluster zu verteilen. Zum eigentlichen konfigurieren und überwachen des Hadoop-Clusters wird *Apache AmbariTM* genutzt.

Zusätzlich existieren dutzende weitere Projekte die auf dem Hadoop-Ökosystem aufbauen oder sich integrieren lassen. Mit *Apache Accumulo[®]* existiert eine weitere Key-Value Datenbank, welche eine Alternative zu HBase bietet. *Apache Livy* kann zur Ausführung

³Durch das In-Memory Computing ist Apache Spark deutlich schneller als das bereits erwähnte Hadoop Map-Reduce.

von Apache Spark Anwendungen, über eine REST-Schnittstelle, genutzt werden.⁴ *Apache NiFi* hingegen ermöglicht das Aufbereiten von Daten und organisiert Datenimporte.

Im Rahmen dieser Thesis wird auch das bekannte Open-Source Projekt *Apache SolrTM* verwendet, um innerhalb des Hadoop-Ökosystems eine Datenindexierung für eine Volltextsuche durchzuführen.

Prinzipiell sind die Komponenten auch unabhängig voneinander einsetzbar. So kann ein HDFS ausschließlich zur Datenhaltung aufgebaut werden, ohne eine Komponente zur Datenverarbeitung verwenden zu müssen. Umgekehrt lassen sich Komponenten zur Datenverarbeitung, wie Apache Spark, auch ohne das HDFS und YARN nutzen und können damit auch in andere Umgebungen integriert werden. Die einzelnen Komponenten entfalten, gerade durch die Kombination miteinander, ihr Potential zur performanten Datenanalyse.

Es gibt einige Unternehmen, die sich darauf spezialisiert haben, das Hadoop-Ökosystem inklusive weiterer Komponenten zu einzelnen Analyseplattformen zusammenzufassen. Sie bieten dafür kostenpflichtigen Support an, wobei diese Plattformen auch kostenfrei betrieben werden können. So wird im Praxisteil der Masterthesis die *Hortonworks Data Platform (HDP)* des Unternehmens *Hortonworks* genutzt.

3.2 Apache Hadoop HDFS

Das Hadoop Distributed File System (HDFS) ist ein verteiltes Dateisystem, welches die Grundlage zur Speicherung von Daten im Hadoop-Ökosystem bietet. Nachfolgende Zwecke soll es erfüllen.

Es soll ausfallsicher sein. In der Standardkonfiguration wird jede Datei im HDFS dreifach auf unterschiedlichen physikalischen Knoten gespeichert. Damit kann selbst bei einem Ausfall von zwei Knoten immer noch auf die Datei zugegriffen werden. Darüber hinaus verteilt das HDFS die Dateien automatisch und regeneriert sich selbst nach einem Knotenausfall. In großen Computer-Clustern mit mehreren hunderten Knoten ist ein Ausfall eines Knotens kein Sonderfall, sondern die Regel. Daher muss es sich selbst heilen können, um auch ohne manuelle Administration weiter verfügbar zu sein.

Das HDFS (und auch Hadoop im Allgemeinen) soll horizontal skalierbar sein. Wird mehr Speicher benötigt, werden einfach weitere Knoten hinzugefügt.

Das HDFS ist auf hohen Datendurchsatz und die Speicherung großer Datenmengen ausgelegt. So können einzelne Dateien mehrere Gigabyte bis hin zu Terabyte groß sein und es können mehrere Millionen Dateien im HDFS gespeichert werden. Die Optimierung auf einen möglichst hohen Datendurchsatz geht mit einer schlechteren Reaktionszeit, im Vergleich zu herkömmlichen Dateisystemen, einher.

Das Prinzip *Write-once-Read-many* wird im HDFS implementiert. Wenn Daten einmal geschrieben wurden, dann werden sie in der Regel nicht mehr geändert. Dies ermöglicht ein einfache Datenkohärenz. Der Lesedurchsatz wird gefördert, indem die Unterstützung der Datenmodifikation stark eingeschränkt wird. Ein wahlfreies Schreiben in eine existierende Datei wird beispielsweise nicht unterstützt. Änderungen an Daten, welche von Algorithmen vorgenommen werden, resultieren in neuen Datensätzen.

⁴ *Representational State Transfer (REST)* bezeichnet ein Programmierparadigma in verteilten Systemen. Hierbei werden Ressourcen über das Hypertext Transfer Protocol (HTTP) angefordert, gespeichert und verarbeitet.

Darüber hinaus gilt das Prinzip der Datenlokalität. Algorithmen werden dort ausgeführt, wo die Daten liegen, um das Transportieren von Daten über das Netzwerk zu vermeiden.[18]

Der Aufbau des HDFS bildet eine Master-Slave Architektur aus einem *Name Node* und mehreren *Data Nodes*. Der Name Node ist einmalig im verteilten System vorhanden und enthält alle Metainformationen zu den Dateien. Eine Datei wird in ein oder mehrere Blöcke aufgeteilt und auf mehreren Data Nodes gespeichert. Der Name Node organisiert diese Speicherung und bestimmt, wo welche Daten persistiert werden. Über den Name Node fließen aber keine Rohdaten von Dateiinhalten. Auf Dateisystemebene ist das HDFS, wie gängige Dateisysteme, hierarchisch organisiert. Jede Datei wird über einen absoluten Pfad eindeutig bestimmt und erhält entsprechende Metadaten, wie Dateirechte und Zeitstempel.

Abbildung 3.2 verdeutlicht die Struktur im HDFS. Angenommen es soll eine Datei im HDFS unter `/home/foo.txt` gespeichert werden. Dazu kann ein HDFS-Client genutzt werden, welcher Zugang zum Hadoop-Cluster hat. Der HDFS-Client speichert zuerst die Metadaten der Datei auf dem Name Node. Der Name Node kennt die Größe der Datei und entscheidet, in wie viele Blöcke sie unterteilt werden soll. Er ermittelt für jeden einzelnen Block, auf welchen Data Nodes dieser Block gespeichert werden soll. Diese Blockaufteilung und die Zuordnung zu den Data Nodes werden an den HDFS-Client zurückgeschickt. Dieser übermittelt die Blöcke an einen der Data Nodes. Sobald ein Data Node einen Block empfangen hat, schickt er diesen Block auch an die Knoten, welche eine Replikation des Blocks speichern sollen. Die Data Nodes stehen in Kontakt zum Name Node und senden Informationen über ihren Zustand und die momentan gespeicherten Blöcke. Der Name Node erhält dadurch auch eine Rückmeldung, falls ein Data Node ausfällt.

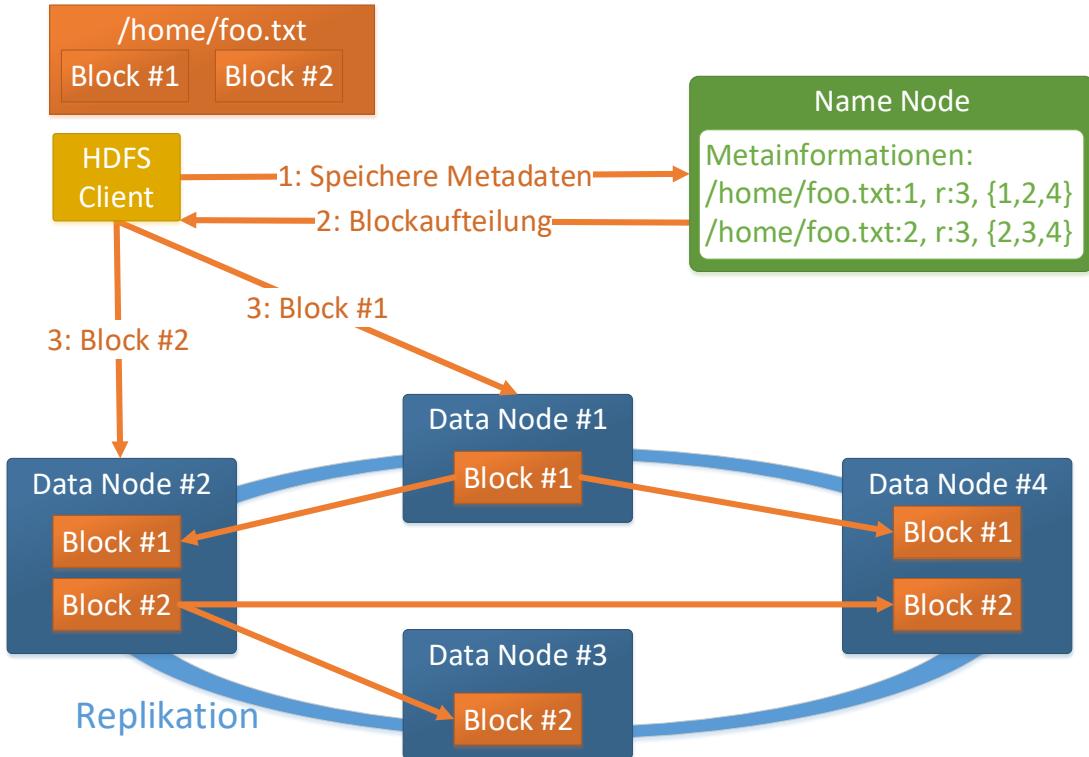


Abbildung 3.2: HDFS - Datenspeicherung im Verbund (Vgl. [18],[13])

Ein Block ist in der Standardkonfiguration 128 MB groß. Er kann bis zu 512 MB Blockgröße konfiguriert werden. Bei der Replikation wird der gleiche Block in unterschiedlichen Data Nodes angelegt.

Es ist nicht erlaubt, den gleichen Block mehrmals im gleichen Data Node zu replizieren. Dies wäre ohnehin sinnfrei, da die Replikation gerade vor einem Datenverlust, bei Ausfällen von einzelnen Knoten, schützen soll. Wichtig hierbei ist auch, dass im Produktivsystem auf jedem physikalischen Knoten nur ein Data Node oder ein Name Node läuft. Denn würden beispielsweise mehrere Data Nodes auf dem gleichen physikalischen Knoten laufen, so wäre bei einem Ausfall nicht mehr garantiert, dass die Dateiinhalte auch noch auf mindestens zwei anderen verfügbaren Knoten gespeichert sind. Denn der Replikationsmechanismus im HDFS kann nicht erkennen, ob jeder Knoten physikalisch unabhängig arbeitet. Allerdings hat Hadoop eine sogenannte *Rack-Awareness*. So ist es möglich, zu bestimmen, welche physikalischen Knoten in einem gemeinsamen Rack gruppiert sind. Abhängig davon, versucht das HDFS die Daten teilweise im selben Rack redundant zu speichern aber auch einige Replikationen außerhalb des Racks anzulegen. So kann auch der Ausfall eines Racks im Notfall kompensiert werden.

In einzelnen Testumgebungen ist es aber durchaus möglich, einen Name Node und einen Data Node oder mehrere Data Nodes gemeinsam auf einem physikalischen Knoten zu installieren. Allerdings greifen dann die eben beschriebenen Mechanismen zur Datensicherheit gegenüber Hardwareausfällen nicht mehr.

Wie in Abbildung 3.2 ersichtlich, ist der Name Node die Schlüsselstelle im HDFS-Cluster. Zusätzlich existiert ein sogenannter *Secondary Name Node*, der den (First) Name Node beim Speichern von Daten in gewisser Hinsicht unterstützt. Der Name Node hält die Metainformationen des HDFS im Arbeitsspeicher. Zusätzlich existieren zwei Dateien, das sogenannte *FsImage* und ein *EditLog*, welche persistent auf der Festplatte gespeichert sind. Das FsImage beschreibt einen Zustand der Dateisystemmetainformationen zu einem gewissen Zeitpunkt (Checkpoint). Im EditLog befinden sich alle Änderungen seit dem letzten Checkpoint bis zum aktuellen Zeitpunkt.

Der Secondary Name Node erstellt aus dem FsImage und dem EditLog regelmäßig neue Checkpoints, welche wiederum als neue FsImages gespeichert werden. Dieser Mechanismus wurde implementiert, um bei einem Neustart des Name Nodes die Startzeit zu optimieren. Dadurch kann die Verfügbarkeit des gesamten HDFS verbessert werden. Der *Secondary Name Node* unterstützt also den (First) Name Node, er kann ihn aber nicht ersetzen. Bei einem Ausfall wäre das HDFS nicht mehr einsatzbereit. Um dieses Problem zu umgehen, kann ein sogenannter *Standby Name Node* konfiguriert werden. Dieser kann einspringen, sobald der erste Name Node ausgefallen ist. Allerdings muss er extra konfiguriert werden.[13, S. 40 ff.]

Das HDFS kann über mehrere Wege genutzt werden. Es gibt eine Kommandozeilenschnittstelle, die sogenannte *FS Shell*. Mit der FS Shell können simple Dateioperationen durchgeführt werden. Die Befehlssyntax ähnelt hierbei stark der Befehlssyntax von UNIX/Linux-Betriebssystemen. Es ist auch möglich, über eine Java oder C++-Schnittstelle auf die Daten zuzugreifen. Das Dateisystem kann über eine REST-Schnittstelle via HTTP(S) genutzt werden. Auch das Mounten als *Network File System (NFS)* ist möglich. Das HDFS bietet auch eine Web-Oberfläche an, die es erlaubt, Daten auf einfache Weise hoch- und herunterzuladen.

3.3 Apache Hadoop YARN

YARN (Yet Another Resource Negotiator) ist eine Ressourcenverwaltung, welche die verfügbaren Ressourcen innerhalb des Hadoop Clusters organisiert und die Ausführungsreihe von Jobs plant und überwacht. Es gibt einen separaten *Resource Manager*, welcher nur die Ressourcen verwaltet. Auf jedem Knoten, der auch Datenverarbeitungen durchführt, ist ein *Node Manager* installiert. Zuletzt gibt es noch einen *Application Manager* für jeden einzelnen Job, der ausgeführt werden soll. Der Application Manager kontrolliert die Ausführung des Jobs. Abbildung 3.3 zeigt die Komponenten von YARN im Cluster.

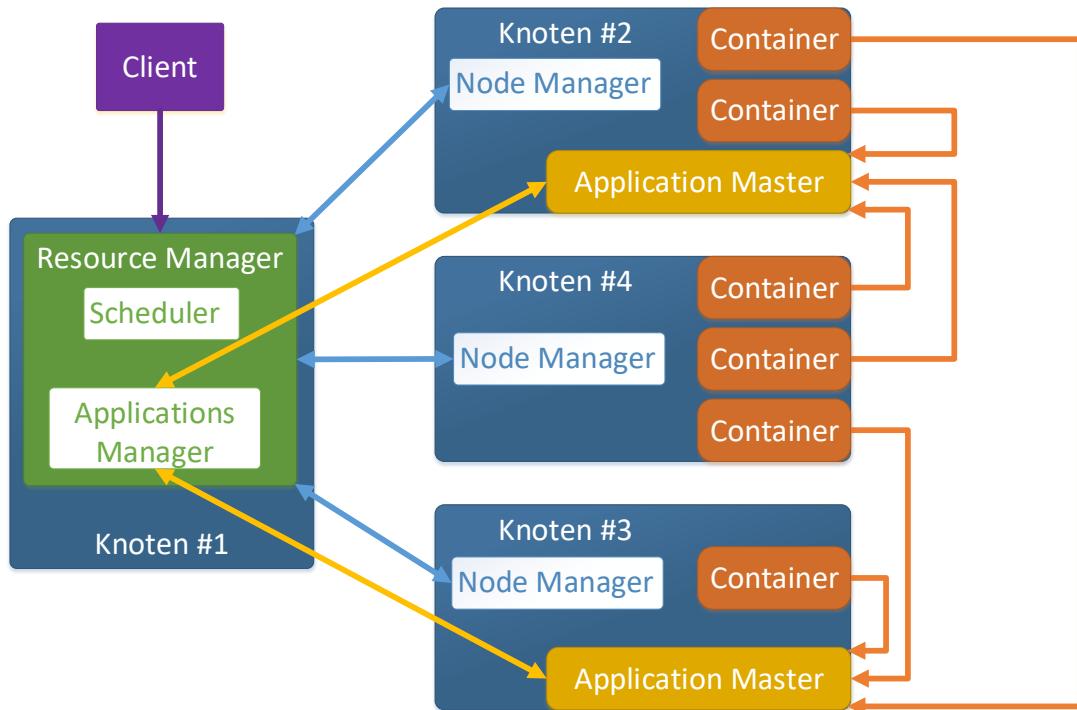


Abbildung 3.3: Ressourcenverteilung mit YARN (Vgl. [17],[13])

Ein Job oder eine Anwendung besteht aus mehreren Tasks. Diese Tasks können parallel in mehreren Containern ausgeführt werden. Ein Container ist eine abstrakte parallele Verarbeitungseinheit, welcher vordefinierte CPU- und Speicher-Ressourcen enthält. Es können mehrere dieser Container auf einem Knoten innerhalb des Clusters ausgeführt werden. Beispielsweise werden bei einem Knoten mit einer Quad-Core CPU und Hyperthreading (mit insgesamt 8 ausführbaren Threads) bis zu 8 Container erstellt. Bei 32 GB verfügbarem Arbeitsspeicher werden jedem Container 4 GB zugeteilt.⁵

Es ist nur möglich, die Anzahl der CPU-Cores (Ausführbare CPU-Threads) und die Größe des nutzbaren Arbeitsspeichers als Konfigurationsparameter festzulegen.[13, S. 48-57]

In den meisten Fällen sind diese beiden Parameter ausschlaggebend, um die Parallelität und den Ressourcenverbrauch des Systems zu steuern.

⁵In der Praxis ist es meistens weniger, da entsprechende Ressourcen für das darunter liegende Betriebssystem und die Hadoop-Komponenten reserviert werden.

Wenn nun eine Anwendung über YARN im Cluster ausgeführt werden soll, dann sendet ein Client eine Anfrage an den Resource Manager. Für jeden auszuführenden Job erstellt der Resource Manager den ersten Container. In diesem Container wird dann der Application Master gestartet, welcher sich im weiteren Verlauf um die Ausführung des Jobs kümmert. Der Resource Manager kennt die Anwendung nicht, noch weiß er wie diese ausgeführt wird. Er ist nur dafür zuständig, Ressourcen zu verteilen.

Der Application Master hingegen ist sehr spezifisch. Wird zum Beispiel eine Apache Spark Anwendung mit YARN ausgeführt, so ist der Application Master der sogenannte *Spark App Master*. Nachdem der Application Master im ersten erzeugten Container gestartet wurde, kann dieser wiederum neue Ressourcen beim Resource Manager anfordern. An dieser Stelle zeigt sich der Vorteil von YARN in Kombination mit dem HDFS. Denn bei der Anforderung von Ressourcen gibt der Application Master an, wie viele Container (inklusive Arbeitsspeicher und CPU) er benötigt. Zusätzlich übermittelt er die Dateiblöcke, welche er aus dem HDFS braucht und auf welchen Knoten er wie viele Container starten will.

In Abbildung 3.3 fordert der Application Master des Knoten #2 einen Container auf dem gleichen Knoten an. Zusätzlich möchte er zwei Container auf dem Knoten #4 erstellen. Der Application Master weiß, dass dort die benötigten Datenblöcke im HDFS gespeichert sind. Hierbei ist es wichtig zu verstehen, dass die Knoten aus Abbildung 3.3 den Data Nodes des HDFS aus Abbildung 3.2 entsprechen.⁶[13, S. 48-57]

Der Application Master erhält die Zustimmung vom Resource Manager, nachdem der Scheduler die geforderten Ressourcen entsprechend eingeteilt hat. Zusätzlich befiehlt der Resource Manager den Node Managern auf den jeweiligen Knoten, entsprechende Container zu erstellen.

Die einzelnen Node Manager stehen in Kontakt zum Resource Manager und senden ihm den aktuellen Status des Knotens und dessen Auslastung.

Nach der Ausführung der einzelnen Tasks in den Containern und dem Abschluss des Jobs, schickt der Application Master über den Applications Manager die Ergebnisse zurück zum Client.⁷ Danach meldet er sich beim Resource Manager. Zum Schluss gibt der Resource Manager die allokierten Ressourcen wieder frei.

Ähnlich wie beim Prozessscheduling in einem Betriebssystem, gibt es auch für YARN unterschiedliche Algorithmen, die festlegen, in welcher Reihenfolge und Zeitdauer die einzelnen Jobs ausgeführt werden. Bekannte Scheduler sind der *Fair Scheduler* und der *Capacity Scheduler*. Abhängig von der genutzten Plattform/Distribution einzelner Hersteller, ist für YARN ein anderer Scheduler konfiguriert.

Der Capacity Scheduler ist als Standard konfiguriert, da dieser versucht alle Knoten möglichst effizient auszusteuern, um den höchstmöglichen Datendurchsatz zu erreichen. Der Fair-Scheduler prüft hingegen, dass jedem Job die gleichen Ressourcen zugeteilt werden, um möglichst alle Jobs parallel bedienen zu können.

In großen Clustern wird die Prozessierung in mehrere Sub-Cluster, mit eigenen Resource Managern, aufgeteilt. Diese Struktur wird in der Literatur als *Federated YARN* beschrieben und soll die Skalierbarkeit von YARN in großen Clustern ermöglichen.

⁶Wobei ein physikalischer Knoten, auf welchem ein Data Node läuft, nicht zwingend auch für die Datenverarbeitung mit YARN verwendet werden muss. Beziehend auf das Paradigma der Datenlokalität ist es aber üblich, dass ein Knoten, welcher Daten persistiert, auch Daten verarbeitet.

⁷Hierbei werden die fachlichen Ergebnisse meistens als Datei im HDFS gespeichert.

3.4 Apache Spark

*Apache Spark*TM ist ein Framework zur verteilten Verarbeitung von großen Datenmengen. Mit Apache Spark können verschiedene Algorithmen und Verarbeitungsschritte über eine einheitliche Programmierschnittstelle auf gespeicherte Daten angewendet werden. Spark kümmert sich dabei um die Verteilung, Ausführung und Überwachung der datenverarbeitenden Applikationen.[7, S. 2]

Apache Spark ist mittlerweile schon fast der Standard, wenn es im Hadoop-Umfeld um die Datenverarbeitung geht. Es löst damit auch das ursprünglich verwendete Map Reduce Framework von Hadoop ab, denn Spark bietet einen enormen Geschwindigkeitsvorteil gegenüber von Hadoop Map Reduce. Dies lässt sich auf eine intelligente Ausführung einzelner Verarbeitungsschritte und diverse Optimierungen zurückführen.[13, S. 148-153]

Spark ermöglicht vielseitige Einsatzzwecke. So wird die klassische Datenverarbeitung von statischen Datenmengen⁸ unterstützt, aber auch die Verarbeitung von dynamischen Datenmengen (Streaming-Data).⁹ Auch die Prozessierung von Graphen-Strukturen und das maschinelle Lernen werden unterstützt.[13, S. 152]

Darüber hinaus steht es dem Anwender frei, ob er seine Applikationen in Scala, Python oder Java schreibt. Bei den Skriptsprachen Scala und Python gibt es eine Spark-Shell zur interaktiven Datenverarbeitung und Analyse. Diese Vielseitigkeit macht sich auch in unzähligen Projekten und Programm-Bibliotheken bemerkbar, welche rund um Apache Spark entwickelt werden. Es existieren sogenannte *Spark-Connectoren*, welche die Verbindung zu anderen Komponenten herstellen. Damit können diverse Datenspeicher als Datenquelle verwendet werden. Beispielsweise können Daten aus dem HDFS geladen werden. Oder die Daten werden aus anderen Datenspeichern, wie HBase, Cassandra, Neo4j oder Elasticsearch gelesen.

Abbildung 3.4 zeigt die Ausführung einer Spark-Applikation mit YARN. Es wird der physikalische Kontext innerhalb eines Hadoop-Clusters dargestellt. Dieser Aufbau beschreibt im Rahmen der Thesis den primären Anwendungsfall zur Datenverarbeitung.

Apache Spark kann auch vollständig unabhängig von dem Hadoop-Framework, in einem eigenen Spark-Cluster, ausgeführt werden und bietet dafür einen eigenen Ressourcenmanager.

Allerdings wird innerhalb des Hadoop-Umfelds die Spark-Ausführung mit dem bereits erwähnten Ressourcenmanager YARN durchgeführt (siehe Kapitel 3.3). Dies hat den Vorteil, dass YARN die Ressourcen auf den einzelnen Knoten besser verwalten kann. Wenn der Spark-Ressourcenmanager parallel zu YARN auf den gleichen Knoten genutzt wird, so kann dies zu Ressourcen-Engpässen führen. Denn die Ressourcenmanager würden nicht miteinander kommunizieren und die Last der ausgeführten Anwendungen im Cluster könnte nicht gleichmäßig verteilt werden. Aus diesem Grund ist es ratsam, YARN auch die Ausführung von Spark-Anwendungen im Cluster zu überlassen.

⁸In diesem Kontext ist die simple Ausführung einer Anwendung auf eine bereits existierende Datenmenge gemeint, welche am Ende ein definiertes Ergebnis liefert.

⁹Bei der Datenverarbeitung von Streaming-Data wächst die zu verarbeitende Datenmenge dynamisch an, während die ausgeführte Anwendung die neu hinzugekommenen Daten verarbeitet. Ein Beispiel hierzu ist das Filtern von Tweets auf Twitter, wobei auch neu hinzukommende Tweets bearbeitet werden und nicht nur die Tweets, welche beim Startzeitpunkt der Anwendung bereits existieren.

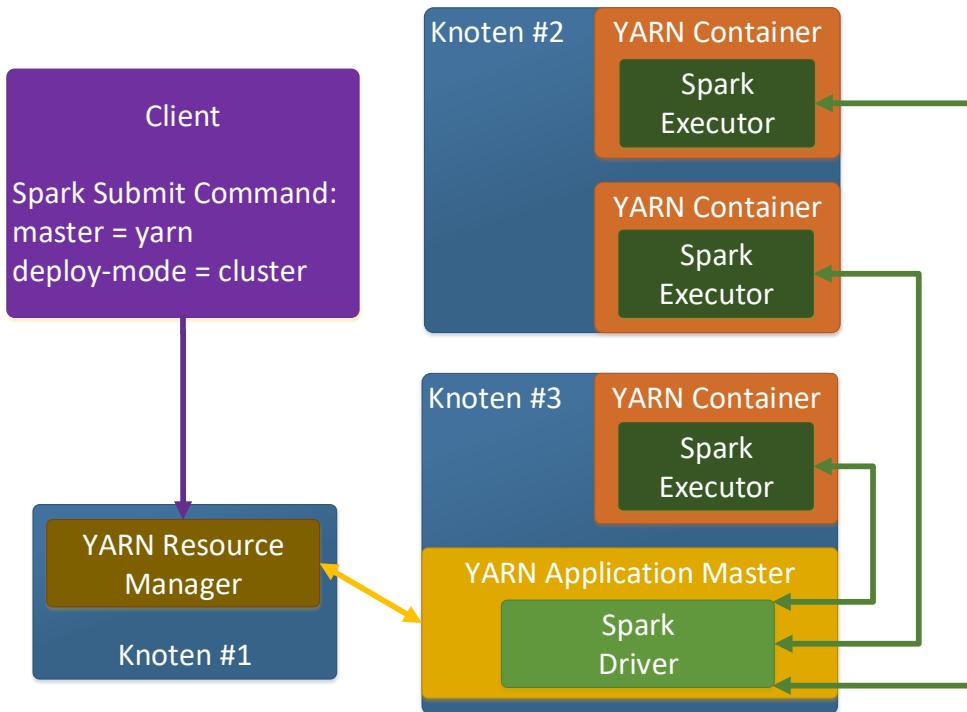


Abbildung 3.4: Spark Datenverarbeitung im Cluster

Wie in Abbildung 3.4 ersichtlich, wird die Ausführung einer Spark-Anwendung über den YARN-Ressourcenmanager gestartet. Es gibt hierbei unterschiedliche Varianten, wie eine Spark-Anwendung ausgeführt werden kann. Im konkreten Fall wird das *Spark-Submit*-Kommando genutzt. Letztlich handelt es sich dabei um einen Konsolenbefehl, welcher die eigentliche Anwendung¹⁰ entgegen nimmt und über diverse Parameter konfiguriert werden kann. Damit YARN die Ressourcen der Applikation verwaltet, müssen die Parameter *Master* und *Deploy Mode* entsprechend angepasst werden. Wie in Abbildung 3.3 (siehe Kapitel 3.3) bereits beschrieben, wird bei YARN ein Application Master erstellt, welcher wiederum diverse Ausführungscontainer auf den einzelnen Knoten anfordert und diese überwacht. Bei der Ausführung einer Spark-Anwendung werden diese Komponenten wiederverwendet und kapseln letztlich die fachlichen Komponenten von Spark.

So gibt es bei Spark einen sogenannten *Driver*, welcher im YARN Application Master läuft und die sogenannten *Executor* aussteuert. Diese werden in einzelnen YARN Containern auf den Knoten ausgeführt. Ein Spark Executor entspricht, aus Sicht des Betriebssystems eines Knotens, der Ausführung einer Java Virtual Machine (JVM) in einem eigenständigen Prozess. Aufgrund der Kapselung durch YARN, können die einzelnen JVM-Prozesse überwacht und zur Not auch beendet werden, falls sie zu viel Ressourcen auf den Knoten anfordern.

Spark und YARN müssen entsprechend konfiguriert sein, damit die Anwendungen korrekt im Cluster skaliert werden. Analog zur YARN wird bei Spark die Anzahl der genutzten

¹⁰Bei einer Spark-Anwendung, welche in Java geschrieben wurde, besteht die Applikation aus einem herkömmlichen *Java Archiv* im *JAR*-Dateiformat.

CPU-Cores und die Größe des genutzten Arbeitsspeichers konfiguriert.

Wenn YARN einzelne Application-Container stoppt, weil sie zu viel Arbeitsspeicher benötigen, dann deutet dies meistens auf eine falsche Konfiguration oder falsche Programmierung der Spark-Anwendungen hin. Um das Problem zu lösen, wird oftmals der nutzbare Arbeitsspeicher pro Executor höher konfiguriert. Dies ist in den meisten Fällen jedoch der falsche Ansatz, da hierdurch kritische Probleme in der Programmlogik der Anwendung nur kaschiert werden.

Daher ist es sinnvoll, bei der Anwendungsentwicklung relativ kleine Cluster mit geringen Ressourcen zu nutzen, denn auch dort müssen die Anwendungen fehlerfrei ausführbar sein. Lediglich die Ausführungsgeschwindigkeit sollte sich in kleinen Clustern verlangsamen. Aus diesem Grund werden im Rahmen der Thesis die Spark-Anwendungen auch auf einem einzelnen Knoten getestet, um Programmfehler besser und früher erkennen zu können. Einzelheiten zu den Programmierparadigmen und den grundlegenden Datenstrukturen, sind in Kapitel 5 beschrieben.

3.5 Apache HBase

*Apache HBase*¹¹ ist eine spaltenorientierte *NoSQL*-Datenbank. Sie entstand auf den Grundlagen der *BigTable*-Datenbank von Google und wurde für das Speichern von Daten im Hadoop-Umfeld entwickelt.¹¹

Der Begriff *NoSQL*-Datenbank steht hierbei für *Not only SQL* und beschreibt letztlich Datenbanken, welche Daten vorwiegend nicht in herkömmlichen relationalen Datenbankschemata speichern. Größtenteils sind diese Datenbanken schemafrei und können horizontal skaliert werden. Diese Bedingungen sind optimal zur Speicherung großer unstrukturierter Datenmengen.

Anhand des sogenannten *CAP-Theorems* können diese Datenbanken kategorisiert werden. Das CAP-Theorem besteht aus den Eigenschaften Konsistenz, Verfügbarkeit und Partitionstoleranz und besagt, dass maximal zwei dieser drei Eigenschaften von einer Datenbank garantiert werden können. Konsistenz beschreibt hier die Garantie, dass alle Knoten im verteilten System den gleichen Datenstand haben. Die Verfügbarkeit bezieht sich auf die dauerhafte Erreichbarkeit der Daten. Wohingegen die Partitionstoleranz die Funktionsfähigkeit bei einem Ausfall einzelner Knoten im Datenbank-Verbundsystem garantiert. Apache HBase garantiert die Eigenschaften der Partitionstoleranz und der Konsistenz. Dies führt dazu, dass die Verfügbarkeit der Daten weniger stark ausgeprägt ist. [5, S. 189 ff.]

Während bei klassischen relationalen Datenbanken die Daten zeilenweise in Tabellen strukturiert werden, wird in spaltenorientierten Datenbanken hingegen eine andere Struktur genutzt. Die Daten werden in einzelnen Spalten gruppiert und in sogenannten *Column Families* abgespeichert. Der Vorteil dieser Speicherart hängt stark von deren fachlichen Nutzung ab. Wenn alle Daten einer Spalte abgefragt werden, dann können diese Daten effizient gelesen werden, da sie zusammen persistiert wurden.

Apache HBase basiert auf dieser Spaltenorientierung. Die Datenbank wird im Rahmen der Thesis für das Speichern beliebiger Dateiinhalte und Dateimetadaten verwendet. Ein vereinfachtes Beispiel einer möglichen Datenstruktur wird in Abbildung 3.5 dargestellt.

Anhand der Abbildung werden einige Eigenschaften von HBase sichtbar. So existieren zwei *Column Families* mit den Namen *metadata* und *content*. Die Column Family *metadata* ent-

¹¹Der Name *HBase* basiert auf der Kombination von *Hadoop* und *Database*.

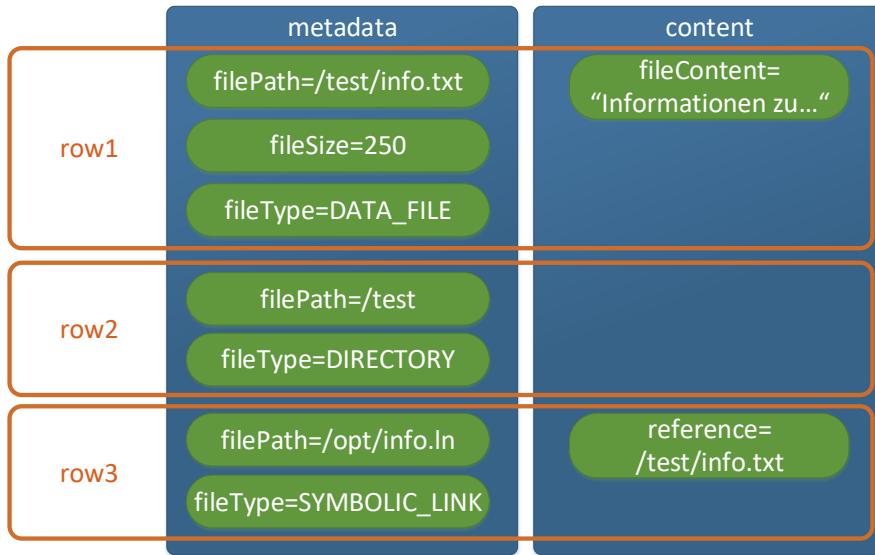


Abbildung 3.5: Schema-Beispiel einer HBase Tabelle (Vgl. [5])

hält wiederum die Spalten *filePath*, *fileSize* und *fileType*. Alle Werte werden als Binär-Inhalt gespeichert. Eine Zeile hat einen eindeutigen Spaltenschlüssel, wie zum Beispiel *row1*. Über diesen Schlüssel können die spezifischen Inhalte der einzelnen Spalten für eine bestimmte Zeile erfragt werden. Interessant hierbei ist, dass die Spaltenwerte optional sind und nicht für jede Zeile existieren müssen. So hat eine Datendatei einen konkreten Inhalt, welcher in der Spalte *fileContent* der Spaltenfamilie *content* gespeichert wird. Wohingegen ein Verzeichnis keinen Dateinhalt hält. Daher ist in der zweiten Zeile auch kein Inhalt in der Spalte *fileContent* abgelegt. In der dritten Zeile wird ein symbolischer Link gespeichert. Dieser hat auch keinen Inhalt in der Spalte *fileContent*. Dafür wird aber die Referenz auf die Originaldatei in einer weiteren Spalte gespeichert. Aufgrund der Gruppierung und Speicherung in Column Families, benötigen leere Spaltenwerte auch keinen Speicherplatz.

Eine einzelne Zelle beschreibt letztlich den Wert einer Spalte für eine konkrete Zeile. Hierbei wird zu jeder Zelle auch ein Zeitstempel gespeichert. Durch die Zeitstempel können ältere Werte einer Zelle ausgelesen werden. So wird bei einer Modifikation einer konkreten Zelle der Wert zusammen mit einem neuen Zeitstempel geschrieben.

Die einzelnen Spalten innerhalb einer Spaltenfamilie müssen nicht bei der Erstellung einer Tabelle bekannt sein. Lediglich die Spaltenfamilien müssen initial angegeben werden und können später auch nicht mehr geändert werden. Dadurch ist eine nachträgliche Erweiterung der Tabelle, um zusätzliche Spalten, problemlos möglich.[11, S. 577]

Die Skalierbarkeit und die Partitionstoleranz wurden bei der Entwicklung von HBase berücksichtigt. Es baut auf dem Hadoop HDFS auf und speichert darin die Daten. Analog zu HDFS, YARN und Spark existiert eine Master-Slave Architektur über alle Knoten hinweg. Abbildung 3.6 zeigt die physikalische Aufteilung.

Auf den einzelnen Knoten im Computer-Cluster existieren sogenannte *Region Server*. Diese Region Server speichern jeweils unterschiedliche Teile der angelegten HBase-Tabellen.

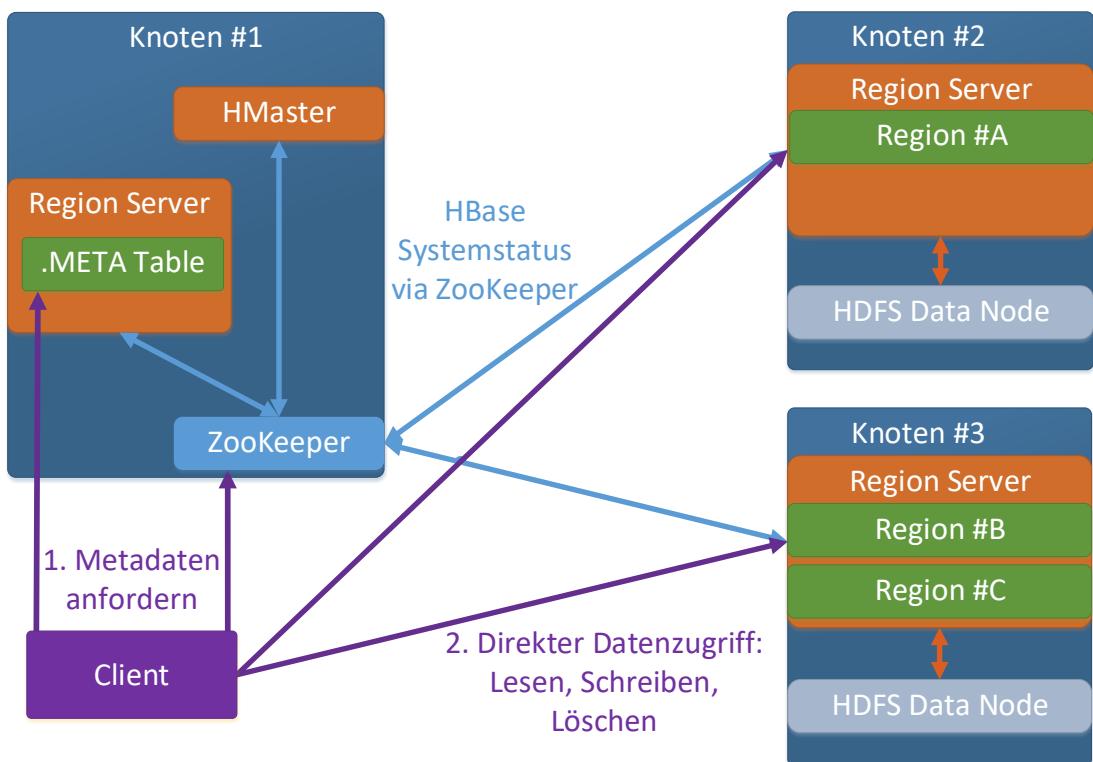


Abbildung 3.6: HBase Datenspeicherung im Cluster

Eine Tabelle wird hierbei anhand der Zeilenschlüssel in mehrere Bereiche, den sogenannten *Regions*, unterteilt. Beispielsweise könnte die Region A die Daten einer Tabelle der Zeilen 1 bis 3.000 enthalten (siehe Abbildung 3.6). Die Region B wiederum enthält die Daten von den Zeilen 3.001 bis 8.540 der gleichen Tabelle. Und die Region C könnte die Daten der Zeilen 1 bis 22.300 von einer anderen Tabelle enthalten. Somit kann ein Region Server mehrere Regions von gleichen oder auch unterschiedlichen Tabellen verwalten. Das Prinzip der Datenlokalität greift auch bei HBase. So sollte auf jedem Knoten, auf dem ein Region Server läuft, auch ein HDFS Data Node existieren. Dieser speichert die Daten der einzelnen Regions als Dateien im HDFS.

Wenn neue Tabellen erstellt werden, oder einzelne Regions zu groß werden, dann koordiniert eine übergeordnete Instanz die Umverteilung von Daten und die Erstellung neuer Regions. Diese Instanz ist bei HBase der sogenannte *HMaster*. Es ist ein unabhängiger Prozess, welcher auf einem beliebigen Knoten im Cluster läuft und über Apache ZooKeeper den Status der Region Server überwacht.¹² Um die Ausfallsicherheit zu gewährleisten, ist der Prozess redundant ausgelegt.¹³ Darüber hinaus kümmert sich der HMaster-Prozess auch um die Restrukturierung bei Teilausfällen einzelner Region Server. Wenn nun ein Client auf die Daten einer Tabelle zugreifen möchte, muss dieser wissen, auf welchem Knoten die Daten abgelegt sind. Hierfür verbindet sich der Client zuerst mit ZooKeeper und erfährt darüber, welcher Region Server die sogenannte *Meta-Tabelle* speichert.[11, S. 579]

¹²Die Funktionsweise von Apache ZooKeeper wird in Kapitel 3.6 näher erläutert.

¹³Über ZooKeeper kann der primäre HMaster-Prozess ermittelt werden. Ist der aktive HMaster nicht mehr erreichbar, schaltet sich ein Backup-HMaster ein.

Diese Meta-Tabelle enthält Informationen über alle HBase-Tabellen und der Region Server, welche die Regions bereitstellen. Anhand der Metadaten kann der Client die benötigten Daten direkt von den zuständigen Region Servern anfordern. Dieses Vorgehen ist für den sporadischen Zugriff auf einzelne Datensätze nicht wirklich effizient. Es skaliert aber sehr gut bei großen Datenmengen, da kein Flaschenhals vorhanden ist. Üblicherweise speichert der Client die angeforderte Meta-Tabelle temporär ab, so dass er bei nachfolgenden Anfragen direkt auf die entsprechenden Region Server zugreifen kann.

Im Rahmen der Thesis wird HBase verwendet, um Metadaten zu speichern. Diese werden wiederum mit Apache Spark ausgelesen und verarbeitet. Hierbei kann das Prinzip der Datenlokalität sehr gut genutzt werden.

In der Theorie ist es durchaus möglich, die HDFS Data Nodes, die Spark Worker und die HBase Region Server getrennt auf unterschiedlichen Knoten auszuführen. Dies ist aber nicht sinnvoll, da dadurch die Daten über das Netzwerk transportiert werden und die Verarbeitungsgeschwindigkeit verringert wird.

Sinnvoller ist es, die HDFS Data Nodes auf den Knoten auszuführen, wo auch die Region Server ausgeführt werden. Darauf aufbauend sollten auch die Spark Worker auf den Knoten gestartet werden, auf welchen die Region Server laufen. Dadurch können die Daten, welche von Apache Spark benötigt werden, direkt von dem lokalen HBase Region Server bereitgestellt werden. Dieser erhält die Daten wiederum von dem lokalen Data Node. Somit können die Daten direkt auf dem Knoten verarbeitet werden, wo sie auch gespeichert sind und müssen nicht über das Netzwerk an andere Knoten gesendet werden.¹⁴ Die Koordinierung dieser Komponenten ist allerdings entsprechend komplex. Schon bei der Entwicklung von Anwendungen, können einzelne Fehler beim Datenzugriff dieses Prinzip der Datenlokalität aushebeln. Daher müssen die Anwendungen genau untersucht werden, ob sie das Prinzip der Datenlokalität korrekt umsetzen.

3.6 Apache ZooKeeper

Innerhalb eines Computer-Clusters zur verteilten Datenverarbeitung existiert oftmals das Problem, dass sich die einzelnen Komponenten koordinieren müssen. Beispielsweise teilt HBase die Daten auf mehrere Region Server auf, welche wiederum auf den einzelnen Knoten ausgeführt werden. Doch welche Instanz koordiniert diese Aufteilung? Ein anderes Problem ist der Datenzugriff. Ein Client möchte eine Zeile einer bestimmten Tabelle auslesen. Woher weiß der Client, welchen konkreten Knoten er anfragen muss, um genau diese Zeile zu erhalten?

In den meisten Fällen existiert hierzu eine bestimmte Instanz, welche die Koordinierung der Knoten übernimmt. Bei HBase gibt es den HMaster-Prozess, der für diese Aufgaben verantwortlich ist. Das Problem dabei ist, dass auch der Knoten auf dem diese Master-Instanz läuft, ausfallen kann und das komplette System zum erliegen bringt. Diese Verwaltungsinstanzen im Allgemeinen, sind kritische Komponenten und können als Single-Point-of-Failure zu einem Stillstand des kompletten Systems führen. Um solche Totalausfälle zu vermeiden, müssen bestimmte Automatismen definiert werden, wie sich die Knoten selbst organisieren können, um einen Ausfall beliebiger Knoten zu überstehen.

¹⁴Siehe auch Kapitel 3.3 und Kapitel 3.4.

An dieser Stelle bietet *Apache ZooKeeperTM* Mechanismen an, wie sich die einzelnen Knoten in einem verteilten System organisieren und Informationen verteilt synchronisieren können. Aus logischer Sicht stellt ZooKeeper einen Service zu Verfügung. Dieser Service ermöglicht das Speichern von Informationen in einem strukturierten Verzeichnis mit einzelnen Dateien. Bei den Informationen handelt sich normalerweise um wichtige Konfigurationen, welche im Cluster verteilt werden müssen und zentral über ZooKeeper aktualisiert werden können. Jeder Client, der sich mit ZooKeeper innerhalb des Computer-Clusters verbindet, sieht die gleiche Konfiguration und kann bei Bedarf auch bestimmte Konfigurationen ändern.[14, S. 4-5]

Aus Sicht des Entwicklers, stellt dieser Service die aktuellen Informationen im Cluster zur Verfügung. Wie der Service dies bewerkstellt, ist ein Implementierungsdetail. Neben dem bereits erwähnten Konfigurationsmanagement, bietet ZooKeeper einen Naming-Service an oder ermöglicht es auch den Live-Status einzelner Knoten zu überwachen.[6]

Wie bei HBase in Kapitel 3.5 bereits erwähnt wird, kann sich ein Client mit ZooKeeper verbinden und erhält darüber den aktuellen Knoten, auf welchem der HMaster-Prozess läuft. Darüber kann er die Metadaten zu allen Tabellen abfragen. Ein anderes Beispiel zeigt die Backup-Instanz des HMaster-Prozesses. Dieser prüft über ZooKeeper den Status des primären HMaster-Prozesses und wird informiert, wenn letzterer nicht mehr verfügbar ist. Daraufhin propagiert sich die Backup-Instanz als neuen HMaster-Prozess im Cluster, um so die Funktionsfähigkeit von HBase aufrecht zu erhalten. Abbildung 3.7 zeigt die Verzeichnisstruktur, welche stark an ein Verzeichnis eines Dateisystems erinnert. Die einzelnen Einträge werden *ZNodes* genannt.¹⁵

```
[zk: localhost:2181(CONNECTED) 5] ls /hbase
[replication, meta-region-server, rs, splitWAL, backup-masters, table-lock,
 flush-table-proc, region-in-transition, online-snapshot, master, running,
 recovering-regions, draining, namespace, hbaseid, table]
```

Abbildung 3.7: Gespeicherte Informationen von HBase in ZooKeeper

Normalerweise ist ZooKeeper auf mehreren Knoten im Cluster installiert. Sie bilden ein sogenanntes *ZooKeeper Ensemble* und bestehen zumeist aus 3 oder 5 Einzelinstalltionen auf beliebigen Knoten. Ein ZooKeeper Ensemble, welches für die gleiche Anwendungsdomäne zuständig ist, wird auch *Quorum* genannt. Innerhalb eines Quorums gibt es einen Leader und mehrere Follower, die sich die gleichen Konfigurationsinformationen teilen. Fällt der Leader aus, können die Follower selbstständig einen neuen Leader bestimmen.[6]

3.7 Apache Solr und Lucene

Apache SolrTM ist eine skalierbare und performante Plattform zur Volltextsuche. Die Daten werden vorher indexiert und können effizient durchsucht werden.[9] Mithilfe von Apache Solr werden zum Beispiel Volltextsuchen für Dokumente oder Produktsuchen für Webshops implementiert.

Im Allgemeinen ist ein Suchsystem in mehrere Analyseschritte aufgeteilt. Ein Großteil dieser Verarbeitungsschritte wird nicht von Solr selbst übernommen. Vielmehr baut Solr auf

¹⁵Siehe Link <http://zookeeper.apache.org/doc/r3.5.4-beta/zookeeperOver.html>. Letzter Zugriff: 26.7.2018.

dem Open-Source Projekt *Apache LuceneTM* auf und erweitert letzteres um eine skalierbare Infrastruktur und diverse Schnittstellen zur Verarbeitung der Daten.

Zu Beginn liegen beliebige Daten in Form von Dateien oder Dokumenten vor. Diese Daten durchlaufen eine textuelle Aufbereitung, bevor sie indexiert werden können.

Bei der Textanalyse wird der relevante Text aus den Daten extrahiert. Hierbei hängt die Extraktion der Daten auch davon ab, ob die Daten strukturiert, semistrukturiert oder unstrukturiert sind. Anhand der Dateiformate können diverse Bibliotheken genutzt werden, um Daten zu extrahieren. Beispielsweise kann mithilfe von *Apache PDFBox^{®16}* Text aus PDF-Dokumenten extrahiert werden. Mithilfe der *Geospatial Data Abstraction Library (GDAL)¹⁷* können Geopositionen aus den EXIF-Metadaten von JPEG-Bildern extrahiert werden. Mithilfe von *Tesseract OCR¹⁸* kann lesbarer Text direkt aus Bildern extrahiert werden.[9, S. 39]

Im nächsten Schritt wird der extrahierte Text aufbereitet. Die Aufbereitung hängt stark von dem spezifischen Anwendungsfall und den Daten ab. Im Allgemeinen werden Satzzeichen und überflüssige Füllwörter entfernt und Großbuchstaben werden in Kleinbuchstaben umgewandelt. Darüber hinaus kann auch eine Stammformreduktion durchgeführt werden. Darauf aufbauend kann der Text detaillierter analysiert werden. Beispielsweise könnten Redewendungen erkannt oder Synonyme einzelner Wörter identifiziert werden.[9, S.44]

Nach der Aufbereitung des Textes, erfolgt die Erstellung eines sogenannten *Inverted Indexes*. Ein Inverted Index ist ähnlich aufgebaut wie ein Stichwortverzeichnis. Jedes Wort wird darin mit den Verweisen zu den Vorkommen in den einzelnen Dokumenten versehen. Auf Basis dieses Indexes können sehr schnell alle Dokumente gefunden werden, welche das gesuchte Wort enthalten.[9, S. 47]

Auf die erstellten Indizes können nun Suchanfragen durchgeführt werden. Aber auch hier gibt es unterschiedliche Modelle, wie die relevanten Dokumente ermittelt werden und in welcher Reihenfolge die Ergebnismenge zurückgeliefert wird.

Es gibt das sogenannte *Boolean Model* auf Basis der booleschen Algebra. Beispielsweise könnte eine forensische Suchanfrage lauten: Suche alle Bilder oder Videos, welche das Wort *Unfall* im Dateinamen haben, aber nicht kleiner als 1 MB groß sind. Diese Suchanfrage wird in einen booleschen Ausdruck überführt und die Dateien werden zurückgeliefert. Allerdings liefert dieses Modell keine Aussage zur Reihenfolge der Ergebnismenge.

Hierzu gibt es komplexere Suchmodelle, wie das sogenannte *Vector Space Model*. Es basiert auf gewichteten Faktoren und ermöglicht es, für jedes Dokument der Ergebnismenge die Trefferwahrscheinlichkeit zu ermitteln. Nach dieser Bewertung wird die Reihenfolge der Ergebnisse festgelegt. Beispielsweise sollte ein Dokument eine höhere Bewertung erhalten, wenn das gesuchte Wort mehrfach im Dokument vorhanden ist.[9, S. 47 ff.]

Solr besitzt einen *Cloud-Mode*, der es erlaubt, die indexierten Daten verteilt auf mehreren Knoten zu speichern. Dieser Cloud-Mode ist für eine Integration in das Hadoop-Ökosystem optimal.¹⁹ Abbildung 3.8 skizziert diese Verteilung im Computer-Cluster.

¹⁶Siehe Link: <https://pdfbox.apache.org/>. Letzter Zugriff: 01.08.2018.

¹⁷Siehe Link: <https://www.gdal.org/>. Letzter Zugriff: 01.08.2018.

¹⁸Siehe Link: <https://github.com/tesseract-ocr/tesseract>. Letzter Zugriff: 01.08.2018.

¹⁹Der Cloud-Mode kann aber auch ohne Apache Hadoop auf einem beliebigen Cluster genutzt werden.

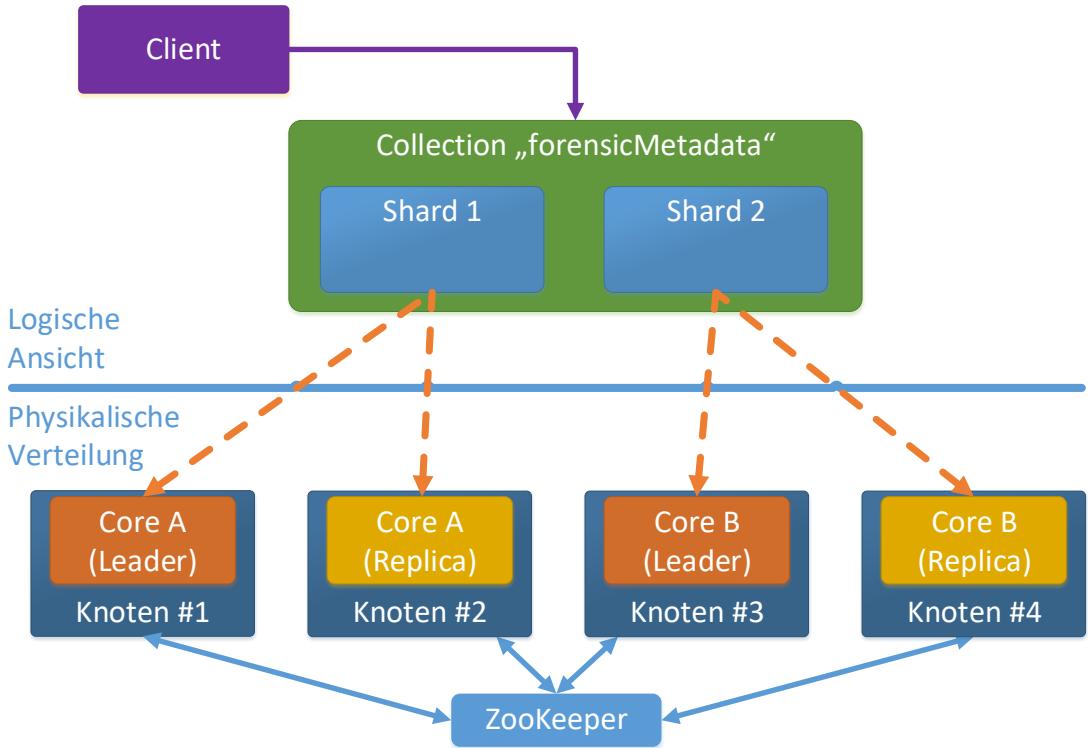


Abbildung 3.8: Solr Cloud-Mode im Cluster

Dieser Cloud-Mode wird auch bei der Integration in die Analyseplattform genutzt.²⁰ Solr kann als zusätzliches Software-Paket in das Hadoop-Ökosystem integriert werden.²¹ Es können beliebige Daten in der Solr-Cloud indexiert werden. Darüber hinaus nutzt Solr im Cloud-Mode das bereits beschriebene ZooKeeper-Projekt²² zur Koordinierung und Überwachung der einzelnen Knoten.

Innerhalb des Cloud-Modes werden die oben beschriebenen Indizes (Inverted Index) in mehrere sogenannte *Shards* aufgeteilt. Ein einzelner Shard ist ein Teil des Indexes, welcher unabhängig von den anderen Shards durchsucht werden kann. So werden bei einer Suchanfrage alle Shards parallel durchsucht. Einzelne Shards können wiederum auf anderen Knoten repliziert werden, um die Ausfallsicherheit zu gewährleisten. Solr spricht hierbei von Cores. Ein Core ist die physikalische Repräsentation eines logischen Shards auf einem konkreten Knoten. Alle logischen Shards bilden zusammen den Index, welcher bei Solr als sogenannte *Collection* dargestellt wird.[3]

Jedes Dokument, das in einer Collection indexiert werden soll, wird einem der logischen Shards zugewiesen. Hierbei wird zuerst anhand eines eindeutigen Dokumentenschlüssels entschieden, in welchen Shard das Dokument aufgenommen werden soll.²³ Ein logischer Shard wird abermals aufgeteilt in mehrere Replicas, den bereits erwähnten Cores auf den einzeln

²⁰Siehe Kapitel 5.3.4.

²¹Die Hortonworks Dataplatform bietet ein passendes Software-Paket zur Installation von Solr an. Primär wird dieses Paket genutzt, um eine performante Suche im HDFS-Dateisystem zu ermöglichen. Die Solr-Installation kann aber auch für andere Zwecke genutzt werden.

²²Siehe Kapitel 3.6.

²³Der Dokumentenschlüssel kann zum Beispiel von der Hashsumme der Datei abgeleitet werden.

Knoten. Für jeden logischen Shard wird ein *Leader*-Knoten bestimmt.²⁴ Der Leader speichert einen physikalischen Core des logischen Shards und indexiert eingehende Dokumente. Sobald der Index für diesen Shard neu aufgebaut wurde, wird die Aktualisierung an die Knoten weitergesendet, die eine Replica (Core) des gleichen logischen Shards speichern.[21, S. 867-872]

Apache Solr und Lucene sind beide in Java implementiert. Daher gibt es einen Java Client, zur Durchführung von Suchanfragen. Andererseits existiert auch ein REST-Endpunkt, der für Anfragen genutzt werden kann. Damit können Anfragen simpel und schnell in beliebige Websites integriert werden oder direkt mit dem Kommandozeilentool *curl* durchgeführt werden. Hierbei können die Anfragen in XML (Extensible Markup Language) oder JSON (JavaScript Object Notation) formatiert sein. Ein simples Beispiel zeigt nachfolgende Anfrage (siehe Abbildung 3.9).

```
> curl "http://localhost:8983/solr/forensicMetadata/query?q=*shot*"
{
  "responseHeader": {
    "status": 0,
    "QTime": 20,
    "params": {
      "q": "*shot*"
    }
  },
  "response": {
    "numFound": 1,
    "start": 0,
    "maxScore": 1.0,
    "docs": [
      {
        "filePath": ["Screenshot from 2018-05-13 05-55-23.png"],
        "fileType": ["DATA_FILE"],
        "fileSize": [360377],
        "owner": ["johannes"],
        "group": ["johannes"],
        "permissions": ["[OWNER_READ, GROUP_WRITE, OWNER_WRITE, OTHERS_READ, GROUP_READ]"],
        "lastModified": ["2018-05-13T03:55:31.613Z"],
        "lastAccessed": ["2018-05-13T03:55:31.613Z"],
        "created": ["2018-05-13T03:55:31.613Z"],
        "mediaType": ["image/png"],
        "fileHash": ["c894fcc169d7971bfc4fc6fee973a852333db485fcf1ac772fd2e573f9701fa7baa9c7180d0c1ad402efd89ae1aed4e873e1d4d02b024b4cffae415dacc25fcf"]
      },
      {
        "id": "row4",
        "_version_": 1607729961236430848
      }
    ]
  }
}
```

Abbildung 3.9: Solr-Suchanfrage via *curl*

In dem Beispiel ist die Solr-Instanz unter <http://localhost:8983> erreichbar. Die Suchanfrage wird auf der Collection *forensicMetadata* ausgeführt. Es soll in allen Feldern nach einem Vorkommen von dem Wort *shot* (*q=*shot**) gesucht werden. Die Antwort ist im JSON-Format definiert. Unter anderem wird die Anzahl der Treffer (*numFound:1*) mitgeliefert. Bei dieser konkreten Anfrage, wurde ein Bild mit dem Dateinamen *Screenshot...* gefunden.

²⁴Diese Leader werden mittels ZooKeeper im Cluster propagiert.

4 Datenspeicherung

4.1 Allgemeiner forensischer Analyseprozess

Im Praxisteil dieser Arbeit soll eine Analyseplattform auf Basis von Apache Hadoop aufgebaut werden. Diese Analyseplattform dient zur Auswertung sichergestellter Asservate und dem Auffinden von Beweisen in großen Datenmengen. Hierbei behandelt die Plattform nur einen Teil der Arbeitsvorgänge, die während einer forensischen Analyse anfallen.

Abbildung 4.1 skizziert einen allgemeinen forensischen Analyseprozess für digitale Beweismittel.[16, S.16] Die grün hinterlegten Schritte definieren den Arbeitsbereich, bei welchen die hier entwickelte forensische Analyseplattform den Forensiker unterstützen kann.

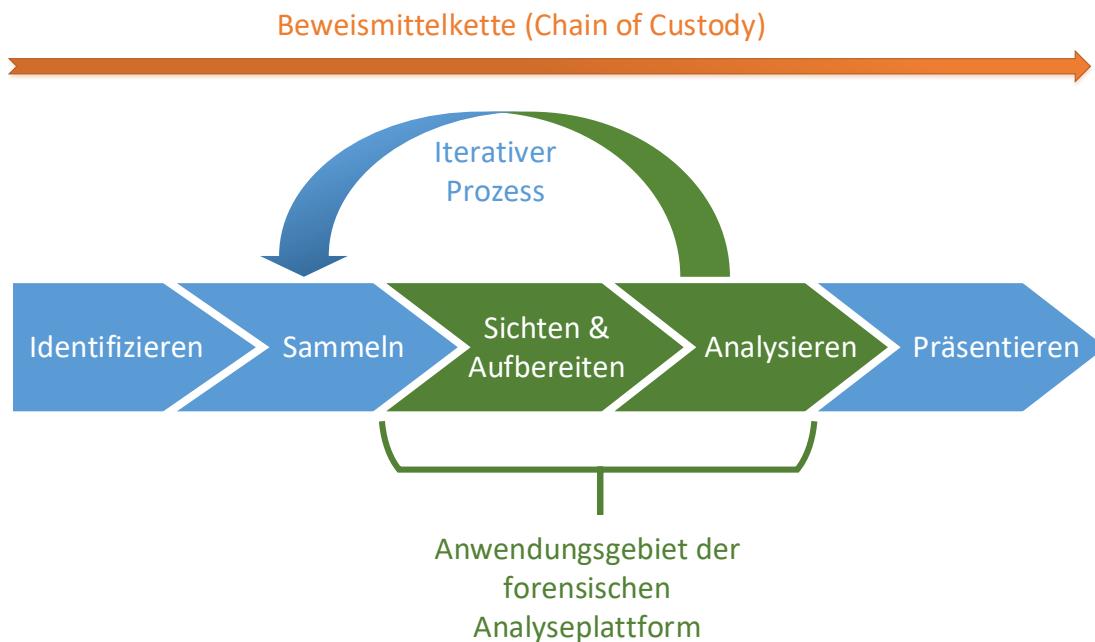


Abbildung 4.1: Forensischer Analyseprozess für digitale Beweismittel (Vgl. [16, S.16])

Zu Beginn existiert ein Vorfall oder ein Tatverdacht für eine Straftat. In einem nachfolgenden Schritt ermittelt beispielsweise die Staatsanwaltschaft. Während dem Ermittlungs-

verlauf wird der Tatort analysiert und es wird bei Tatverdächtigen nach Hinweisen für die Tat und gegebenenfalls deren Tathergang gesucht. Dieser Schritt beschreibt die Identifikationsphase aus Abbildung 4.1. Hierbei geht es um die Identifikation von potentiellen Beweismitteln, welche sichergestellt oder beschlagnahmt werden sollen.[16, S. 17-24]

In der Forensik wird häufig hypothesenbasiert vorgegangen. So entwickelt der Ermittler eine Hypothese, wie eine mögliche Straftat begangen wurde und wer diese begangen haben könnte. Darauf aufbauend überlegt er sich, welche Spuren für oder gegen diese Hypothese sprechen und welche möglichen Beweismittel diese Spuren enthalten könnten (z.B. Kommunikationsdaten auf dem PC oder Bildmaterial auf einem Mobiltelefon).

Im zweiten Schritt aus Abbildung 4.1 geht es um das Vereinnahmen von potentiellen Beweismitteln. Hierbei werden identifizierte Datenträger und Geräte sichergestellt oder beschlagnahmt. In dieser Phase werden beispielsweise auch schon forensisch korrekte Datenträgerabbilder erstellt, auf welchen dann später eine Datenanalyse ausgeführt werden kann.[16, S. 24-33] In vielen Fällen, beispielsweise bei Unternehmensservern, werden nicht die Geräte selbst sichergestellt, sondern nur wichtige Teile der Daten forensisch korrekt kopiert. Auch hier findet teilweise schon eine Vorselektion statt, welche Daten benötigt werden und welche Daten für den konkreten Fall irrelevant sind.

Die dritte Phase aus Abbildung 4.1 behandelt das Sichten und Aufbereiten der sichergestellten Daten. Gerade bei großen unstrukturierten Datenmengen erfolgt in dieser Phase auch eine Vorselektion, um die Datenmenge nochmals einzuschränken. Dies kann automatisiert oder auch manuell erfolgen.[16, S. 33-39]

An dieser Stelle beginnt das Anwendungsgebiet der hier entwickelten forensische Analyseplattform. So können alle gesammelten Daten in die forensische Analyseplattform importiert und prozessiert werden. Darauf kann über eine allgemeine Suche nach spezifischen Stichworten, Hashsummen oder Zeitpunkten gesucht werden. Dies soll dem Ermittler das Auffinden von fallrelevanten Daten erleichtern. Die meisten bekannten forensischen Analysetools bieten ebenfalls eine Stichwortsuche an, weil damit große Datenmengen schnell nach bestimmten Kriterien gefiltert werden können.[2, S. 116-123]

In dieser Phase werden aber auch gelöschte, verschlüsselte oder verschleierte Daten wiederhergestellt oder entschlüsselt, sofern dies möglich ist. Eine klassische Methode ist beispielsweise das sogenannte *File Carving* auf Datenträgern.¹[16, S. 38-39]

Diese Art von Datenaufbereitung beherrscht die hier entwickelte forensische Analyseplattform derzeit noch nicht.²

Auch in der anschließenden Analysephase kann die hier entwickelte forensische Analyseplattform genutzt werden (siehe Abbildung 4.1). In dieser Phase werden die aufbereiteten Daten detailliert analysiert, um Informationen zu erhalten, die für oder gegen einen bestimmten Tathergang sprechen.[16, S. 39-45] Anhand dieser Informationen werden die eingangs beschriebenen Hypothesen, zu möglichen Tathergängen, verifiziert. Bei einer Analyse werden aus den Daten komplexe Zusammenhänge und Beziehungen erarbeitet. Beispielsweise werden aus den Rohdaten Kommunikationsverläufe auf Basis von E-Mails oder

¹Beim File Carving wird versucht, logisch zusammenhängende Daten allein anhand des Dateiinhalts zu rekonstruieren, ohne die Dateisystemmetadaten zu nutzen. Die Methode wird gerne angewendet, wenn das Dateisystem nicht wiederherstellbar ist oder wenn gelöschte Dateien auf bereits freigegebenen Speicherbereichen gesucht werden.

²Es wäre aber durchaus möglich diverse Methoden der Datenaufbereitung zu implementieren. Siehe auch Kapitel 9.

zeitliche Abläufe basierend auf Zeitstempelanalysen erstellt.[16, S. 33-39]

Auch die Aussagekraft eines potentiellen Beweismittels muss ermittelt werden. So könnte beispielsweise urheberrechtsverletzendes Material auf einem Datenträger eines PCs gefunden werden. Allerdings kann die Aussagekraft dieses potentiellen Beweismittels sehr gering sein, wenn das System bereits durch Schadsoftware kompromittiert wurde.

Einige Analyseschritte können automatisiert werden und sind daher prädestiniert für die hier entwickelte Analyseplattform (siehe auch Kapitel 5).

Bei der Analyse können Verbindungen zu neuen potentiellen Beweismitteln gefunden werden, die dann wieder über den forensischen Analyseprozess vereinnahmt und aufbereitet werden. Daher ist der Prozess iterativ anzusehen. Gerade durch die Nutzung der forensischen Analyseplattform, sollen diese Iterationen verkürzt werden, indem durch die parallelisierte Prozessierung Zeit eingespart wird.

In der letzten Phase des Analyseprozesses müssen die Ermittlungsergebnisse visuell aufbereitet werden, um sie auch vor Gericht präsentieren zu können. Letztlich muss ein Analysebericht erstellt werden, welcher einerseits die Ergebnisse enthält und andererseits nachvollziehbar beschreibt, wie diese Analyseergebnisse zustande gekommen sind.³[16, S. 45-47] Viele Analysetools, unter anderem auch das hier genutzte Referenztool *Autopsy*, ermöglichen die halbautomatische Erstellung von Analyseberichten. Die hier entwickelte Analyseplattform kann dies derzeit noch nicht. Bei einer Weiterentwicklung der Analyseplattform wäre diese Funktionalität aber durchaus brauchbar.

Ein primärer Aspekt bei dem allgemeinen forensischen Analyseprozess aus Abbildung 4.1 ist die Dokumentation der Beweismittelkette. Mit ihr steht und fällt die Aussagekraft der Ergebnisse aus einer forensischen Analyse. Daher muss bei der Dokumentation der Asservate lückenlos festgehalten werden, wie diese aufbereitet und gegen unberechtigten Zugriff oder ungewollte Modifikationen gesichert wurden. Nachfolgende Liste liefert wichtige Kriterien, die im Protokoll zur Beweismittelkette festgehalten werden sollten:

- Die Ermittler, welche das Beweismittel sichergestellt und später analysiert haben.
- Die Prozesse, Datenaufbereitungen und Analysen, welche durchgeführt wurden.
- Die Zeitpunkte der Sicherstellung, Aufbereitung und der Analyse.
- Die Umstände, wie das Beweismittel sichergestellt wurde.
- Gründe, wieso das Beweismittel sichergestellt wurde.
- Transportwege und Lagerstätten des Beweismittels.
- Personen die Zugang zu dem Beweismittel hatten und allgemeine Informationen, wie das Beweismittel vor unbefugtem Zugriff geschützt wird.

Ein sehr wichtiger Punkt bei der Dokumentation der Beweismittelkette ist die Verifikation der Datenintegrität der Asservate während des Analyseprozesses. Dies wird primär durch die Prüfung mittels kryptografischer Hashes erreicht. Letztlich dienen diese zum Schutz vor einer Modifikation des Beweismittels. Das Ändern von Asservaten oder deren Kopien,

³Der Bericht sollte so geschrieben sein, dass andere Parteien oder Ermittler die gleichen Ergebnisse reproduzieren können.

sollte eigentlich immer vermieden werden. In vielen Fällen ist dies jedoch notwendig, um beispielsweise defekte Datenstrukturen wiederherstellen zu können. Bei solchen bewussten Datenänderungen ist eine entsprechende Dokumentation erforderlich.

Bei der Analyse mit der hier entwickelten Analyseplattform muss auch die Beweismittelkette entsprechend dokumentiert werden. Die derzeitige Implementierung der forensischen Analyseplattform behandelt diesen Aspekt noch nicht. Aber auch hier könnte in einer Weiterentwicklung eine Beweismittelkette erstellt werden, welche die einzelnen Verarbeitungsprozesse, Zeitpunkte und Nutzerzugriffe dokumentiert. Da das System gegen unbefugten Zugriff gesichert werden muss, könnten in einer zukünftigen Weiterentwicklung Maßnahmen zur Nutzeridentifikation und Authentifizierung implementiert werden (siehe Kapitel 7.1). Diese Mechanismen protokollieren einzelne Nutzeranmeldungen und Datenzugriffe, welche dann wiederum als Grundlage zur automatischen Erstellung eines Protokolls zur Beweismittelkette dienen können.

4.2 Klassisches Analysevorgehen

Um die fachlichen Anforderungen an das Analyse-System herauszuarbeiten, soll das herkömmliche Analysevorgehen mit einem vergleichbaren Open-Source Analysewerkzeug betrachtet werden.

Die Ausgangslage liefern einige Datenträgerabbilder aus diversen Testszenarien. Diese Datenträgerabbilder sind, bezogen auf den forensischen Analyseprozess aus Abbildung 4.1, die Grundlage für die dritte Phase - dem Sichten und Aufbereiten der Daten.

Bei gängigen Analysevorgehen werden beispielsweise die Datenträgerkopien mit Betriebssystemprogrammen unter Linux oder mithilfe des Open-Source Analysetools *Autopsy*⁴ unter Windows analysiert. Im kommerziellen Bereich existieren etliche weitere Analyse-Tools mit größerem Funktionsumfang. Nachfolgend wird Autopsy als Referenzsystem unter Windows betrachtet, da es eines der bekanntesten Analysewerkzeuge unter den kostenfreien Open-Source Programmen ist.

Die Datenträgerabbilder können in unterschiedlichen Dateiformaten vorliegen. Mithilfe klassischer Open-Source Anwendungen, wie beispielsweise *dd*⁵, können Abbilder im so genannten *RAW*-Format erstellt werden. Von dd existiert eine forensische Variante *dcfldd*, welche beim Kopieren auch Hashsummen zur Verifikation berechnet.[8] Andere Tools, wie der *FTK-Imager*, können auch Datenträgerabbilder in speziellen Container-Formaten erstellen und lesen. Zum Beispiel gibt es das *EnCase Physical*-Format mit der Dateiendung *.E01* oder das *Advanced Forensic Format* mit der Endung *.AFF*.⁶ Diese Formate unterstützen eine bessere Extraktion von Metadaten oder bieten eine zusätzliche Datenkompression oder Verschlüsselung der darin gespeicherten Dateien an.[16, S. 35]

Es wird unterschieden, ob es sich um ein vollständiges Datenträgerabbild handelt oder um ein logisches Dateiarchiv. Bei den vollständigen Datenträgerabbildern werden auch nicht al-

⁴Siehe Link: <https://www.sleuthkit.org/autopsy/>. Letzter Zugriff: 10.8.2018. Es wird die Version 4.7.0 in der 64-bit Variante unter Windows 10 Pro genutzt.

⁵dd ist ein bekanntes Werkzeug zum Kopieren von Daten, welches unter den meisten Unix-basierten Betriebssystemen läuft. Damit können auch ganze Partitionen in einzelne logische Dateien kopiert werden.

⁶Siehe Link: <https://support.accessdata.com/hc/en-us/articles/222778608-What-Image-Formats-Do-AccessData-Products-Support->. Letzter Zugriff: 4.4.2018.

lokierte Speicherbereiche innerhalb des Dateisystems, der Partition oder des Datenträgers gesichert. Hier können sich potentiell versteckte und gelöschte Dateifragmente befinden. Auf diesen Datenträgerabbildern kann auch das bereits beschriebene File Carving ausgeführt werden, um gelöschte Dateien wiederherzustellen.

Ein logisches Dateiarchiv hingegen enthält wirklich nur die Dateien auf einer logischen Ebene und keine unallokierten Speicherbereiche. Diese Archive haben meistens eine geringere Speichergröße. Allerdings tritt durch die logische Sicherung ein potentieller Informationsverlust auf, da unallokierte Speicherbereiche nicht berücksichtigt werden, die aber dennoch potentiell auswertbare Informationen liefern können. Vertreter logischer Dateiarchive sind die bekannten Archiv-Formate ZIP oder TAR.

Letztlich werden die Beweismittel in unterschiedlichsten Formaten auf dem lokalen Analysecomputer gespeichert. Darauf aufbauend können die Daten in spezifische Formate konvertiert werden. Dies hängt aber meistens davon ab, wie sie weiter verarbeitet werden sollen und welche Werkzeuge zu dieser Verarbeitung genutzt werden.

Im konkreten Testszenario ist das Datenträger-Abbild eines Linux-Rechners im RAW-Format auf dem lokalen Analyse-Rechner gespeichert. Das Abbild kann ein oder mehrere Partitionen enthalten. Innerhalb der Partition werden Daten mithilfe unterschiedlicher Dateisysteme strukturiert gespeichert. Diese Dateisysteme können unter Windows mit dem Werkzeug *X-Mount* oder unter Linux direkt mit dem Befehl *mount* schreibgeschützt gemountet werden. Darauf wird das Dateisystem vom Betriebssystem interpretiert und als logisches Volume auf dem Analyse-Rechner bereitgestellt. Nun können die Dateien mit beliebigen Werkzeugen analysiert werden.

In der Praxis hat das einfache schreibgeschützte Mounten den Vorteil, dass der Analyst relativ schnell im Dateisystem beliebige Dateien finden und dessen Inhalt mit diversen Tools anzeigen kann. Gerade für eine schnelle Vorprüfung ist dies sinnvoll. In Kapitel 4.3 werden Möglichkeiten zur Speicherung und Aufbereitung des Datenträgerabbildes, mithilfe der forensischen Analyseplattform, untersucht.

Nachfolgend wird dargestellt, wie ein Datenträgerabild mit Autopsy (Version 4.7.0 64-bit) unter Windows 10 geöffnet und analysiert wird.

Zuerst wird in Autopsy ein neuer Fall erstellt. Hierbei kann ein Name für den Fall angegeben werden und ein Verzeichnis, worin Autopsy die Anwendungsdaten der Analyse speichert. Danach können noch einige optionale Informationen, wie beispielsweise der Bearbeiter, Adressdaten, die Organisation und eine kurze Beschreibung angegeben werden (siehe Abbildung 4.2). Bei der Erstellung des Falls wird unter anderem eine neue Falldatenbank angelegt. Diese Datenbanken werden lokal auf dem Analysecomputer gespeichert.

Im nächsten Schritt kann dem Fall eine neue Datenquelle hinzugefügt werden. Es werden folgende Typen von Datenquellen unterstützt:

- Ein Datenträgerabild im *RAW*-Format, Encase-Format oder ein Abbild einer virtuellen Maschine (z.B. von Virtual Box).
- Ein lokales Laufwerk (z.B. eine externe Festplatte).
- Logische Dateien aus einem verfügbaren Dateisystem (z.B. ein beliebiger Ordner).
- Ein Abbild eines beliebigen Speicherbereichs in einer Datei.

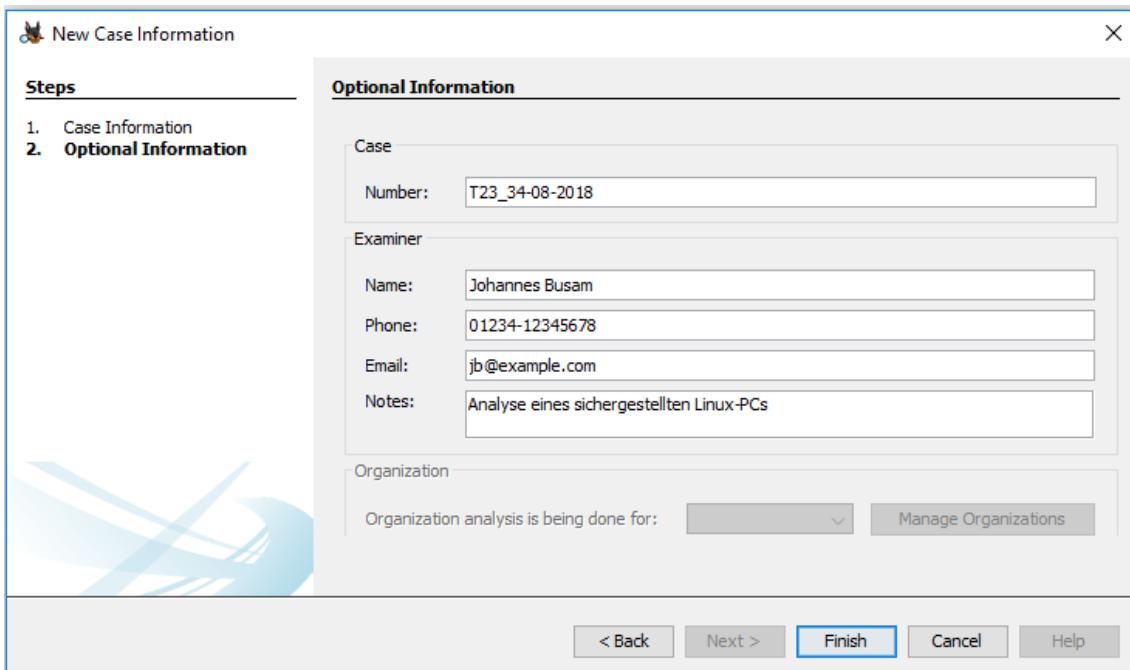


Abbildung 4.2: Erstellung eines neuen Falls mit Autopsy

Im konkreten Fall wird ein Datenträgerabbild als Datenquelle hinzugefügt. Dabei muss auch eine Zeitzone angegeben werden. Diese Zeitzone kann entscheidend für die Analyse der Zeitstempel auf einem Datenträger sein. In einem *ext*-Dateisystem bei gängigen Linux-Betriebssystemen werden die Zeitstempel als Anzahl der Sekunden seit dem 1. Januar 1970 in der Zeitzone UTC gespeichert.⁷[1, S. 326] Bei den älteren *FAT*-Dateisystemen hingegen wird die Zeit ohne Zeitzone gespeichert.[1, S. 192-194] Je nachdem in welcher Zeitzone das Betriebssystem konfiguriert wurde, welches die Dateien in dem *FAT*-Dateisystem änderte, ergeben sich zeitliche Unterschiede. Daher muss bei der Auswertung von Zeitstempeln immer auf die Zeitzone geachtet werden.⁸

Im nächsten Schritt können diverse Verarbeitungsmodule aktiviert werden. Diese Module dienen zur automatischen Datenaufbereitung und werden ausführlich in Kapitel 5.1 beschrieben. In dem Kapitel erfolgt auch der Vergleich zur automatisierten Auswertung mit der hier entwickelten Analyseplattform.

Nachdem die entsprechenden Module ausgewählt wurden, beginnt Autopsy die Datenquelle zu analysieren. Dies läuft vollständig im Hintergrund ab und der Nutzer kann parallel hierzu die Datenquelle manuell analysieren.

Das Importieren einer Datenquelle bei Autopsy, besteht aus dem Erstellen eines Falls und der Angabe einiger Konfigurationsmöglichkeiten. Die Datenquelle wird hierbei nicht in einen internen Anwendungsordner kopiert, sondern während der Analyse auf dem Rechner

⁷Diese Zeitdefinition entspricht der sogenannten Unixzeit.

⁸Ein weiteres interessantes Problem ergibt sich auch bei der Sicherung der Beweismittel an einem Tatort. Dort ist nie garantiert, dass alle gesicherten Beweismittel überhaupt zeitlich synchronisiert sind. Gerade in Kombination mit Netzwerkverbindungsdaten können bei einer fehlenden Zeitsynchronisation kritische Abläufe zeitlich versetzt sein. Daher muss die Aussagekraft von Zeitstempel immer kritisch betrachtet werden.

bereitgestellt (entweder als Datenträgerabbild oder direkt als externer Datenträger). In dem Anwendungsordner von Autopsy werden Metainformationen, wie beispielsweise die Indexierung bestimmter Daten, abgespeichert, um während der Analyse schneller darauf zugreifen zu können. Prinzipiell ist dieses Vorgehen sehr gut, da der Ermittler direkt mit der Arbeit beginnen kann und keine Daten kopiert werden müssen.⁹

4.3 Umsetzung in der forensischen Analyseplattform

Im vorangegangen Kapitel wird beschrieben, wie Datenträgerabbilder als Datenquelle in Autopsy importiert werden. Autopsy arbeitet direkt auf den Daten, um ein unnötiges Kopieren von Daten und dessen Ressourcenaufwand zu vermeiden.

Im Vergleich dazu arbeitet die hier entwickelte forensische Analyseplattform auf einem eigenen Computer-Cluster. Dieses Cluster besteht aus mehreren Knoten, welche die Daten der Datenträgerabbilder verarbeiten. Daher müssen die forensisch relevanten Daten zuerst in die Analyseplattform importiert werden.

Da die Analyseplattform auf dem Hadoop-Framework aufbaut, bildet der Kern der Datenspeicherung das HDFS.¹⁰ Zur Speicherung der Daten gibt es mehrere Möglichkeiten, deren Vor- und Nachteile nachfolgend dargestellt werden sollen.

4.4 Variante 1 - Speicherung der Datenträgerabbilder

Die naheliegende Variante zur Speicherung der Asservate, ist die Datenträgerabbilder direkt im HDFS abzuspeichern. Die Größe der Abbilder ist nicht problematisch. Um eine entsprechende Aufteilung kümmert sich das HDFS. Allerdings hat die Lösung den entscheidenden Nachteil, bei der Weiterverarbeitung der Daten.

Auf Betriebssystemebene können Datenträger mit mehreren Partitionen und unterschiedlichen Dateisystemen interpretiert und eingebunden werden. Dabei liegen die Dateien als fragmentierte Blöcke in einer spezifischen Datenstruktur vor, welche das Dateisystem des Abbildes beschreiben. Je nachdem, ob ein Datenträgerabbild direkt von einer Partition eines Datenträgers oder vom ganzen Datenträger erstellt wurde, sind in dem Abbild unter Umständen auch mehrere Partitionen samt Partitionstabelle enthalten. Von diesen Partitionen kann wiederum jede einzelne Partition ein eigenes Dateisystem, wie zum Beispiel ext4 oder NTFS, enthalten. Dieses Dateisystem enthält die eigentlichen Dateien, welche logisch zusammengesetzt werden müssen. Viele Betriebssysteme bieten bereits eine weitreichende Unterstützung zum Lesen und Schreiben der Dateisysteme an. Hierzu können die Dateisysteme einzelner Partitionen *gemountet* werden.

Innerhalb des Hadoop-Frameworks existiert jedoch keine Unterstützung zum Lesen von beliebigen Dateisystemen. Denn normalerweise nutzen Java-Applikationen eine definierte Schnittstelle auf Basis von Dateien, die wiederum vom Betriebssystem bereitgestellt werden. Um die logischen Dateien aus dem Datenträgerabbild extrahieren zu können, muss für jedes Dateisystem eine eigene Implementierung in Java geschrieben werden. Diese Implementierung muss dann auch noch für das HDFS-Dateisystem optimiert sein.

⁹Das Erstellen eines Datenträgerabbildes wird vorher durchgeführt.

¹⁰Siehe Kapitel 3.2.

Darüber hinaus ist das Extrahieren von Dateien aus einem Datenträgerabbild, welches im HDFS gespeichert wird, nicht effizient lösbar. Beispielsweise wird nun mit Apache Spark eine Datei aus dem gespeicherten Abbild gelesen. Aufgrund der eingangs beschriebenen Datenlokalität (siehe Kapitel 3), sind auf jedem Knoten einzelne Blöcke von 128 MB Größe vorhanden. Um im ext4-Dateisystem eine Datei lesen zu können, sollten zumindest die Dateisystemmetadaten verfügbar sein. Darüber hinaus kann der Dateiinhalt einer einzelnen Datei verstreut innerhalb des Dateisystems liegen. Je nach Grad der Fragmentierung des Dateisystems, müssten auf einem Data Node innerhalb des Clusters schlimmstenfalls dutzende weitere Blöcke von anderen Knoten nachgeladen werden, um den Inhalt einer einzelnen Datei zu verarbeiten. Dies würde das Prinzip der Datenlokalität aushebeln.

Abbildung 4.3 skizziert diese verstreute Aufteilung einer Datei im physikalischen Hadoop-Cluster.

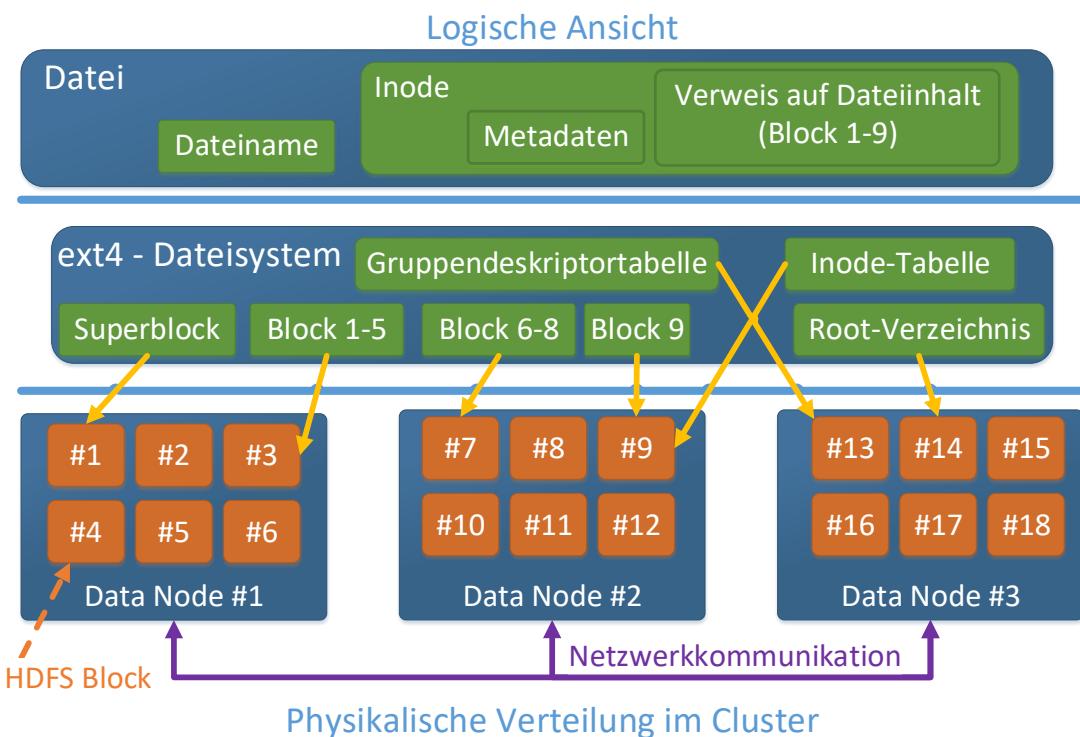


Abbildung 4.3: Aufteilung der Daten des Datenträgerabbildes im Hadoop-Cluster

Das Abbild zeigt eine Datei, welche aus logischer Sicht einen Dateinamen, Metadaten (beispielsweise Zugriffsrechte) und einen Inhalt besitzt. Der Inhalt ist in 9 Blöcke zu jeweils 2048 Byte aufgeteilt.¹¹ Um nun den Inhalt einer Datei aus dem ext4-Dateisystem auszulesen, wird zuerst der Superblock benötigt. Dieser enthält allgemeine Informationen zum Dateisystem.

¹¹Die Blockgröße wird hierbei vom ext4-Dateisystem bestimmt und ist die kleinste allozierbare Einheit im Dateisystem. In der physikalischen Aufteilung im HDFS gibt es auch sogenannte Blöcke, welche aber eine Größe von 128 MB aufweisen (orange in Abbildung 4.3).

Darauf wird die Gruppendedeskriptortabelle benötigt, um auf einzelne Blockgruppen zuzugreifen.¹² Über eine Blockgruppe kann wiederum auf die Inode-Tabelle zugegriffen werden. Diese speichert die Metadaten einzelner Dateien als sogenannte *Inodes* ab. Ein Inode-Eintrag hält wiederum Verweise auf die Blöcke, welche den Dateinhalt beschreiben. Der Dateiname hingegen ist in dem logisch übergeordneten Verzeichnis gespeichert. Das oberste Verzeichnis ist das Wurzelverzeichnis. Dieses enthält die Namen der Kind-Dateien und entsprechende Verweise zum Inode.

Beim Auslesen einer Datei müssen nun etliche Speicherstellen innerhalb des Dateisystems gelesen und interpretiert werden. Angenommen, es wird ein konkretes ext4-Dateisystem in einer 100 GB großen Partition als Datei im HDFS gespeichert. So wird diese große Datei im HDFS-Dateisystem in 800 Blöcke zu je 128 MB aufgeteilt und auf den einzelnen Knoten des Clusters gespeichert. Hierbei kann aber kein Einfluss darauf genommen werden, wo welche Blöcke mit welchem Inhalt gespeichert werden. Letztlich bedeutet dies wiederum, wenn in einem Apache Spark Executor zur Verarbeitung der Daten, eine Datei des Knotens gelesen werden soll, müssen dutzende weitere Datenblöcke von anderen Knoten angefordert werden. Dadurch wird auf Netzwerkebene unnötig viel Last erzeugt. Um das Prinzip der Datenlokalität einhalten zu können, müssen die einzelnen Blöcke im HDFS unabhängig voneinander interpretierbar sein. Diese Problematik tritt übrigens nicht nur bei der ext-Dateisystemfamilie auf, sondern auch bei anderen Dateisystemen.

Aus den oben genannten Gründen ist die direkte Speicherung von Datenträgerabbildern im HDFS nicht geeignet, für die forensische Analyse im Hadoop-Cluster.

4.5 Variante 2 - Speicherung der logischen Dateien

In dieser Variante wird das Beweismittel auf dem lokalen Analyserechner gemountet. Darauf aufbauend werden alle Dateien auf logischer Ebene direkt in das HDFS importiert. Damit ist die gesamte Dateisystemstruktur aus dem Datenträgerabbild im HDFS abgelegt. Einzelne Dateien aus dem Datenträgerabbild sind nun auch als einzelne Dateien im HDFS gespeichert und können unabhängig voneinander prozessiert werden. Darüber hinaus ist die Datenstruktur im HDFS unabhängig von dem Dateisystem des importierten Datenträgerabbildes.

Damit sind die Nachteile der vorangegangenen ersten Variante aus Kapitel 4.4 behoben. Allerdings ist das bereits erwähnte File Carving, beziehungsweise das Auffinden von gelöschten Dateien, nun nicht mehr im Hadoop-Framework möglich. Denn bei dieser Variante werden nur die Dateien aus dem Dateisystem in das Hadoop-Framework importiert. Freie Speicherbereiche werden nicht weiter untersucht. Es wäre aber möglich, zusätzlich das vollständige Datenträgerabbild in das HDFS zu importieren, um dann später freie Speicherbereiche analysieren zu können.

Im Rahmen der Thesis wird diese Einschränkung jedoch vorerst akzeptiert. Ein File Carving ist daher mit der hier entwickelten forensischen Analyseplattform noch nicht möglich. Analog zur Referenzsoftware Autopsy können nun auch beliebige Verzeichnisse als Datenquelle in die Analyseplattform geladen werden.¹³

¹²Das Dateisystem ist in mehrere autarke Bereiche unterteilt, welche für sich genommen eigenständig die Daten einer Teilmenge aller Dateien vorhalten. Das sind die sogenannten Blockgruppen.

¹³Siehe Kapitel 4.2.

Interessant an dieser Variante ist das Verhalten des HDFS-Dateisystems bezüglich der Metadaten und der unterschiedlichen Dateigrößen. Zur Analyse der Dateien auf dem Datenträger werden auch die Metadaten zu den Dateien benötigt. Beim Importieren muss darauf geachtet werden, dass alle Metadaten des lokalen Dateisystems im Datenträgerabild unverändert in das HDFS kopiert werden. Im HDFS werden auch Metadaten zu den einzelnen Dateien gespeichert. Möglicherweise könnten diese Dateiattribute wiederverwendet werden, um die Metadaten aus dem originalen Dateisystem zu speichern. Welche Metadaten bereits im HDFS angelegt werden, zeigt Abbildung 4.4 anhand eines Ausschnitts aus der Web-Oberfläche eines HDFS.

Browse Directory

| | Permission | Owner | Group | Size | Last Modified | Replication | Block Size | Name |
|--------------------------|------------|----------|------------|---------|---------------|-------------|------------|--------------------------|
| <input type="checkbox"/> | drwxr-xr-x | johannes | supergroup | 0 B | Apr 04 06:38 | 0 | 0 B | DiagrammeUndRessourcen |
| <input type="checkbox"/> | -rw-r--r-- | johannes | supergroup | 12.9 MB | Apr 04 06:38 | 1 | 128 MB | M105 Studienbriefe.pdf |
| <input type="checkbox"/> | -rw-r--r-- | johannes | supergroup | 2.06 MB | Apr 04 06:38 | 1 | 128 MB | M107-windows10-05-31.pdf |

Abbildung 4.4: HDFS - Dateieigenschaften

Daraus ist ersichtlich, dass jede Datei entsprechende Dateirechte hat und einem Nutzer und einer Gruppe zugeordnet ist. Zusätzlich wird die Größe und der Zeitstempel der letzten Änderung gespeichert.¹⁴ Die Anzahl der Replikationen und die Blockgröße sind spezifisch für das HDFS. Jede Datei kann auf einer unterschiedlichen Anzahl von Knoten repliziert sein. Die Standardkonfiguration definiert 3 Replikationen im realen Cluster, wobei Verzeichnisse nur logisch auf dem Name Node abgelegt werden und damit auf keinem Data Node explizit repliziert werden. Auch die Blockgröße ist in der Standardkonfiguration auf 128 MB festgelegt. Wie im Grundlagenkapitel 3.2 erwähnt, werden die Dateien in mehreren Blöcken zu maximal 128 MB gespeichert und repliziert.¹⁵

Bezogen auf klassische Dateisysteme, entspricht ein Block im HDFS einem Block im ext4-Dateisystem oder einem Cluster im NTFS-Dateisystem. Es ist letztlich die kleinste allozierbare Dateneinheit im Dateisystem.[1, S.129-140] Dies bedeutet allerdings nicht, dass für jede Datei im HDFS auf den jeweiligen Data Nodes immer mindestens 128 MB Speicher belegt werden. Denn die reale Speicherbelegung auf dem Data Node beschränkt sich auch auf die reale Größe der Datei im lokalen Dateisystem des Data Nodes.[14, S. 16-17]

Mit dem Befehl aus Listing 4.1 können lokale Dateien in das HDFS importiert werden.

```
1 # hdfs dfs -put [source] [destination]
2 hdfs dfs -put test.pdf /test.pdf
```

Listing 4.1: Befehl zum Speichern einer Datei im HDFS

¹⁴Bei Dateiverzeichnissen ist die Größe 0 Byte.

¹⁵Diese Blockgröße kann konfiguriert werden.

Hierbei werden die ursprünglichen Metadaten der Datei nicht übernommen. So beschreibt der oben erwähnte Modifikationszeitstempel den Zeitpunkt, zu dem die Datei im HDFS das letzte Mal geändert wurde. Dies entspricht initial dem Import-Zeitpunkt. Auch die Nutzer- und Gruppenrechte werden nicht übernommen. Prinzipiell wäre es aber möglich, die Metadaten aus dem lokalen Dateisystem mit in das HDFS zu übernehmen.¹⁶ Ratsam ist dies jedoch nicht, da der Nutzer, die Gruppe und die dazugehörigen Zugriffsrechte in einem produktiven HDFS-Cluster verwendet werden, um Zugriffsbeschränkungen einzelner Nutzer und Anwendungen auf Dateien im HDFS einzusetzen. Die Metadaten des originalen Dateisystems sollten daher mit einer anderen Methode im HDFS gespeichert werden.

Eine bessere Möglichkeit bietet das HDFS mithilfe von erweiterten Dateiattributen. Diese können beliebige Informationen zu einer Datei speichern. Mit nachfolgenden Befehlen kann beispielsweise der Zeitstempel der Erstellung einer Datei aus dem ursprünglichen Dateisystem im HDFS als erweitertes Attribut gespeichert und ausgelesen werden. Hierbei kann der Name des Attributs (`user.ntfs.creationtime`) und dessen Inhalt (`2018-04-07T11:14:42,798583789+02:00`) frei gewählt werden.

```

1 # Erweitertes Dateiattribut erstellen
2 hdfs dfs -setfattr -n user.ntfs.creationtime -v "2018-04-07T11
   :14:42,798583789+02:00" /test.pdf
3
4 # Erweitertes Dateiattribut auslesen
5 hdfs dfs -getfattr -d -n user.ntfs.creationtime /test.pdf

```

Listing 4.2: Befehl zum Hinzufügen und Auslesen von Metadaten

Mit dem obigen Befehl ist es möglich, alle Metadaten des ursprünglichen Dateisystems als erweiterte Dateiattribute im HDFS zu speichern. Allerdings müssen diese Metadaten für jede Datei im HDFS explizit eingetragen werden.

Zusätzlich müssen bei der Datenverarbeitung mit Apache Spark die Metadaten auslesbar sein. Das Auslesen im Spark-Kontext ist umständlich, aber möglich.¹⁷

Es gibt jedoch zwei entscheidende Nachteile bei dieser Variante, die beide den gleichen Ursprung haben. Der erste Nachteil ist, dass jede einzelne Datei aus dem ursprünglichen Dateisystem als getrennte eigenständige Datei in das HDFS hochgeladen werden muss. In einem einzigen Dateisystem können Millionen kleine Dateien gespeichert sein, die alle auch in das HDFS importiert werden müssen. Allerdings ist das HDFS primär für größere Dateien (in der Größenordnung einer Blockgröße von 128 MB) ausgelegt und kann viele kleine Dateien nicht wirklich effizient speichern und bereitstellen. Dies ist dem Umstand geschuldet, dass alle Metadaten auf dem Name Node gespeichert werden und nur der Dateinhalt im Cluster aufgeteilt wird.[14, S. 16] Wenn nun viele kleine Dateien gespeichert werden, dann steigt der Speicherverbrauch im Name Node an und beeinträchtigt die Performanz des Systems. Der zweite Nachteil verstärkt dieses Problem. Denn wenn nun auch noch die Metadaten aus dem ursprünglichen Dateisystem als erweiterte Metadatenattribute im HDFS gespeichert werden, dann benötigt der Name Node noch mehr Ressourcen. Darüber hinaus wäre die Verarbeitung der Metadaten mit Apache Spark nur bedingt parallelisierbar, da diese Daten immer zuerst an dem Name Node angefordert und über das Netzwerk

¹⁶Hierzu kann dem `put`-Befehl aus Listing 4.1 der Parameter `-p` mit übergeben werden.

¹⁷Siehe Metadaten-Extraktion im Projekt `foam-processing-spark` unter <https://github.com/jobusam/foam-processing-spark> (Letzter Zugriff: 6.10.2018).

zu den einzelnen Spark Executoren gesendet werden müssten. Erst dann könnten die Executoren die Daten parallel verarbeiten. Abbildung 4.5 skizziert nochmals den Datenfluss bei dieser Lösung.

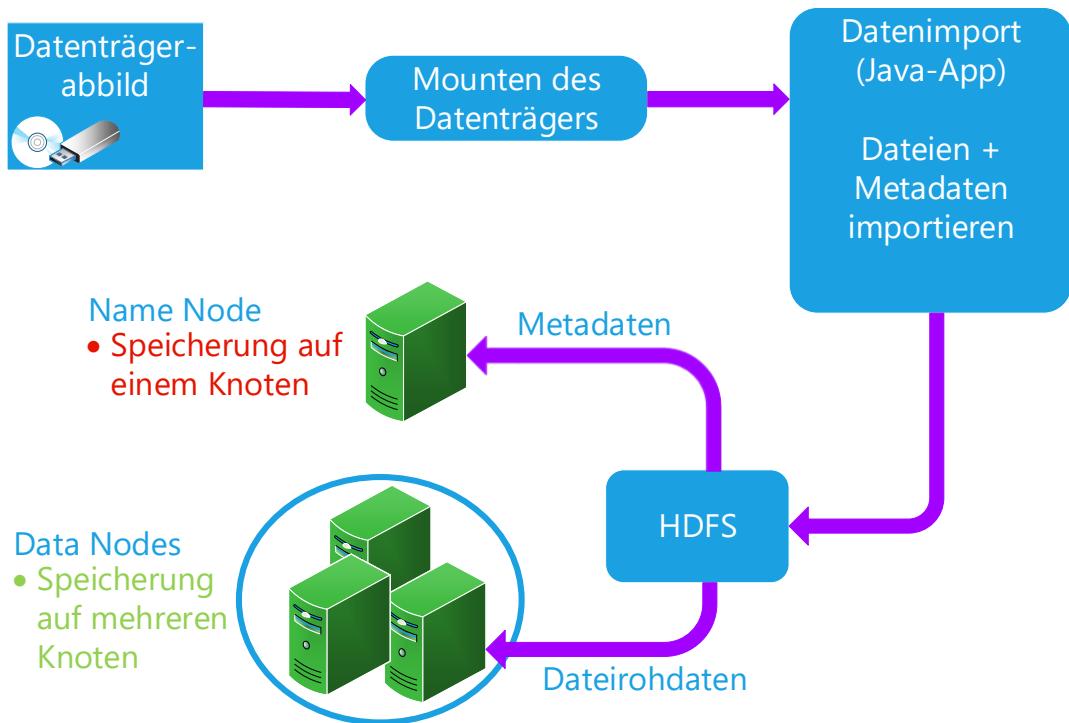


Abbildung 4.5: Datenspeicherung mit erweiterten Dateiattributen im HDFS

Das Fazit der Variante 2 lautet daher, dass die Dateimetadaten des originalen Datenträgerabbildes höchstens als erweiterte Attribute im HDFS abgelegt werden könnten. Beim Importieren müssten diese Metadaten bei jeder einzelnen Datei explizit nachgetragen werden. Alle Dateimetadaten werden nur auf dem Name Node gespeichert. Dadurch benötigt der Name Node mehr Speicher und könnte zu einem Flaschenhals im System werden. Zudem ist die parallelisierte Datenverarbeitung eingeschränkt, da die Metadaten immer zuerst von dem Name Node angefordert werden müssen. Aus diesen Gründen ist die Variante 2 nicht akzeptabel.

4.6 Variante 3 - Speicherung in Dateicontainer

Die vorangegangene Variante überzeugt nicht, da die Speicherung vieler kleiner Dateien nicht effizient im HDFS durchgeführt werden kann. Da alle Metadaten einer Datei im Name Node abgelegt werden, bildet der Name Node bei vielen kleinen Dateien einen Flaschenhals. Zur Lösung dieser Problematik existieren im Hadoop-Umfeld diverse Dateicontainer. Diese Dateicontainer können mehrere Dateien in einem strukturierten Format speichern. In Analogie zu bekannten Dateicontainern, wie beispielsweise ZIP-Archiven oder TAR-Archiven, existieren im Hadoop-Umfeld *Sequence Files*, *RC/ORC Files*, *Avro-Files* und *Parquet-Files*.[13, S. 296]

Ziel dieser Dateiformate ist es, viele kleine Daten in größere Dateien zu speichern, um eine bessere Parallelisierung und eine effiziente Speicherung in Hadoop zu ermöglichen. Oftmals unterstützen diese Formate auch eine Datenkompression, um gegebenenfalls Speicherplatz sparen zu können. Viel wichtiger ist jedoch die Teilbarkeit dieser Dateiformate. Wie bereits beschrieben, werden Dateien im HDFS in größere Blöcke geteilt und auf unterschiedlichen Knoten gespeichert. Innerhalb eines Blocks muss es also möglich sein, einzelne Einträge, beziehungsweise Datensätze, lesen zu können. Die oben erwähnten Hadoop Dateiformate unterstützen eben diese Teilbarkeit.¹⁸

Nachfolgend soll das *Sequence File*-Format in Abbildung 4.6 näher betrachtet werden.¹⁹

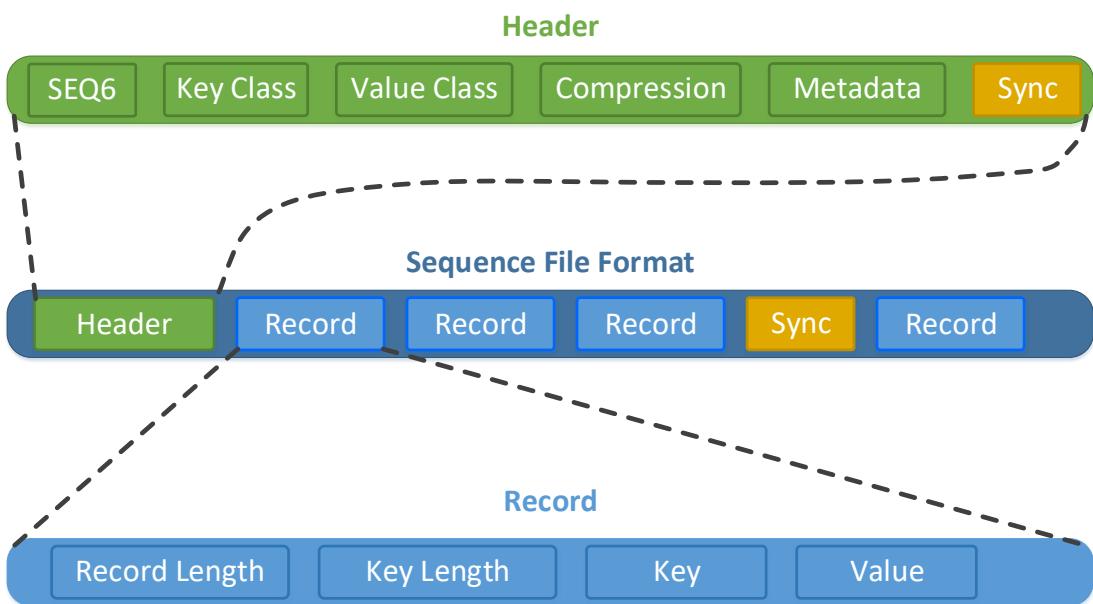


Abbildung 4.6: Sequence File Format (Vgl. [11, S. 134])

Das Sequence File Format besteht aus einem Header und mehreren Einträgen. Diese Einträge sind eigenständige Schlüsselwertpaare, welche die eigentlichen Daten beinhalten. Ein Schlüsselwertpaar, in Abbildung 4.6 auch *Record* genannt, enthält einen eindeutigen Schlüssel (*Key*) und einen Inhalt (*Value*). Zusätzlich wird am Anfang die Gesamtlänge des Schlüsselwertpaars und die Länge des Schlüssels in Bytes angegeben. Damit ist es möglich, den Schlüssel sowie den Inhalt innerhalb des Sequence Files zu bestimmen. Allerdings ist dadurch noch nicht klar, wie der Schlüssel oder Inhalt zu interpretieren ist. Daher sind im Header des Sequence File Formats jeweils die Namen der Java-Klassen in den Feldern *Key*

¹⁸Im Gegensatz dazu sind die klassischen Dateisysteme innerhalb einer Partition nicht teilbar. Denn wenn ein Block in der Mitte des Dateisystems ausgelesen werden soll, so können die Daten nicht ohne die Dateisystemmetadaten interpretiert werden. Daher ist auch die erste Variante aus Kapitel 4.4 eben nicht im HDFS anwendbar.

¹⁹Siehe auch [11, S. 134] und nachfolgenden Link: <https://hadoop.apache.org/docs/r2.7.5/api/org/apache/hadoop/io/SequenceFile.html>. Letzter Zugriff: 18.8.2018.

Class und *Value Class* gespeichert, die den Datentyp definieren. Im Header befinden sich auch Informationen, ob und in welcher Form eine Datenkompression auf die Daten angewendet wurde.

Zuletzt werden in unregelmäßigen Abständen sogenannte Sync-Felder abgespeichert. Diese dienen zur Unterstützung der eingangs erwähnten Teilbarkeit des Dateiformats. Eine Anwendung kann sich mithilfe der Sync-Felder, von einer beliebigen Stelle innerhalb der Datei, auf den Anfang eines Schlüsselwertpaars synchronisieren. Damit können auch Schlüsselwertpaare aus einem beliebigen HDFS-Block interpretiert werden.²⁰

Prinzipiell können damit sehr kleine Dateien in mehrere Sequence Files strukturiert im HDFS gespeichert werden. Diese Variante enthält aber noch einige Hindernisse. Zuerst stellt sich hier die Frage, wie diese Sequence Files erstellt werden sollen. Hierbei müsste die Anwendung zum Datenimport auf dem Analyse-Rechner die Sequence Files zuerst lokal auf dem Rechner erstellen und danach in das HDFS hochladen. Gegebenenfalls müssten diese Sequence Files auf dem lokalen Rechner persistent zwischengespeichert werden. Die Datenimport-Anwendung würde mehr Ressourcen benötigen.

Ein interessantes Problem ist auch die Datenverarbeitung im HDFS. Angenommen es existieren nun Sequence Files mit den Dateiinhalten und den Metadaten. Mit Apache Spark können diese Sequence Files gelesen werden. Darauf aufbauend können die Hashsummen und die Medientypen ermittelt werden.²¹ Allerdings müssen die Daten beim Schreibvorgang in neue Sequence Files geschrieben werden. Denn im HDFS ist es nicht möglich, existierende Dateien wahlfrei zu modifizieren.[13, S. 42] Es können ausschließlich neue Daten an das Dateiende eines Sequence Files geschrieben werden. Daher müssen bei der Datenverarbeitung nochmals alle Daten neu geschrieben werden. Dies führt zu unnötigem Ressourcenverbrauch. Andererseits können die Rohdaten und die Metadaten in getrennte Sequence Files gespeichert werden. Damit müssen nur die Sequence Files mit den Metadaten neu geschrieben werden. Es wäre auch denkbar, alle neu gewonnenen Metadaten in eigenständige neue Sequence Files zu schreiben.

Allerdings kann dies wiederum zu einer Art von Fragmentierung von logisch zusammenhängenden Daten führen. Denn nun sind die Metadaten und Rohdaten in mehrere Sequence Files aufgeteilt. Schlimmstenfalls können dadurch die Metadaten und Rohdaten, welche eine logische Datei repräsentieren, auf unterschiedlichen Knoten im Hadoop-Cluster liegen. Dadurch wird das Prinzip der Datenlokalität in gewissem Maße beeinträchtigt. Dies hängt aber auch stark davon ab, wie die Daten für die Verarbeitung angefordert werden. Ist es notwendig, die Metadaten und die Rohdaten einer logischen Datei gemeinsam zu verarbeiten oder können diese auch unabhängig voneinander auf getrennten Knoten prozessiert werden?

Eine getrennte Verarbeitung von Metadaten und Rohdaten schränkt die Algorithmen zur Datenanalyse stark ein. Denn schon bei simplen Analysen, wie beispielsweise der Ermittlung des Medientyps einer Datei, werden Informationen aus den Metadaten und den Rohdaten benötigt. Daher können die Metadaten und die Rohdaten, im Kontext der forensischen Analyseplattform, nicht getrennt verarbeitet werden.

Zusammengefasst ist diese Variante technisch möglich. Allerdings besteht die Problematik beim Speichern von neu gewonnenen Informationen. Letztlich ist es sinnvoll, wenn die

²⁰Voraussetzung hierbei ist allerdings, dass die Anwendung vorher schon die Datentypen der Schlüsselwertpaare kennt.

²¹Siehe auch Kapitel 5.

Rohdaten, die originalen Metadaten aus dem ursprünglichen Dateisystem und die neu gewonnenen Metadaten aus der Datenverarbeitung, für eine logische Datei auch physikalisch zusammen gespeichert werden.²²

Ein anderer Aspekt ist die Komplexität der Anwendung. Bei der praktischen Implementierung dieser Variante muss immer betrachtet werden, wo nun welche Informationen gespeichert sind und wie alle Informationen zu einer logischen Datei zusammengesetzt werden müssen. Dadurch wird die Implementierung sehr komplex. Darauf hinaus sind Sequence Files nur bei kleinen Dateien wirklich sinnvoll. Große Dateien hingegen können direkt im HDFS gespeichert werden. Dies würde die Anwendungskomplexität weiter erhöhen. Daher überzeugt auch diese Variante nicht zur Datenspeicherung.²³

4.7 Variante 4 - Speicherung in HBase und HDFS

4.7.1 Allgemeines

Die vorherige Variante beschreibt einen möglichen Ansatz zur Speicherung von kleinen Dateien. Allerdings wird die Speicherung der Metadaten noch nicht optimal gelöst. Zumal beachtet werden muss, dass während der Datenverarbeitung weitere Metadaten aus den Rohdaten ermittelt und gespeichert werden.²⁴ Da es sich bei den Metadaten um strukturierte Daten handelt, wäre die Speicherung in einer Datenbank naheliegend. Im Hadoop-Umfeld ist hierzu die spaltenorientierte *NoSQL*-Datenbank *Apache HBase* sehr gut geeignet.²⁵ Auch die Speicherung von kleinen Dateien ist in HBase möglich. Für große Dateien hingegen, ist eine Speicherung im HDFS sinnvoll.

4.7.2 Speicherung kleiner Dateien

Die Problematik von kleinen und großen Dateien wird bereits in den vorherigen Varianten aufgezeigt. An dieser Stelle wird die Thematik nochmals näher betrachtet. Anhand einiger Datenträgeranalysen wird ein Grenzwert ermittelt, nach welchem die Analyseplattform die Dateien entweder in HBase oder im HDFS ablegt.

Das HDFS kann mit großen und kleinen Dateien umgehen. Die Speicherung großer Dateien ist jedoch der primäre Anwendungsfall. Im Gegensatz dazu können viele kleine Dateien nicht effizient gespeichert werden. Es geht aber nicht darum, dass eine einzelne kleine Datei weniger effizient abgespeichert werden kann als eine große Datei. Vielmehr kann der Informationsgehalt einer einzelnen großen Datei, wie beispielsweise einem Sequence File, effizienter gespeichert werden, als der gleiche Informationsgehalt aufgeteilt in dutzende kleine Dateien. Dies liegt daran, dass für jede Datei Metadaten gespeichert werden. Diese Metadaten werden auf dem Name Node gespeichert und auch im Arbeitsspeicher vorgehalten.[18] Ein Eintrag ist beispielsweise ungefähr 150 bis 200 Bytes groß. Für jede Datei wird ein Metadateneintrag und ein Blockeintrag im Name Node angelegt (insgesamt 300-400 Byte). Wenn nun eine Million kleine Dateien abgespeichert werden, dann werden 300-400 MB Arbeitsspeicher benötigt. Dies klingt nach einem vertretbaren Ressourcenverbrauch.

²²Zumindest sollten die Daten auf dem gleichen Knoten liegen, um Netzwerkverkehr zu vermeiden.

²³Die Entscheidung, diese Variante nicht zu verfolgen, basiert nur auf den theoretischen Vorüberlegungen. Auf eine prototypische Implementierung dieser Variante wurde verzichtet, weil mit der vierten Variante zur Datenspeicherung ein Ansatz gefunden wurde, der auch schon in der Theorie mehr überzeugt, als die Variante mit den Sequence Files.

²⁴Siehe Kapitel 5.

²⁵Siehe Kapitel 3.5.

Letztlich geht es aber auch um die Netzwerklast. Denn bei der Verarbeitung der Daten werden auch eine Million Aufrufe an den Name Node gesendet, da nur er weiß, wo der Dateinhalt liegt. Wenn nun diese eine Million Dateien in ein einzelnes Sequence File gepackt wird, dann benötigt der Name Node nur 300-400 Byte Arbeitsspeicher und deutlich weniger Netzwerkressourcen bei Anfragen.

Nun stellt sich die Frage, ob eine Million Dateien realistisch anzusehen sind und wie groß kleine Dateien sind. Nachfolgende Abbildungen zeigen die Resultate einer Analyse der Dateigröße von diversen Datenträgern. Abbildung 4.7 zeigt hier die kumulierte Häufigkeit der Dateien, unterteilt in mehrere Dateikategorien. Diese Kategorien sind nach dem dekadischen Logarithmus aufgeteilt.²⁶ Eine Kategorie beschreibt die Anzahl aller Dateien in einem Datenträgerabbild, welche kleiner als die angegebene Kategoriegröße ist. Zum Beispiel existieren auf dem Datenträgerabbild des Windows Systems knapp 400.000 Dateien die kleiner 10 Kilobyte sind.

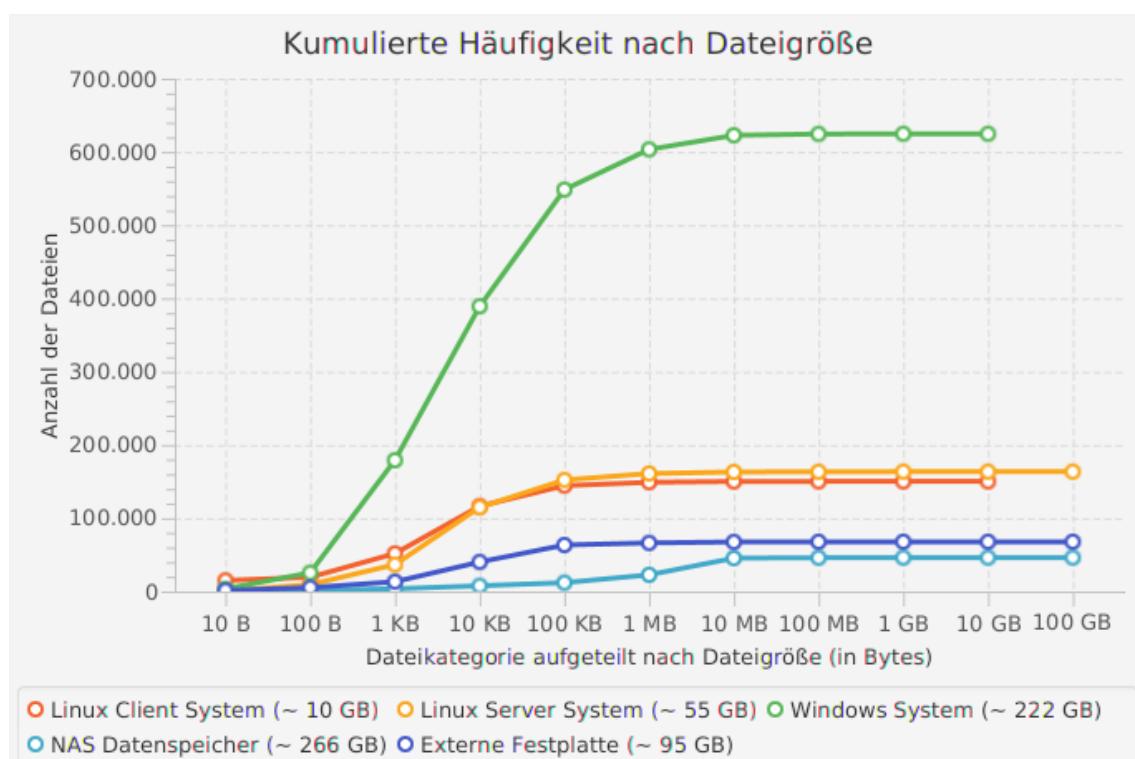


Abbildung 4.7: Kumulierte Häufigkeit nach Dateigröße

Nachfolgend werden die Testdaten beschrieben:

- Das *Linux Client System* ist ungefähr 10 GB groß.²⁷
Darauf ist ein Ubuntu-Betriebssystem installiert. Es wurde als Testdatenträgerabbild im Rahmen der Masterthesis erstellt. Das Abbild enthält 150.229 Dateien.²⁸

²⁶Die Ergebnismenge der Kategorien wird linear interpoliert. Der Quellcode wird unter nachfolgendem Link: <https://github.com/jobusam/foam-data-analysis-ui> bereitgestellt. Letzter Zugriff: 8.10.2018.

²⁷Die Größenangaben entsprechen den reinen Rohdaten der Dateien. Verzeichnisse und Dateisystemmetadaten sind nicht inkludiert.

²⁸Es handelt sich ausschließlich um Datendateien. Verzeichnisse, symbolische Links und spezielle Dateien werden nicht berücksichtigt.

- Das *Linux Server System* ist ungefähr 55 GB groß.
Darauf ist ein CentOS-Betriebssystem installiert. Das System ist ein Name Node eines kleinen Hadoop-Clusters. Das Abbild enthält 163.555 Dateien.
- Das *Windows System* ist ungefähr 222 GB groß. Das darauf installierte Windows 10 ist seit mehreren Monaten im Einsatz. Das Abbild enthält 624.650 Dateien.
- Der *NAS Datenspeicher* entspricht einem QNAP-System mit ungefähr 266 GB an realen Rohdaten. Hierbei ist auf dem Datenträgerabbild kein Betriebssystem installiert. Es handelt sich hauptsächlich um Dokumente und Mediendateien. Das Abbild enthält 46.215 Dateien.
- Die *Externe Festplatte* mit ungefähr 95 GB Daten, wird als Backup für diverse Mediendateien genutzt. Das Abbild enthält 67.809 Dateien.

Da die forensische Analyseplattform mehrere Datenträgerabbilder speichern kann, sollte das System durchaus mehrere Millionen Dateien verarbeiten können. Abbildung 4.8 relativiert die Ergebnisse der einzelnen Abbilder.

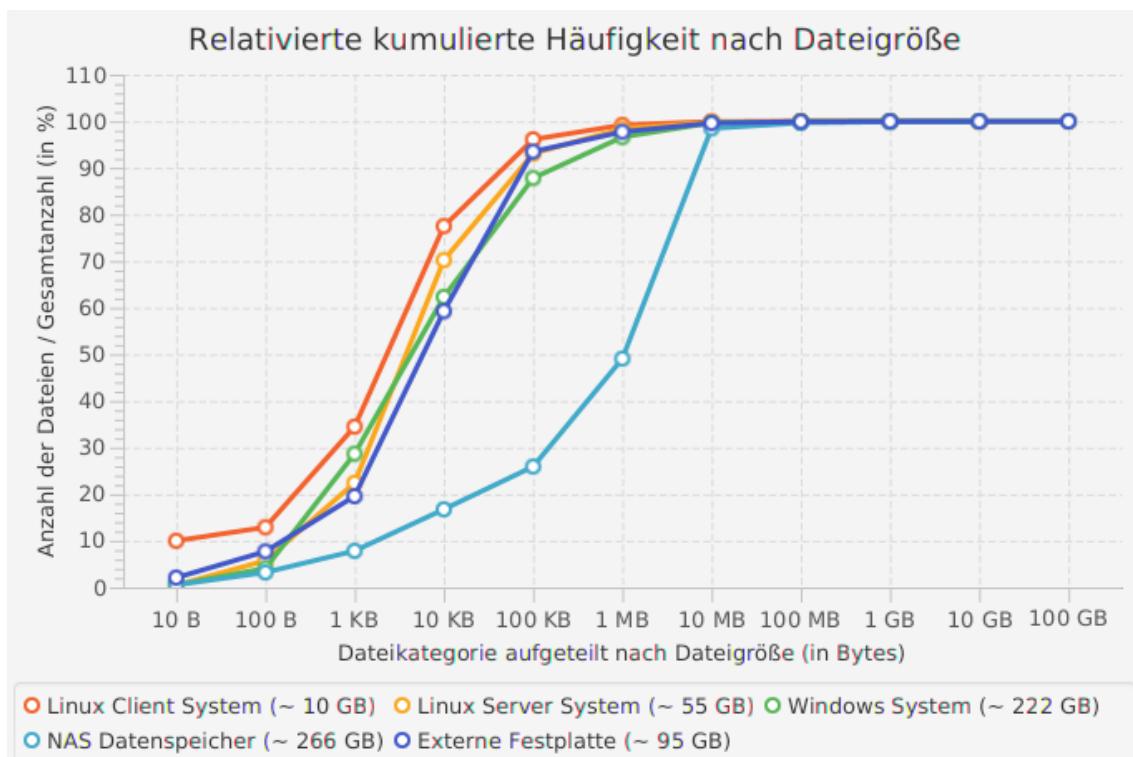


Abbildung 4.8: Relativierte kumulierte Häufigkeit nach Dateigröße

Anhand der relativierten kumulativen Häufigkeit aus Abbildung 4.8 wird klar, dass fast 80-90 % der Dateien kleiner 100 Kilobyte und mehr als 95% der Dateien kleiner 10 Megabyte sind. Allerdings sind diese Angaben mit Vorsicht zu genießen, denn je nach Anwendungsfall können Datenträger beliebige Dateien unterschiedlicher Größe speichern. Ist beispielsweise ein Betriebssystem auf dem Datenträger installiert, existieren allein durch das Betriebssystem tausende von Dateien mit minimaler Dateigröße. Umgekehrt enthält das Datenträgerabbild des NAS-Datenspeichers sehr viele Dateien zwischen 1 und 10 MB. Dies liegt

daran, dass von den 46.215 Dateien ungefähr 30.000 Dateien Fotos sind. Diese wiederum sind für gewöhnlich 500 Kilobyte bis 10 Megabyte groß. Die Kurve könnte allerdings anders aussehen, wenn beispielsweise auch Filme und Videos auf dem NAS gespeichert wären.

Die nachfolgende Abbildung 4.9 und die Abbildung 4.10 zeigen die absolute und relativierte kumulative Kategoriegröße der einzelnen Kategorien an. Die Kategoriegröße beschreibt die Gesamtgröße aller Dateien einer spezifischen Kategorie. Beispielsweise sind bei dem Windows System ungefähr 90 Gigabyte der Gesamtdatengröße in Dateien kleiner 10 Megabyte gespeichert.

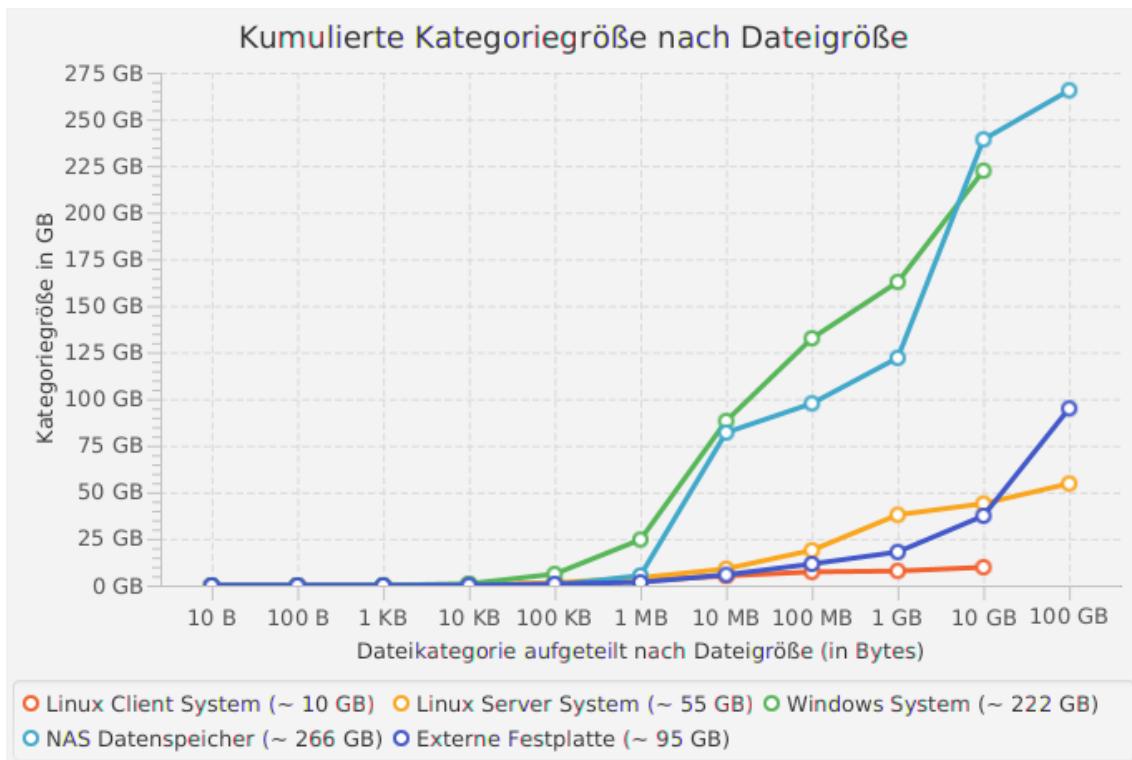


Abbildung 4.9: Kumulierte Kategoriegröße nach Dateigröße

Die relativierte kumulative Kategoriegröße in Abbildung 4.10 verdeutlicht den Kontrast in Bezug auf die relativierte kumulative Häufigkeit aus Abbildung 4.8. Während mehr als 95% aller Dateien kleiner 10 Megabyte sind, beansprucht dieser Anteil doch nur ungefähr 10-55 % der Gesamtspeichergröße.

Anhand der Diagramme empfiehlt es sich den Grenzwert der Dateigröße zwischen 1 und 10 Megabyte zu definieren. Für die Implementierung im Rahmen der Thesis wird der Grenzwert für die forensische Analyseplattform auf 10 Megabyte gesetzt. Dies bedeutet, dass alle Dateien kleiner 10 Megabyte direkt in HBase gespeichert werden. Darunter fallen beispielsweise auch größtenteils Fotos und Dokumente. Nur die wenigen großen Dateien (größer 10 Megabyte) werden direkt im HDFS gespeichert.

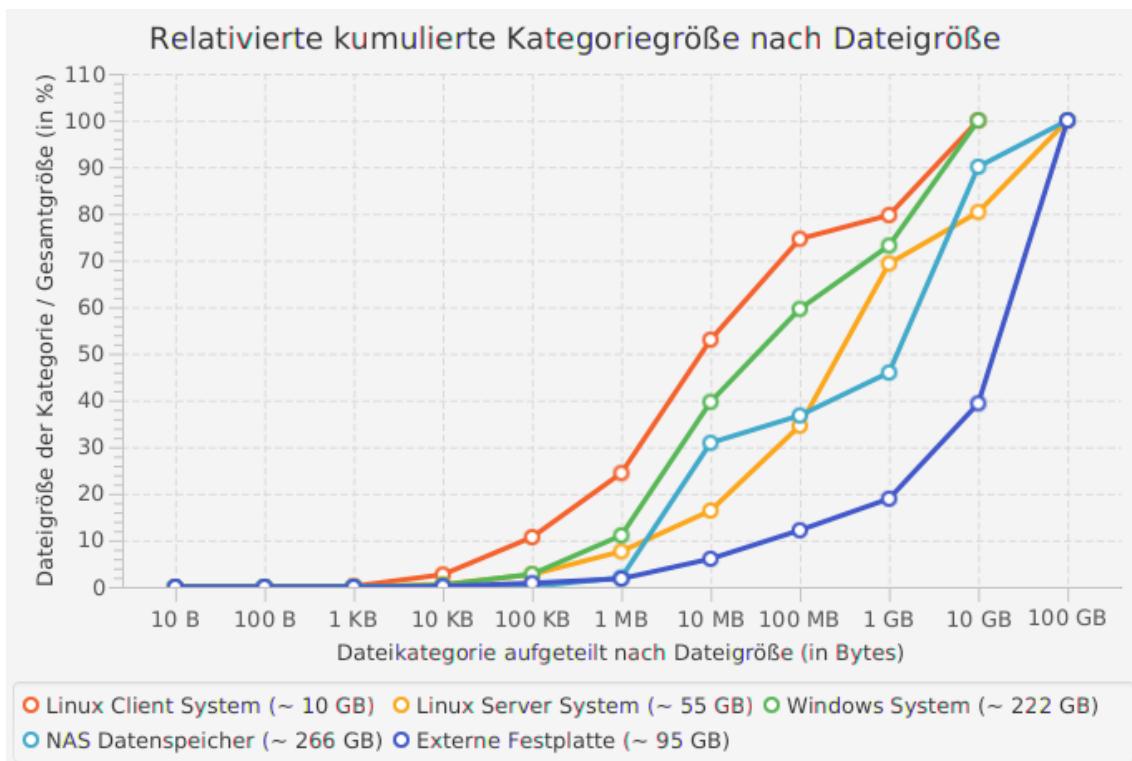


Abbildung 4.10: Relativierte kumulierte Kategoriegröße nach Dateigröße

4.7.3 Anwendungimplemtenierung

Die Variante zur Datenspeicherung im HDFS-Dateisystem und der HBase-Datenbank wird im Rahmen dieser Thesis implementiert. Das GitHub-Projekt *foam-data-import* enthält diese Anwendung.²⁹ Abbildung 4.11 skizziert die Datenaufbereitung und Speicherung in HBase und im HDFS.

Der Datenimport ist aufgeteilt in zwei Schritte. Der erste Schritt ist das Mounten des Datenträgerabbildes (siehe Abbildung 4.11). Darüber hinaus müssen die Zugriffsrechte geprüft werden. Die eigentliche Datenimport-Applikation sollte aus sicherheitstechnischen Gründen nicht mit erhöhten Privilegien ausgeführt werden. Daher müssen beim Mounten der Abbilder entsprechende Vorkehrungen getroffen werden. Dieser Vorgang des Mountens muss derzeit manuell mit Betriebssystemwerkzeugen durchgeführt werden. In Kapitel 4.7.6 wird detailliert beschrieben, wie die Zugriffsrechte berücksichtigt werden.

Im zweiten Schritt wird die Datenimport-Anwendung genutzt, um die Daten zu importieren. Die Applikation importiert ein vorgegebenes Verzeichnis. Dies kann entweder ein gemountetes Datenträgerabbild sein oder aber auch ein beliebiges logisches Verzeichnis.³⁰ Beim Importieren wird jede einzelne Datei des vorgegebenen Verzeichnisses analysiert. Es werden allgemeine Metadaten, wie Name, Größe, Zeitstempel, Zugriffsrechte und Dateityp ermittelt. Das Datenmodell wird detailliert in Kapitel 4.7.4 beschrieben.

²⁹Siehe Link: <https://github.com/jobusam/foam-data-import>. Letzter Zugriff: 6.10.2018.

³⁰Damit können, analog zu Autopsy, unterschiedliche Datenquellen importiert werden. Beispielsweise könnte dies ein gemountetes Datenträgerabbild, ein lokaler Datenträger oder einfach nur ein beliebiges Verzeichnis sein. Siehe Kapitel 4.2.

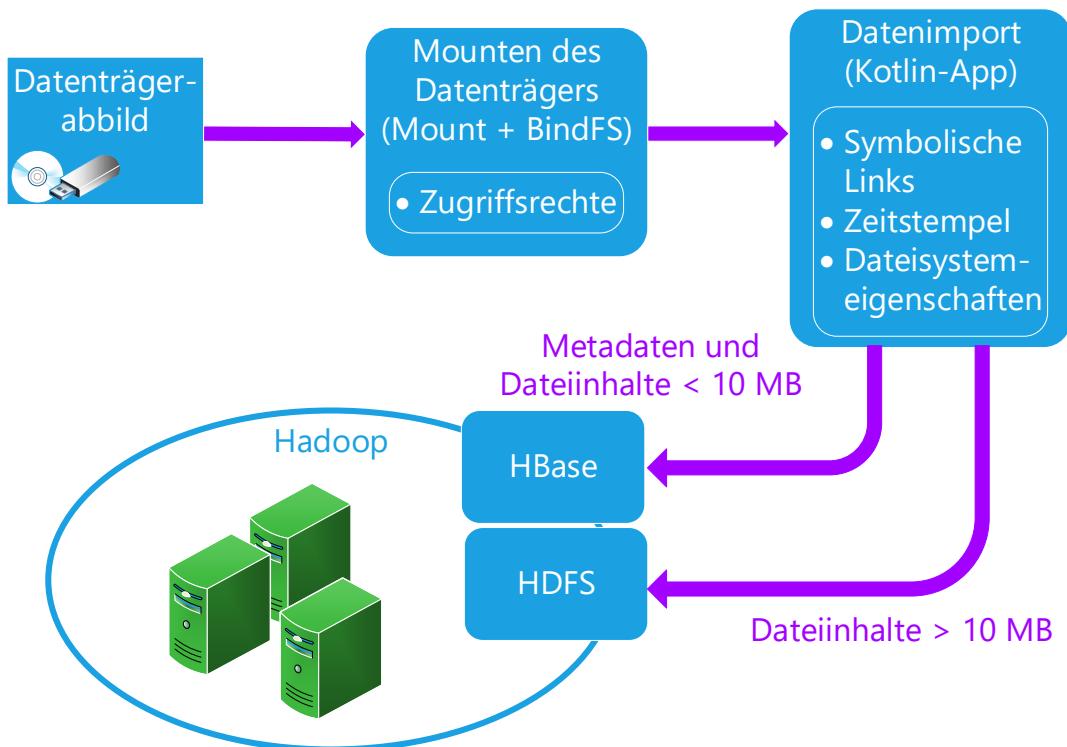


Abbildung 4.11: Datenimport in HBase und HDFS

Abhängig von dem Datentyp handelt es sich um ein Verzeichnis, eine Datendatei oder um eine spezielle Datei, wie beispielsweise einen symbolischen Link. Wenn es eine Datendatei ist, dann wird die Dateigröße geprüft. Ist die Datendatei größer als 10 MB dann wird sie direkt im HDFS unter einem vorher konfigurierten Dateipfad abgelegt. Ist die Datei kleiner oder gleich groß, dann wird sie zusammen mit den Metadaten in HBase gespeichert.

Die Applikation parallelisiert die Metadatenextraktion und den Datenversand über das Netzwerk. Dennoch kann es bei großen Datenträgern durchaus lange dauern, da hier auch die Bandbreite des Netzwerks und vor allem auch die Lesegeschwindigkeit des Datenträgers eine Rolle spielen. Befindet sich beispielsweise das zu importierende Verzeichnis auf einem herkömmlichen Festplattenlaufwerk mit Magnetscheiben, ist die Lesegeschwindigkeit und damit auch der Datenimport oftmals um ein Vielfaches geringer als der Import von einer *Solid State Disk (SSD)*.

Die Anwendung wird in *Kotlin* implementiert.³¹ Diese Sprache wurde zur Entwicklung der Datenimport-App gewählt, um die Vorteile von Java zu nutzen und gleichzeitig neue Sprachkonstrukte verwenden zu können. So ist die entwickelte Applikation interoperabel und kann unter mehreren Betriebssystemen ausgeführt werden. Es muss lediglich ein *Java Runtime Environment (JRE)* installiert sein. Auch die Anbindung zum HDFS und zu HBase kann einfach realisiert werden, da für beide Komponenten eine Java-Bibliothek bereitsteht. Letztlich ist es möglich, alle benötigten Dateisystemmetadaten auch mit Java und somit mit Kotlin auszulesen.

Zum Bauen der Anwendung wird *Gradle* genutzt. Dies ermöglicht eine einfache Handha-

³¹Siehe auch Kapitel 2.2 zum allgemeinen Entwicklungsvorgehen.

bung von Third-Party-Bibliotheken und deren Versionierung. Darüber hinaus kann mithilfe von Gradle der Quellcode auch ohne Entwicklungsumgebung schnell und einfach gebaut werden. Somit könnte ein forensischer Ermittler die aktuelle Version aus der Versionsverwaltung unter dem Link <https://github.com/jbusam/foam-data-import> herunterladen und mit Gradle bauen.

Das Build-Artefakt ist ein Dateiarchiv (ZIP/TAR). Es kann auf einem Analyserechner entpackt und ausgeführt werden. Der Datenimport wurde als Konsolenanwendung implementiert. Über mehrere Parameter kann der Import konfiguriert werden. Auf eine grafische Oberfläche wurde bewusst verzichtet. Durch die Ausführung als Konsolenanwendung kann das Programm auch sehr gut in andere Analyse-Skripte eingebettet werden.

Abbildung 4.12 zeigt hier die Hilfeseite und listet alle konfigurierbaren Parameter auf.³² Beschreibung der Parameter:

- Bei dem Datenimport muss mindestens das Verzeichnis (*Input Directory*) angegeben werden, welches importiert werden soll.
- Mit der Option *-o*, *--hdfsBaseDirectory* kann angegeben werden, in welches HDFS-Verzeichnis die Dateien gespeichert werden sollen.³³
- Die Option *-x*, *--hbaseSiteXml* gibt den Dateipfad zur Konfiguration von HBase an. Diese Datei kann von einem existierenden Hadoop-Cluster auf den lokalen Analyserechner kopiert werden und definiert eine Gruppe von ZooKeeper-Endpunkten (Hostname inklusive Port), damit über ZooKeeper die HBase-Instanzen ermittelt werden können.³⁴
- Die Option *-y*, *--hdfsCoreXml* gibt, analog zur HBase-Konfiguration, eine HDFS-Konfiguration des Computer-Clusters an. In dieser Konfiguration muss wiederum der Endpunkt zum HDFS definiert sein.³⁵
- Mit der Option *-c*, *--caseNumber* kann eine Fallnummer angegeben werden. Damit können mehrere Asservate zu einem bestimmten Fall zugeordnet werden (siehe Kapitel 4.7.4).
- Mit der Option *-d*, *--caseName* kann zusätzlich ein Fallname angegeben werden.
- Die Option *-e*, *--examiner* kann den Namen des forensischen Analysten enthalten. Aktuell muss kein Name angegeben werden. Allerdings wäre dies später für eine automatische Generierung eines Reports zur Beweismittelkette (*Chain of Custody*) sinnvoll.³⁶
- Mit der Option *-f*, *--exhibitname* kann zusätzlich ein Name des Asservats angegeben werden.

³²Die Interpretation der Parameter wurde mit der Kotlin-Bibliothek *CLI KT* durchgeführt. Siehe Link: <https://ajalt.github.io/clikt/index.html>. Letzter Zugriff: 24.8.2018.

³³Hierbei muss der aktuelle Nutzer des Analyserechners die Berechtigungen zum Schreiben in das angegebene HDFS-Verzeichnis besitzen.

³⁴In Kapitel B.1 im Anhang wird eine minimale Konfigurationsdatei dargestellt.

³⁵Siehe Kapitel B.1 im Anhang.

³⁶Diese Funktionalität wird im Rahmen der Thesis jedoch nicht implementiert.

```

Usage: forensicdataimport [OPTIONS] INPUTDIRECTORY

Options:
  -v, --verbose           enable verbose mode
  -o, --hdfsBaseDirectory VALUE
                        contains the base directory in HDFS where
                        large files will be stored. The default is
                        /data/
  -x, --hbaseSiteXml VALUE
                        contains file path to hbase-site.xml
                        configuration file. If not given use
                        localhost:2181 for connecting to Zookeeper
  -y, --hdfsCoreXml VALUE
                        contains file path to Hadoop core-site.xml
                        configuration file. If not given use default
                        hdfs uri hdfs://localhost:9000
  -c, --caseNumber INT
  -d, --caseName TEXT
  -e, --examiner TEXT
  -f, --exhibitName TEXT
  -h, --help               Show this message and exit

Arguments:
  INPUTDIRECTORY  contains the path to local source directory that shall be
                  imported into forensic analysis platform

```

Abbildung 4.12: Datenimport-Ausführung in der Konsole

Mit der gleichen Anwendung ist es auch möglich, alle bereits importierten Fälle und Asservate anzuzeigen. Zusätzlich können die Asservate gelöscht werden, falls die Daten nicht mehr benötigt werden. Dadurch wurde eine rudimentäre Fallverwaltung geschaffen.

4.7.4 Datenmodell

In Abbildung 4.13 wird das Datenmodell der forensischen Analyseplattform beschrieben. Dieses Modell wird in drei HBase-Tabellen aufgeteilt. Es zeigt die gespeicherten Metadaten und auch das Datenmodell der Fallverwaltung.

Die Fallverwaltung ist notwendig, um den Nutzern die Möglichkeit zu geben, mehrere Asservate (z.B. Datenträgerabbilder) in die forensische Analyseplattform zu importieren. Dies ist eine essentielle Voraussetzung, um Beziehungen zwischen den Asservaten identifizieren zu können. Ein Fall (*forensicCase*) besteht aus einer Fallnummer, einem Fallnamen und dem Namen des Auswerters. Die Fallnummer kann beim Datenimport als Parameter angegeben werden. Hierdurch kann der Analyst mehrere Asservate zu einem Fall importieren. Ein Fall kann daher auch mehrere Asservate (*forensicExhibit*) enthalten. Für diese Asservate kann wiederum ein beschreibender Name beim Import angegeben werden. Zusätzlich wird der Zeitpunkt beim Datenimport und das angegebene Basisverzeichnis im HDFS mit abgespeichert. Das Basisverzeichnis wird später bei der Datenverarbeitung ausgewertet, um die großen Dateien im HDFS lokalisieren zu können.

Ein Asservat kann wiederum mehrere Daten (*forensicData*) enthalten. Dies sind die einzelnen Dateien und ihre Metadaten. Hierbei hat jeder Eintrag eine eindeutige Id, welche als Zeilenschlüssel in HBase genutzt wird.³⁷ Das Attribut *filePath* enthält den vollständigen Dateipfad inklusive Dateinamen. Im Attribut *fileType* wird gespeichert, ob es sich

³⁷In Abbildung 4.13 sind diese Zeilenschlüssel dunkelblau hinterlegt.

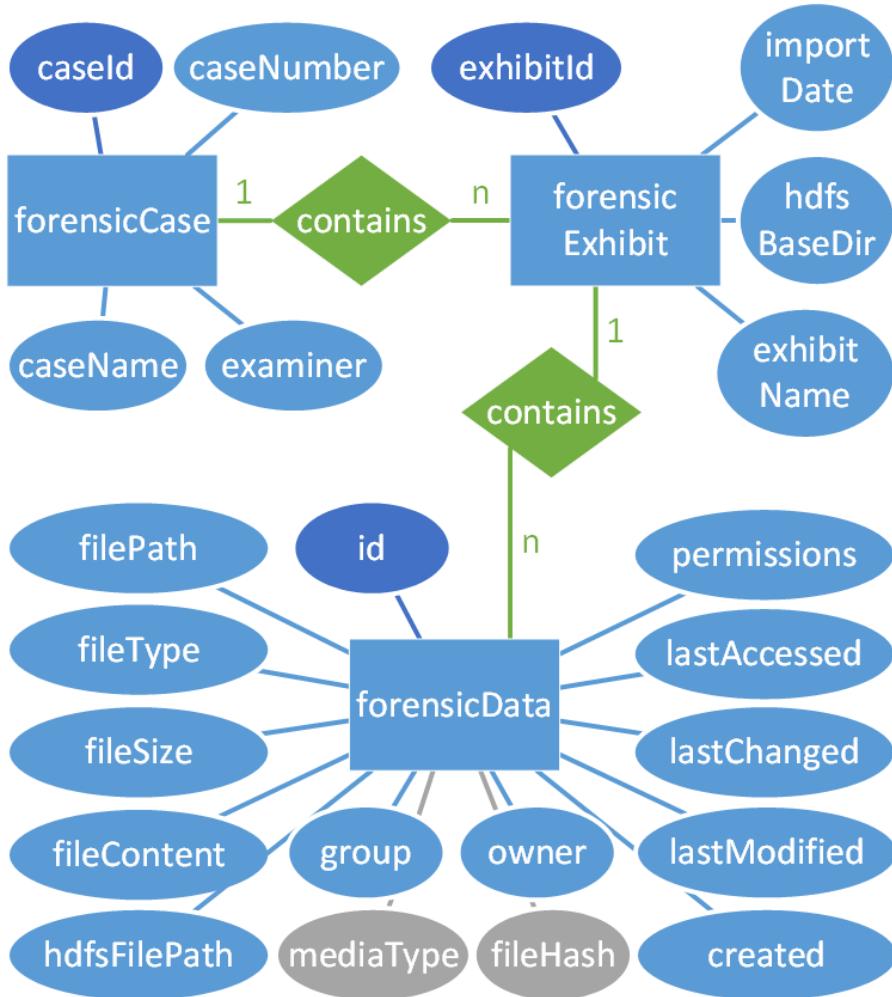


Abbildung 4.13: Datenmodell der forensischen Analyseplattform

um eine Datendatei, ein Verzeichnis, einen symbolischen Link oder um einen anderen Dateityp handelt. Abhängig von der Dateigröße, wird bei kleinen Dateien der Dateinhalt direkt in dem Attribut *fileContent* gespeichert. Bei großen Dateien hingegen, wird nur im Attribut *hdfsFilePath* auf den Dateipfad im HDFS referenziert, wo die Datei gespeichert wird. Der Dateipfad im HDFS hingegen ist eine Kombination aus dem angegebenen *hdfsBaseDir* und dem Zeilenschlüssel (*id*) des Dateneintrags. Dadurch ist es auch möglich, über eine Datendatei im HDFS, die passenden Metadaten in HBase zu identifizieren. Denn der Zeilenschlüssel in der HBase-Tabelle *forensicData* ist innerhalb der forensischen Analyseplattform eindeutig.

Des Weiteren werden noch die Zugriffsrechte, die Besitzer, die Gruppe und die Zeitstempel abgespeichert. Je nach spezifischem Dateisystem des Asservats, sind allerdings nicht immer alle Metadaten vorhanden.

Bei der anschließenden Datenverarbeitung in Kapitel 5 wird das bestehende Datenmodell um neue Metadaten erweitert.³⁸

³⁸Hierzu gehören die Attribute *mediaType* und *fileHash*, welche in Abbild 4.13 grau hinterlegt sind.

4.7.5 Datenspezifische Aspekte

Bei der Implementierung des Datenimports müssen auch datenspezifische Aspekte berücksichtigt werden. Wie bereits erwähnt, werden die Daten auf logischer Dateiebene in das Hadoop-System importiert. Hierbei müssen spezielle Dateitypen berücksichtigt werden. Ein Beispiel ist die Verarbeitung von symbolischen Links, welche gerade unter Linux-basierten Betriebssystemen, beziehungsweise in der ext-Dateisystemfamilie, auftreten können. Denn wenn symbolische Links in einem Dateisystem gespeichert werden und letzteres im Analysestesystem gemountet wird, so können diese Links auch auf Dateien außerhalb des Dateisystems verweisen. Denn letztlich interpretiert das Betriebssystem die symbolischen Links. Bei der forensischen Analyse könnte diese Interpretation aber zu schwerwiegenden Fehlern in den Analyseergebnissen führen, wenn Inhalte des Analyserechners verarbeitet werden, welche ursprünglich nicht auf dem Asservat vorhanden waren. Daher muss beim Import geprüft werden, ob die Datei einem symbolischen Link entspricht. Ist dies der Fall, darf der symbolische Link nur innerhalb des Asservats interpretiert werden.³⁹

Auch beim NTFS-Dateisystem, welches vorzugsweise bei Windows genutzt wird, existieren spezielle Eigenschaften. Bei NTFS ist es möglich, an Datendateien und sogar an Verzeichnissen sogenannte *Alternate Data Streams* anzuhängen. Diese können, wie jede andere Datei, beliebige Binärdaten enthalten.⁴⁰

Ein weiterer Punkt sind auch die Zeitstempel. Das System kann die Zeitstempel zur Erstellung einer Datei (*created*), zur letzten Modifikation einer Datei (*lastModified*), zur letzten Modifikation der Metadaten einer Datei (*lastChanged*) und zum letzten Lesezugriff einer Datei (*lastAccessed*) speichern. Es hängt aber von dem genutzten Dateisystem und von dem Betriebssystem ab, welche Zeitstempel überhaupt geschrieben werden. Beispielsweise wird der letzte Lesezugriff auf eine Datei, nicht immer vom Betriebssystem protokolliert. Derzeit liest die Datenimport-Anwendung diese Zeitstempel aus, falls sie vorhanden sind.

Analog zu diesen beschriebenen Fällen, gibt es noch weitere dateisystemspezifische Eigenschaften, welche beim Datenimport und zukünftigen Weiterentwicklungen berücksichtigt werden sollten.

4.7.6 Zugriffs- und Ausführungsrechte

Die Beschränkung der Dateizugriffe auf Basis der vorgegebenen Zugriffsrechte muss beim Import betrachtet werden. Wie in Abbildung 4.11 in Kapitel 4.7.3 beschrieben ist, wird das Datenträgerabbild, beziehungsweise das Asservat, zuerst auf dem Analyserechner gemountet. Unter Linux kann dies normalerweise nur mit erhöhten Administratorrechten (root) durchgeführt werden. Der forensische Analyst benötigt also zumindest auf seinem Analyserechner privilegierte Ausführungsrechte. Hier unterscheidet sich beispielsweise die Referenzanalysesoftware *Autopsy* von dieser forensischen Analyseplattform. Denn bei Autopsy unter Windows, wird das Dateisystem auf Anwendungsebene direkt mit der Software analysiert. Das Betriebssystem muss das Dateisystem nicht mounten und der Nutzer benötigt daher auch keine besonderen Systemprivilegien.

³⁹Derzeit werden logische Links in das System importiert. Jedoch wird ihre Referenz beim Import nicht interpretiert. Dies wäre bei einer Weiterentwicklung des Systems durchaus sinnvoll.

⁴⁰Auch diese Eigenschaften werden im Rahmen dieser Thesis noch nicht beim Datenimport berücksichtigt.

Beim Import von Dateien, auf einem gemounteten Dateisystem des Datenträgerabbildes, sind jedoch die Dateizugriffsrechte weitaus interessanter. Denn das Betriebssystem des Analyserechners berücksichtigt diese Zugriffsrechte. Während diese Problematik bei NTFS-Dateisystemen eine untergeordnete Rolle spielt, so werden hingegen bei ext-Dateisystemen die Unix-Dateirechte gespeichert und auch auf dem Analysesystem interpretiert. Daher kann der Nutzer und dessen ausgeführte Programme, welche die Daten aus dem Dateisystem auslesen, nicht in allen Fällen auf alle Dateien zugreifen.

Die einfachste Möglichkeit, um die Problematik der Zugriffsrechte zu umgehen, wäre das Ausführen der Datenimport-Applikation mit Root-Rechten. Andererseits soll die Applikation nicht mit Root-Rechten ausgestattet werden, da dies im Fehlerfall zu unvorhergesehenen Rechteausweiterungen führen kann und damit ein Sicherheitsrisiko für die Systemintegrität darstellt. Darüber hinaus kann bei einem Fehlverhalten der Anwendung das Analysesystem beschädigt werden. Letztlich braucht die Anwendung zum Datenimport nur die Berechtigung zum Lesen von Dateien für das gemountete Verzeichnis, unabhängig von dessen Besitzer und seinen Zugriffsrechten.

Beim Mounten des Dateisystems müsste dem Betriebssystem mitgeteilt werden, dass die Dateirechte des gemounteten Dateisystems ignoriert werden sollen. Diese Option existiert aber nicht.⁴¹

Eine weitere Alternative wäre die Nutzung von Access Control Lists (ACLs), um dem nichtprivilegierten Nutzer Rechte zum Lesen der Dateien zu geben. Hierzu müsste die Datenträgerkopie schreibend gemountet werden, damit die Rechte jeder Datei angepasst werden können. Dies würde wiederum dazu führen, dass das Datenträgerabbild als sicher gestelltes Asservat geändert werden würde. Daher ist diese Lösung auch nicht geeignet.

Eine andere Alternative ist die Nutzung von Posix Capabilities.⁴² Diese Variante ist prinzipiell unter CentOS/Fedora möglich. Zum lesenden Zugriff auf Dateien, muss die Posix Capability *CAP_DAC_READ_SEARCH* gesetzt werden.

Mit nachfolgenden Kommando kann diese Capability für das Analyseprogramm gesetzt werden. Damit kann theoretisch auch ein nicht-privilegierter Nutzer lesenden Zugriff auf privilegierte Dateien erhalten.

```
1 setcap CAP_DAC_READ_SEARCH /bin/data.import
```

Listing 4.3: Befehl zum Setzen von Posix Capabilities

Diese Alternative funktioniert primär bei Binärprogrammen, jedoch nicht bei Shell-Skripten oder Java-Anwendungen.

Eine ähnliche Alternative zu den Posix Capabilities ist das Setzen des SUID-Bits als Unix-Dateirecht für die Programmdatei. Aber auch diese Möglichkeit funktioniert nur bei Binärprogrammen und nicht für interpretierte Skripte oder Java-Anwendungen, die wiederum in der Java Virtual Machine ausgeführt werden.

⁴¹Zumindest konnte keine funktionierende Variante gefunden werden. Siehe Man-Page des Mount-Befehls (geprüft unter Fedora 28).

⁴²Siehe Linux Man-Page mit folgendem Befehl: *man 7 capabilities*.

Zuletzt gibt es noch eine Variante, welche die Problematik mit den Dateirechten lösen kann. Mit dem Projekt *bindfs*⁴³ können unter Linux Dateisystemverzeichnisse neu gemountet werden und ihre Zugriffsrechte verändert werden. Der nachfolgende Befehl mountet das existierende Verzeichnis mit den enthaltenen Dateien in einem neuen Verzeichnis und setzt bei jeder Datei die aktuelle Id des Nutzers als Datei-Owner und Group.

```
1 sudo bindfs -u $(id -u) -g $(id -g) src_dir/ target_dir/
```

Listing 4.4: Nutzung von Bindfs zum Ändern von Dateirechten

Zur Ausführung des Befehls werden Root-Rechte benötigt. Der Nutzer kann danach alle Dateien des Zielverzeichnisses lesen. Das originale Datenträgerabbild wird nicht verändert. Der einzige Nachteil an dieser Lösung ist, dass der Besitzer und die Gruppe jeder einzelnen Datei im neu gemounteten Verzeichnis nun von dem Nutzer des Analysesystems überschrieben wurde. Dies bedeutet, dass die Attribute *Owner* und *Group* im Datenmodell der forensischen Analyseplattform derzeit nicht korrekt sind und daher auch nicht zur Datenverarbeitung genutzt werden können. Dieser Nachteil muss zukünftig behoben werden, damit die forensische Analyseplattform auch die Besitzer und Gruppen einer Datei korrekt auswerten kann. Beispielsweise könnte untersucht werden, ob die Implementierung von BindFS modifiziert werden kann, um den ursprünglichen Nutzer und die Gruppe möglicherweise als erweiterte Dateiattribute zu speichern. Diese erweiterten Dateiattribute könnten dann wieder beim Datenimport ausgelesen werden.

Alternativ könnte nach weiteren Möglichkeiten gesucht werden, wie dem Betriebssystem mitgeteilt werden kann, die Dateirechte für bestimmte gemountete Datenträger bei einem lesenden Zugriff zu ignorieren.

4.8 Fazit

Die vierte Variante überzeugt durch eine einfache Lösung zur Speicherung von vielen kleinen und großen Dateien. Darüber hinaus kann mithilfe der HBase-Datenbank auch eine kleine Fallverwaltung implementiert werden, um mehrere Asservate eines Falls zu importieren.

Die prototypische Implementierung bestätigt die Machbarkeit zur Speicherung von großen semistrukturierten Datensätzen durch eine Kombination der Speicherung im HDFS und HBase. Aufbauend auf dieser Implementierung und dem dargestellten Datenmodell können im nächsten Schritt, der Datenverarbeitung, weitere Informationen aus den Daten gewonnen werden.

⁴³Siehe Link: <https://bindfs.org/>. Letzter Zugriff: 21.7.2018.

5 Datenverarbeitung

5.1 Klassisches Analysevorgehen

In Kapitel 4.2 wird beschrieben, wie bei der Open-Source Software *Autopsy* ein Fall angelegt und Datenträgerabbilder hinzugefügt werden können. Schon beim Importieren einer Datenquelle können diverse Module zur automatisierten Datenaufbereitung aktiviert werden. Dies entspricht der dritten Phase, dem *Sichten und Aufbereiten*, aus dem allgemeinen forensischen Analyseprozess.¹ Diese Module werden nachfolgend beschrieben, um einen Vergleich zur hier entwickelten forensischen Analyseplattform zu ermöglichen. Abbildung 5.1 zeigt die verfügbaren Module.

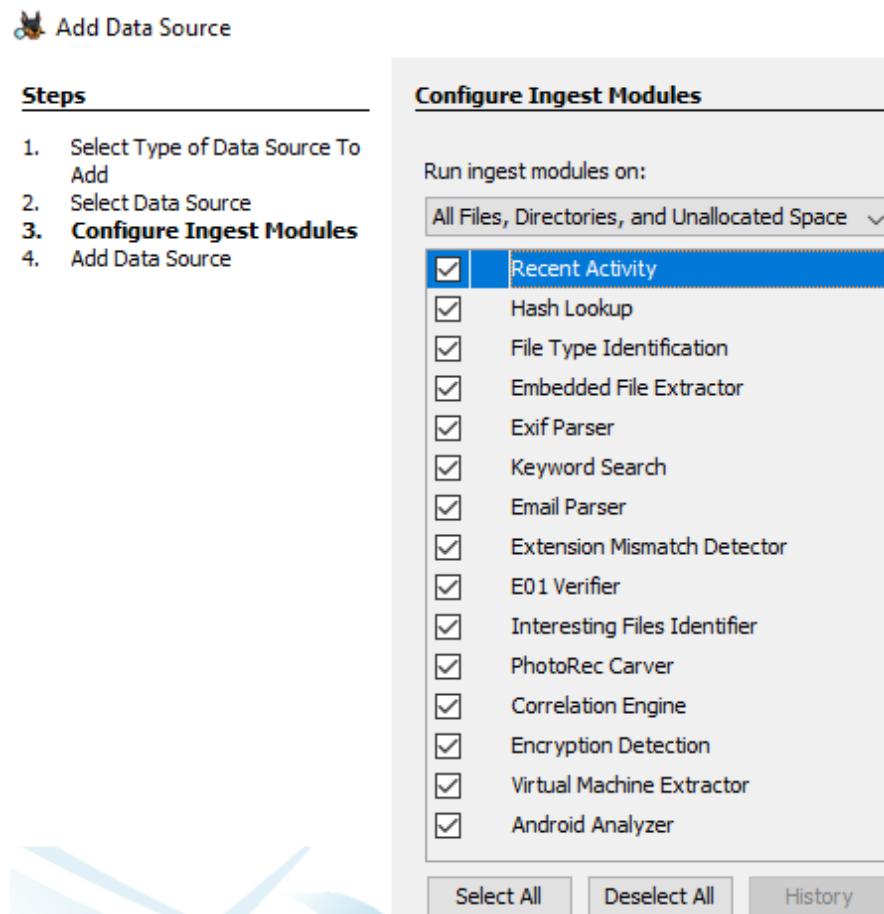


Abbildung 5.1: Module zur automatischen Datenverarbeitung bei Autopsy

¹Siehe Abbildung 4.1 in Kapitel 4.1.

Nachfolgend werden die Module kurz beschrieben und mit der Funktionalität der hier entwickelten forensischen Analyseplattform verglichen. Zuerst werden die Module aufgelistet, welche ganz oder teilweise in der forensischen Analyseplattform implementiert sind.²

- Das *File Type Identification Modul* ermöglicht die Ermittlung von Medientypen und Dateiformaten, wie beispielsweise *JPEG*-Bilder. Autopsy nutzt hier die Open-Source Bibliothek Apache TikaTM. Eine gleichwertige Funktionalität ist auch in der forensischen Analyseplattform vorhanden.³
- Das *Correlation Engine Modul* bietet die Möglichkeit, mehrere Fälle und ihre Datenquellen miteinander zu verknüpfen, um Beziehungen untereinander zu erkennen. Analog hierzu bietet auch die forensische Analyseplattform, mit dem Auffinden von Datei-Duplikaten, eine einfache Funktion, um Beziehungen zwischen mehreren Fällen und deren Asservate herzustellen.⁴
- Das *Keyword Search Modul* enthält eine Schlüsselwortsuche. Hierzu werden Dateien mithilfe von Apache Solr indiziert. Darüber hinaus kann, basierend auf regulären Ausdrücken, nach bestimmten Strukturen, wie beispielsweise E-Mail- oder Web-Adressen, gesucht werden. Die hier entwickelte Analyseplattform implementiert auch eine Textsuche auf Basis von Apache Solr. Derzeit ist es allerdings noch nicht möglich, ganze Dateiinhalte zu indexieren.⁵

Nachfolgend werden die Module von Autopsy aufgelistet, welche noch nicht in der forensischen Analyseplattform vorhanden sind und in Weiterentwicklungen der Plattform implementiert werden können.

- Das *Recent Activity Modul* ermittelt anhand der Zeitstempel alle interessanten Tätigkeiten der letzten 7 Tage, wie zum Beispiel besuchte Websites von diversen Browsern.
- Das *Hash Lookup Modul* vergleicht die Datei-Hashsummen mit bereits bekannten Hashsummen. Damit können bekannte Betriebssystemdateien schnell gefiltert werden. Analog zu einem VirensScanner kann dadurch auch bekannte bösartige Malware gefunden werden.
- Das *Embedded File Extractor Modul* entpackt Dateiarchive, wie beispielsweise *ZIP*-Dateien.
- Das *Exif Parser Modul* wertet die sogenannten *EXIF*-Metadaten aus, welche in *JPEG*-Bilddateien enthalten sind. In der forensischen Analyseplattform kann diese Funktionalität auch mit Apache Tika implementiert werden.
- Das *Email Parser Modul* extrahiert E-Mails aus diversen E-Mail Archiven, wie beispielsweise dem *PST*-Dateiformat, welches von Microsoft Outlook genutzt wird.
- Das *Extension Mismatch Detector Modul* ermittelt Dateien, deren Dateiendung nicht zum analysierten Medientyp des Dateiinhalts passen. Dieser Unterschied kann auf versteckte Dateien hinweisen. Eine ähnliche Funktion kann in der forensischen Analyseplattform über die Volltextsuche implementiert werden, da die Dateiendung und der Medientyp bekannt sind.

²Siehe Link: <http://sleuthkit.org/autopsy/docs/user-docs/4.3/>. Letzter Zugriff: 09.08.2018.

³Siehe Kapitel 5.3.3.

⁴Siehe Kapitel 5.3.2.

⁵Siehe Kapitel 5.3.4.

- Das *E01 Verifier Modul* verifiziert, speziell für das forensische Analyseformat *E01*, die Dateiprüfsummen mit den gespeicherten Prüfsummen. Damit können Änderungen an einem sichergestellten Asservat identifiziert werden.
- Das *Interesting Files Identifier Modul* identifiziert interessante Dateien, welche vorher durch bestimmte Suchkriterien, wie beispielsweise Dateinamen und Datentypen, definiert wurden.
- Das *PhotoRec Carver Modul* ermöglicht das bereits beschriebene File Carving auf ungenutzten Speicherbereichen. Diese Funktionalität wird nicht von der forensischen Analyseplattform unterstützt, da ungenutzte Speicherbereiche aus den originalen Datenträgerabbildern nicht in das Analysesystem importiert werden.
- Das *Encryption Detection Modul* ermöglicht das Auffinden von verschlüsselten Containern. Hierbei wird nach Dateien gesucht, deren Inhalt eine hohe Entropie aufweisen.⁶
- Das *Virtual Machine Extractor Modul* kann Dateien aus Systemabbildern von virtuellen Maschinen extrahieren, welche im Asservat gespeichert sind.
- Das *Android Analyzer Modul* ermöglicht das Extrahieren von bestimmten Informationen aus spezifischen Dateien des Android-Betriebssystems. So können beispielsweise Kontaktdaten und Nachrichten aus spezifischen SQLite-Datenbanken ermittelt werden.

Nachdem die benötigten Module in Autopsy aktiviert und nach fallspezifischen Eigenschaften konfiguriert wurden, erfolgt die Datenaufbereitung im Hintergrund. Parallel hierzu kann der Analyst bereits die Rohdaten analysieren.⁷

5.2 Umsetzung in der forensischen Analyseplattform

Zur Datenverarbeitung in der forensischen Analyseplattform wird Apache SparkTM genutzt. Der physikalische Aufbau wird im Grundlagenkapitel 3.4 behandelt. In diesem Kapitel wird die Implementierung der Datenverarbeitung betrachtet.

Bei Apache Spark (Version 2.3.0) gibt es diverse Programmierschnittstellen (APIs), wie Daten geladen werden können. Es besteht die Möglichkeit, Daten mithilfe von *Resilient Distributed Datasets (RDDs)* zu laden und zu verarbeiten. Aufbauend auf diesen RDDs können die Daten konvertiert, gefiltert oder aggregiert werden. Listing 5.1 zeigt ein simples Beispiel zur Nutzung dieser RDDs, um alle Wörter aus einer Beispieldatei `history.txt` und deren Vorkommen aufzulisten. Die Implementierung kann, abhängig von der Dateigröße und der Konfiguration von Spark, verteilt auf mehreren Knoten ausgeführt werden, um die Datenverarbeitung zu beschleunigen. Die Daten werden aus dem HDFS gelesen und dort gespeichert.

⁶In der Informationstechnik beschreibt die Entropie ein Maß zur Bestimmung des mittleren Informationsgehalts pro Zeichen.

⁷Siehe Kapitel 6 zur Visualisierung von Daten.

```

1 //Datei aus dem HDFS lesen
2 JavaRDD<String> textFile = sc.textFile("hdfs://data/history.txt");
3 JavaPairRDD<String, Integer> counts = textFile
4     // Text separieren
5     .flatMap(s -> Arrays.asList(s.split(" ")).iterator())
6     // Wortvorkommen ermitteln
7     .mapToPair(word -> new Tuple2<>(word, 1))
8     .reduceByKey((a, b) -> a + b);
9 // Ergebnis in HDFS speichern
10 counts.saveAsTextFile("hdfs://...");
```

Listing 5.1: Beispielimplementierung eines Spark RDDs

Bei der Weiterentwicklung von Spark sind in neueren Versionen sogenannte *DataFrames* und *DataSets* hinzugekommen. Diese Datenstrukturen beschreiben eine Schnittstelle, welche der Sichtweise von Tabellen ähnelt. Die Implementierung dieser Typen nutzt wiederum die bereits beschriebenen RDDs.

Welche Datenstrukturen für die Anwendungsfälle von der forensischen Analyseplattform genutzt werden sollten, hängt primär von der Art der Daten ab. *DataFrames* und *DataSets* sind optimiert für strukturierte und semi-strukturierte Daten. Diese Daten lassen sich beispielsweise in Tabellenstrukturen einlesen und verarbeiten. Es gibt komplexe Operationen auf diesen Tabellen, welche dem klassischen SQL Syntax sehr nahe kommen. Apache Spark kann bei der Nutzung von *DataFrames* und *DataSets* viele Optimierungen bei der Ausführung und Verarbeitung durchführen. Andererseits sind diese Strukturen ungeeignet bei unstrukturierten Daten, wie beispielsweise Multimediateien und beliebigen Dateien im Allgemeinen.[15, S. 66 ff.]

Wie beim Datenimport schon beschrieben, sind die Metadaten der analysierten Datenträger strukturiert, beziehungsweise semi-strukturiert, in HBase abgespeichert. Prinzipiell wäre es also möglich, auch mit *DataSets* und *DataFrames* auf diese Daten zuzugreifen. Letztlich kommt es aber auf die Anbindung zwischen Apache Spark und Apache HBase an. Es existieren zwei unterschiedliche Connectoren.⁸ Der *Hortonworks SHC Connector* ermöglicht die Interaktion mit Daten in HBase und nutzt dafür die *DataFrame*/*DataSet* Datenstrukturen.⁹

Als Pendant existiert ein weiterer *HBase-Spark Connector* auf Basis von RDDs. Letzterer wird im Rahmen dieser Thesis genutzt, um Daten von HBase zu lesen und zu schreiben.¹⁰ Daher wird die Datenverarbeitung mithilfe von Spark RDDs implementiert. Auch beim Auslesen von großen Dateien aus dem HDFS, werden Spark RDDs verwendet, da Spark eine passende Schnittstelle zum HDFS auf Basis von RDDs anbietet.

⁸Bei Apache Spark sind Connectoren eine Art von Bibliotheken, welche es ermöglichen im Ausführungs-kontext auf andere Systeme, wie beispielsweise Datenbanken oder Dateisysteme, zuzugreifen.

⁹Siehe Link: <https://github.com/hortonworks-spark/shc>. Letzter Zugriff: 15.8.2018.

¹⁰Siehe Link: <https://github.com/apache/hbase/tree/master/hbase-spark> (Letzter Zugriff: 15.8.2018) und dessen Nutzung im Projekt *foam-processing-spark* unter dem Link: <https://github.com/jobusam/foam-processing-spark> (Letzter Zugriff: 25.9.2018).

5.3 Anwendungsfälle der Datenverarbeitung

5.3.1 Berechnung von Hashsummen

Eine grundlegende Funktionalität einer forensischen Analysesoftware ist die Berechnung von Hashsummen, um die Integrität fallrelevanter Dateien für zukünftige Analysen prüfen zu können. Darüber hinaus können auf Basis der Hashsummen sehr einfach Duplikate erkannt werden (siehe Kapitel 5.3.2).

In der derzeitigen Implementierung wird der *SHA-512* Algorithmus genutzt, um eindeutige und kryptografisch sichere Hashsummen zu berechnen. Bei Autopsy hingegen werden *MD5*-Hashsummen berechnet. Der MD5-Algorithmus gilt mittlerweile jedoch als kryptografisch unsicher, da Hash-Kollisionen in wenigen Stunden berechnet werden können.[20, S. 240-243]

Abbildung 5.2 verdeutlicht den Datenfluss bei der Ermittlung von Hashsummen.

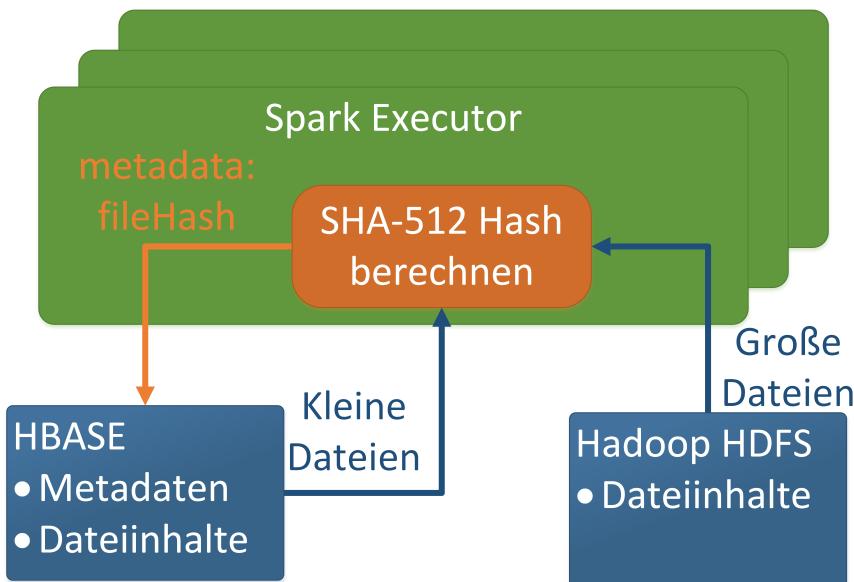


Abbildung 5.2: Datenfluss bei der Berechnung von Hashsummen

Die Datenverarbeitung von kleinen Dateien aus HBase und großen Dateien aus dem HDFS wird unabhängig voneinander in eigenen Spark-RDDs ausgeführt. Aufgrund der unterschiedlichen Datenquellen existieren auch zwei unterschiedliche Datentypen zum Auslesen der Dateiinhalte. Daher wird die Prozessierung in getrennten Tasks innerhalb der Spark Executoren ausgeführt. Um dann später die Hashsumme einer großen Datei aus dem HDFS in dem dazugehörigen Eintrag in HBase abzuspeichern, ist es notwendig den Zeilenschlüssel des Eintrags in HBase als Dateiname im HDFS zu verwenden. Dadurch können die Dateien aus dem HDFS einem Eintrag in HBase zugeordnet werden. Der ermittelte Hashwert wird darauf in der Spalte *metadata:fileHash* in HBase gespeichert.¹¹

5.3.2 Erkennung von Duplikaten

Aufbauend auf der Berechnung von Hashsummen, können nun auch Datei-Duplikate ermittelt werden. Dadurch ist es möglich, Beziehungen zwischen mehreren Asservaten herzustellen, wenn gleiche Dateien gefunden werden. Derzeit werden diese Ergebnisse aber nur

¹¹Siehe auch HBase-Datenmodell in Abbildung 4.13.

als Text im HDFS abgespeichert. In einer Weiterentwicklung könnten diese Informationen sehr gut in einer Graphendatenbank, wie beispielsweise *Neo4j*, abgespeichert werden. Hierdurch wäre visuell sehr schnell sichtbar, welche Beziehungen zwischen den Asservaten bestehen.

In diesem Kontext ist es auch sinnvoll, zwischen technischen Betriebssystemdateien und Nutzerdateien zu unterscheiden. Denn wenn zwei Asservate das gleiche Betriebssystem enthalten, existieren auch zugleich tausende Datei-Duplikate. Gerade für Nutzerdaten, wie beispielsweise Bilder, Dokumente und Videos, ist die Erkennung von Duplikaten interessant. Daran könnte später ermittelt werden, wie beispielsweise urheberrechtlich geschütztes Material über mehrere Systeme verbreitet wurde.

Ein anderer Aspekt, welcher in einer Weiterentwicklung der Plattform implementiert werden könnte, ist der Vergleich mit bekannten Hashsummen von existierenden Datensätzen. Dies wird bei Autopsy verwendet, um gegebenenfalls Malware zu erkennen oder automatisiert nach spezifischen Dateien zu suchen. Ein Beispiel hierzu ist die sogenannte *National Software Reference Library*, welche Hashsummen von bekannten Betriebssystem- und Anwendungsdateien enthält. Diese haben oftmals keinen forensischen Analysewert und können aus der Datenverarbeitung gefiltert werden.¹² [16, S. 36]

5.3.3 Ermittlung von Medientypen

Das Erkennen von Medientypen ist ein elementarer Bestandteil bei der Datenanalyse. Autopsy nutzt hierbei die Open-Source Bibliothek Apache TikaTM. Dieses Projekt wird auch in der forensischen Analyseplattform genutzt und ermittelt die Dateitypen anhand des Dateiinhalts und der gegebenen Dateiendung.

Abbildung 5.3 zeigt den Datenfluss bei der Ermittlung der Medientypen.

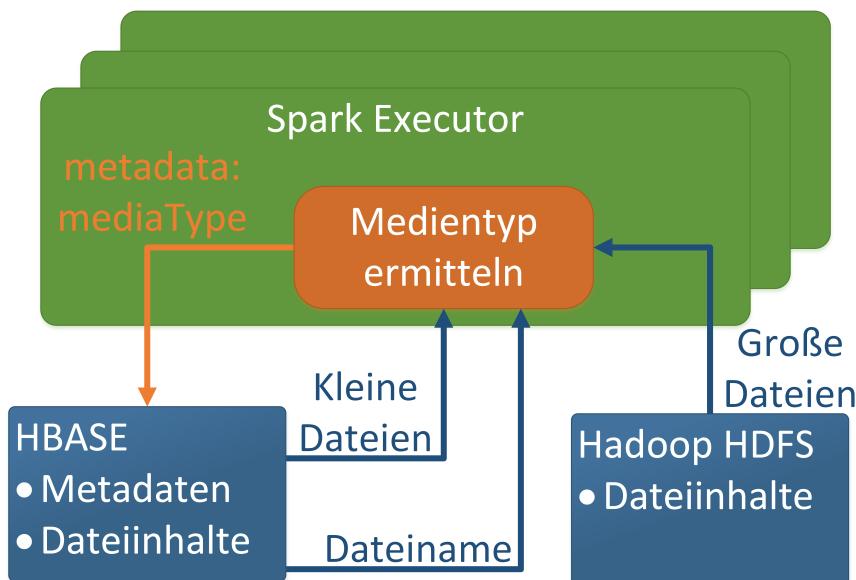


Abbildung 5.3: Datenfluss bei der Ermittlung von Medientypen

¹²Siehe Link: <https://www.nist.gov/itl/ssd/software-quality-group/nsrl-download/current-sets-hash-sets>. Letzter Zugriff: 9.9.2018.

Prinzipiell kann Apache Tika den Medientyp auch nur anhand der Dateiendung oder anhand des Dateiinhalts erkennen. Wird allerdings nur die Dateiendung angegeben, so können beispielsweise Bilddateien mit gefälschter Dateiendung nicht korrekt erkannt werden. Wird hingegen nur der Dateiinhalt angegeben, so prüft Tika formatspezifische Bytesequenzen, welche oftmals am Dateianfang stehen. Bei Textdateien hingegen kann es nur identifizieren, dass es sich um eine Textdatei handeln könnte. Gerade bei Textdateien ist es sinnvoll, die Dateiendung in die Analyse mit aufzunehmen, um ein genaueres Ergebnis zu erhalten. Dadurch kann Tika beispielsweise ermitteln, ob es sich um eine CSV-Datei oder eine HTML-Datei handelt. Allerdings sollten diese Ergebnisse kritisch hinterfragt werden. Wie bereits erwähnt, könnte eine gefälschte Dateiendung bei Textdateien zu einem falschen Ergebnis führen.

Das Ermitteln der Medientypen ist für die Datenvisualisierung sehr nützlich, da damit nach allen vorhandenen Bildern oder Videos gesucht werden kann.¹³

5.3.4 Volltextsuche und Datenindexierung

Um auf die Daten in der forensischen Analyseplattform einfach zugreifen zu können, wäre eine Volltextsuche sinnvoll. Diese sollte performant arbeiten, damit Ergebnisse zu Suchanfragen von beliebigen Schlüsselwörtern in Realzeit angezeigt werden können. Um dies zu ermöglichen, können die Dateiinhalte und Metadaten indexiert werden.

Es gibt hierzu zwei Open-Source Projekte, die eine Datenindexierung anbieten. Dies sind *Apache SolrTM* und *ElasticsearchTM*. Beide bieten eine Indexierung auf Basis von Apache Lucene an. Apache Solr und Apache Lucene werden im Grundlagenkapitel 3.7 beschrieben. Solr und Elasticsearch bieten einen ähnlichen Funktionsumfang. Im Rahmen dieser Thesis wird jedoch Apache Solr aus nachfolgenden Gründen genutzt.

Apache Solr bietet einen Cloud-Modus an und nutzt Apache ZooKeeper, um die einzelnen Instanzen zu koordinieren. Für Apache Solr existiert bereits eine Integration in das Hadoop-Framework und die hier verwendete Hortonworks Data Platform.¹⁴

Elasticsearch ist auch horizontal skalierbar und kann auf einem Computer-Cluster installiert werden. Allerdings wird ein eigener Mechanismus zur Koordination des Verbunds genutzt und es existiert für die Hortonworks Data Platform kein Installationspaket zur Nutzung von Elasticsearch im Hadoop-Umfeld. Dies bedeutet, dass Elasticsearch eigenständig im Computer-Cluster ausgerollt und überwacht werden muss.

Ein weiterer Punkt ist die Absicherung des Clusters mithilfe von Kerberos. Prinzipiell können beide Projekte mit Kerberos abgesichert werden. Allerdings ist die Funktionalität bei Elasticsearch nur in einem kostenpflichtigen Zusatzpaket der Firma *Elastic*¹⁵ enthalten.

Zuletzt unterscheiden sich beide Projekte auch in der Art und Weise, wie die Daten verteilt indexiert werden können. Bei Elasticsearch gibt es eine Bibliothek, welche die bereits bekannten *Apache Spark Resilient Distributed Datasets* (RDDs) direkt indexieren kann.¹⁶ Diese Variante eignet sich sehr gut zur Indexierung von Daten.

¹³Siehe Kapitel 6.

¹⁴Siehe Link: https://docs.hortonworks.com/HDPDocuments/HDPS/HDPS-3.0.0/bk_solr-search-installation/content/ch_hdp-search.html. Letzter Zugriff: 9.9.2018.

¹⁵Siehe Link: <https://www.elastic.co/>. Letzter Zugriff: 9.9.2018.

¹⁶Siehe Link: <https://www.elastic.co/guide/en/elasticsearch/hadoop/current/spark.html>. Letzter Zugriff: 9.9.2018.

Apache Solr ermöglicht es auch, Daten mit Apache Spark zu indexieren.¹⁷ Allerdings ist die Schnittstelle etwas umständlicher nutzbar, da nicht die RDDs, sondern die bereits beschriebenen DataFrames, verwendet werden.

Ein weiterer Vorteil von Apache Solr ist die sogenannte *Solr Content Extraction Library (Solr Cell)*, welche unter anderem auch Apache Tika nutzt, um Text aus PDF-Dokumenten, Word-Dokumenten oder Bildern zu extrahieren.¹⁸ Diese Funktionalität kann wiederverwendet werden, um beliebige Dateiinhalte automatisch zu indexieren. Eine ähnliche Funktionalität für Elasticsearch müsste selbst implementiert werden.

Eine interessante Möglichkeit, Dateien in Solr zu indexieren, bietet das Open-Source Projekt *Lily HBase Indexer*.¹⁹ Damit können Daten direkt aus HBase in den Solr-Cluster indexiert werden. Im Rahmen der Thesis wird das Projekt genutzt, um die Metadaten aus HBase in Solr zu indexieren. Abbildung 5.4 stellt die physikalische Aufteilung mit dem Lily HBase Indexer dar.

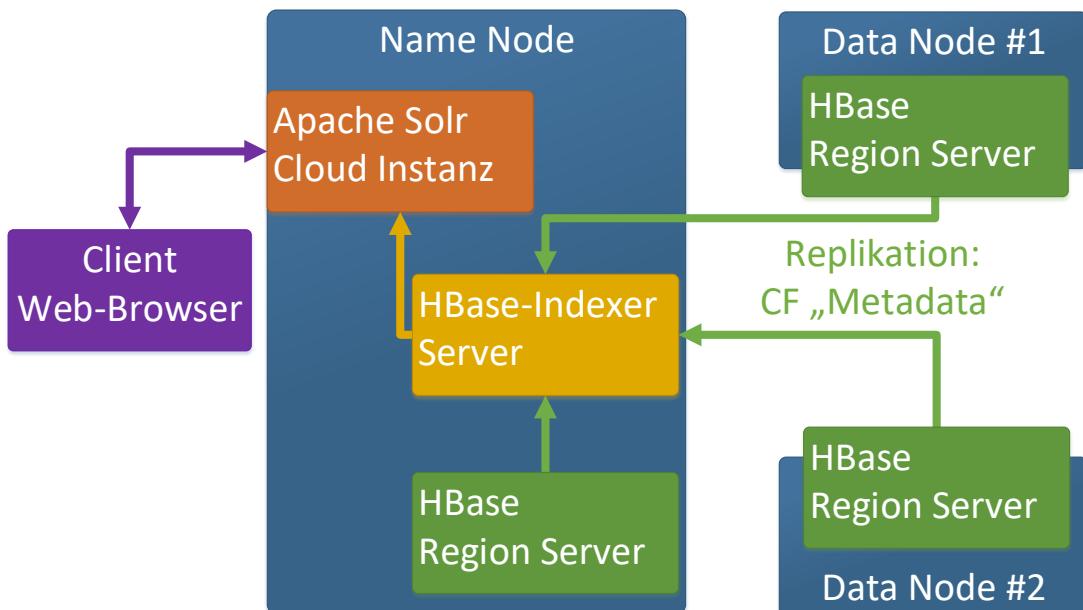


Abbildung 5.4: Indexierung von Daten aus HBase in Solr

Das Projekt bietet mehrere Möglichkeiten, wie Daten indexiert werden können. Die hier genutzte Variante basiert auf einem sogenannten *Side-Effect Processor*.^[19] Dieser Side-Effect

¹⁷Siehe Link: <https://github.com/lucidworks/spark-solr>. Letzter Zugriff: 9.9.2018.

¹⁸Siehe Link: https://lucene.apache.org/solr/guide/7_4/uploading-data-with-solr-cell-using-apache-tika.html#uploading-data-with-solr-cell-using-apache-tika. Letzter Zugriff: 11.9.2018.

¹⁹Siehe Link: <https://github.com/NGDATA/hbase-indexer>. Letzter Zugriff: 9.9.2018.

Processor registriert sich bei HBase als weiterer Knoten zur Datenreplikation. Die Replikation läuft asynchron im Hintergrund und beeinflusst nicht die Schreibgeschwindigkeit von HBase. Jede neue Zeile und jede Datenmodifikation in HBase wird automatisch repliziert und dadurch in Solr indexiert. Auch das Löschen von Zeilen wird entsprechend in Solr übernommen. Damit HBase die Daten repliziert, müssen die Tabellen und deren Spaltenfamilien extra zur Replikation markiert werden. Unabhängig von dieser Replikation, werden die Daten auf mehreren Knoten redundant gespeichert, da HBase die Informationen in Dateien auf dem HDFS ablegt.

Ein Nachteil an dieser Variante ist die Tatsache, dass keine Binärdaten mithilfe von *Solr Cell* verteilt indexiert werden können. Hierzu müsste der Lily HBase Indexer erweitert werden.

Ein weiteres Hindernis zeigt sich bei der Software-Installation. So kann zwar Apache Solr für das Computer-Cluster nachinstalliert werden. Allerdings wird Solr nur auf einem Knoten installiert. Bisher wurde noch keine Möglichkeit gefunden, wie Solr auf allen Knoten im Cluster ausgerollt werden kann. Dies sollte jedoch technisch möglich sein.

Für den Lily HBase Indexer wird eine eigene kleine Server-Komponente benötigt. Diese muss auf allen Knoten installiert sein, damit die Daten nach dem Prinzip der Datenlokalität ordnungsgemäß indexiert werden können. Allerdings läuft auch diese Server-Komponente derzeit nur auf einem Knoten.

Darüber hinaus wird der Lily HBase Indexer aktuell nicht weiterentwickelt.²⁰ Basierend auf einigen Tests, ist die Integration des Indexers nur mit HBase in der Version 1.X.X möglich. Eine erfolgreiche Integration mit bereits verfügbaren neueren Versionen von HBase (ab Version 2.X.X) ist nicht realisierbar.

Aufgrund dieser Probleme ist es sinnvoll, einen neuen Ansatz zur Datenindexierung zu suchen oder den bisherigen Indexer selbst weiterzuentwickeln. An dieser Stelle sollte das *Spark-Solr* Projekt nochmals näher betrachtet werden.²¹ Diese Implementierung könnte eventuell die bestehenden Probleme lösen.

5.4 Praxisbeispiele und deren Optimierungen

Bei der Verarbeitung großer Datenmengen sollte immer das Prinzip der Datenlokalität berücksichtigt werden. Darüber hinaus gibt es weitere Optimierungen, um die Datenmenge auf das nötige Minimum zu reduzieren und die verfügbaren Ressourcen optimal auszunutzen. Im Hadoop-Umfeld und bei der Entwicklung mit Apache Spark ist es besonders wichtig, zu verstehen, auf welchen Knoten welche Teile des Programmcodes ausgeführt werden. Zu dieser Problematik werden in diesem Kapitel einige Beispiele herausgegriffen, welche während der Bearbeitung der Thesis aufgetreten sind.

Datenminimierung

Die Metadaten aus HBase werden mithilfe des *HBase-Spark Connectors* geladen. Dabei können die einzelnen Zeilen mit allen Spalten gelesen und in Spark verarbeitet werden. In Spark werden diese *RDDs* nach bestimmten Kriterien gefiltert. Beispielsweise werden bei der Berechnung von Hashsummen die Zeilen nach logischen Dateien gefiltert. Verzeichnisse oder symbolische Links werden verworfen. Von den Dateien wird nur der Dateinhalt

²⁰Die letzte Änderung im Git-Repository erfolgte im Dezember 2016.

²¹Siehe Link: <https://github.com/lucidworks/spark-solr>. Letzter Zugriff: 9.9.2018.

benötigt. Weitere Metadaten sind nicht notwendig. Auch diese Werte können in den Spark RDDs einfach herausgefiltert werden. Allerdings befinden sich diese Daten zu dem Zeitpunkt schon in den einzelnen Spark Executoren. Viel effizienter ist es, diese Filterungen schon bei der Anfrage in der Datenbank durchzuführen. So bietet der HBase-Spark Connector die Möglichkeit, diverse Filter auf Zeilen und Spalten anzuwenden, um bereits in den einzelnen Region Server die benötigte Datenmenge auf das notwendige Minimum zu begrenzen. Diese Optimierung fällt bei kleinen Datenmengen in einer Testumgebung kaum ins Gewicht. Bei großen Datenmengen in einem produktiven Cluster können dadurch Ressourcen und Zeit eingespart werden.

Lazy Loading

Ein weiterer Aspekt, um den Ressourcenverbrauch minimal zu halten, ist das sogenannte *Lazy Loading*. Bei diesem Entwurfsmuster aus der Softwareentwicklung geht es darum, die Daten nur dann zu laden und zu verarbeiten, wenn sie auch wirklich benötigt werden. Apache Spark implementiert dieses Entwurfsmuster in den Spark RDDs.[22]

Listing 5.2 zeigt ein Beispiel. Dabei werden die Methoden unterteilt in *Transformationen*, wie beispielsweise *map()* oder *filter()* und *Aktionen*, wie zum Beispiel *first()* oder *reduce()*. Alle Transformationen sind *lazy*. Wenn nun eine Transformation auf einem RDD aufgerufen wird, so wird diese Methode noch nicht auf den Daten ausgeführt. Sie wird erst ausgeführt, wenn auf dem RDD auch eine Aktion gestartet wird. Dies kann die Effizienz der Datenausführung steigern, da nur die Transformationen ausgeführt werden, die für das Ergebnis notwendig sind.

```

1 JavaRDD<Data> data = getData();
2 // Definiere Transformationen
3 data.map(x -> convert(x))
4   .filter(Objects::nonNull)
5   .map(y -> convertToZ(y))
6   // Erst bei dem Aufruf der "Aktion" first(),
7   // werden auch die Daten geladen und verarbeitet.
8   .first()

```

Listing 5.2: Lazy Loading bei Apache Spark

Speicherung der Zwischenergebnisse

Wie bereits erläutert, unterscheidet Apache Spark bei den Methoden zwischen Transformationen und Aktionen, die auf ein RDD angewendet werden. Meistens werden ein oder mehrere Transformationen auf ein RDD angewendet und zum Schluss folgt eine Aktion, welche das Ergebnis der Datenverarbeitung zurückliefert. In vielen Fällen werden mehrere Ergebnisse berechnet, welche teilweise auf ähnlichen Transformationen aufbauen. Allerdings kann ein RDD, welches durch eine abschließende Aktion einmal ausgeführt wurde, nicht einfach wiederverwendet werden. Spark bietet aber die Möglichkeit, Zwischenergebnisse einzelner RDDs explizit zwischenzuspeichern, um sie für die Berechnung anderer Ergebnisse wiederzuverwenden. Ein Beispiel aus dem forensischen Umfeld ist die Berechnung von Datei-Hashsummen. Oftmals sollen auch Datei-Duplikate ermittelt werden. Das sind zwei unterschiedliche Ergebnismengen, wobei die Ermittlung der Duplikate auf der Berechnung der Hashsummen aufbaut. Prinzipiell müssen zwei unabhängige RDDs erstellt werden. Beide RDDs berechnen im ersten Schritt die Hashsummen der Rohdaten. Diese Arbeit wird bei zwei unabhängigen RDDs auch zweifach ausgeführt und benötigt daher

doppelt so viele Ressourcen. Daher wäre es in diesem Beispiel sinnvoll, die Berechnung der Hashsummen zwischenzuspeichern und die Ermittlung von Dateiduplikaten darauf aufzubauen. Bei Apache Spark ist es möglich, die Daten im Arbeitsspeicher zwischenzuspeichern oder falls der Speicher nicht ausreicht, auf einen persistenten Datenspeicher auszuweichen. Allerdings müssen die Daten serialisierbar sein. Dies ist gerade bei komplexeren Datentypen nicht immer gegeben. Das Zwischenspeichern von Daten (Caching) spielt bei Apache Spark eine wichtige Rolle, um die Geschwindigkeit der Datenverarbeitung zu optimieren.[22]

Verteilte Datenverarbeitung

Bei der lokalen Entwicklung von Spark-Anwendung ist es einfach, die Resultate eines RDDs über eine Konsole auszugeben. Dadurch kann schnell geprüft werden, ob die Ergebnisse aus fachlicher Sicht korrekt sind. Was hingegen auf kleinen lokalen Testknoten nicht geprüft werden kann, ist die korrekte Skalierung bei großen Datenmengen. Hierbei muss genau überlegt werden, wie die Ergebnisse ausgegeben werden sollen (siehe Listing 5.3).

```

1 HbaseReader hbr = new HbaseReader(jsc, hbaseConfigFile);
2 JavaRDD<Metadata> forensicMetadata = hbr.getForensicMetadata();
3
4 // collect()-Methode
5 forensicMetadata.collect().stream()
6   .forEach(m -> LOGGER.info("Entry = .", m));
7
8 // take(int amount)-Methode
9 forensicMetadata.take(10).stream()
10  .forEach(m -> LOGGER.info("Entry = .", m));

```

Listing 5.3: Anzeige der Ergebnisse eines Spark RDDs

In der ersten Variante wird auf dem RDD die Methode `collect()` aufgerufen und die daraus erhaltene Liste von Objekten wird über ein Logger-Objekt in das Log-File dieser Ausführung geschrieben.

Auf den ersten Blick ist aber nicht ersichtlich, was diese Methode wirklich bewirkt. Wie bereits in Kapitel 3.4 beschrieben, wird bei der Ausführung einer Spark-Anwendung ein sogenannter Spark-Driver gestartet. Dieser wiederum fordert eine gewisse Anzahl von Executoren an, welche die eigentliche Datenverarbeitung übernehmen (Master-Slave-Prinzip). Die Executoren arbeiten auf einzelnen Knoten innerhalb des Clusters. Ein Spark RDD wird bei der Verarbeitung auf diese Executoren aufgeteilt. Doch je nachdem, welche *Aktion* die Ergebnismenge des RDDs zurückliefert, wird das Ergebnis weiterhin verteilt gespeichert oder aber es wird an den Spark-Driver zurückgesendet. In dem Moment, in welchem beispielsweise die `collect()`-Methode auf einem RDD ausgeführt wird, werden die Daten des RDDs *eingesammelt*. Dies bedeutet, dass die Ergebnisse des RDDs, welche verteilt in allen Executoren gespeichert sind, nun an den Spark-Driver geschickt werden.

Dieser Mechanismus ist für sich genommen nicht problematisch und funktioniert beim Testen mit kleinen Datenmengen. Bei großen RDDs werden auch alle Ergebnisse an den Driver geschickt. Da der Driver aber nur begrenzte Ressourcen zugeteilt bekommt, wird in den meisten Fällen der Arbeitsspeicher ausgehen und die Anwendung wird abgebrochen. Daher ist es auch schon beim Testen mit kleinen RDDs sinnvoll, die Daten entweder verteilt auszugeben oder die Ergebnismenge, welche an den Driver gesendet wird, zu begrenzen. Im zweiten Teil von Listing 5.3 wird hierzu die `take()`-Methode verwendet. Diese verhält sich wie die `collect()`-Methode mit dem Zusatz, dass sie nur eine bestimmte Anzahl von Einträgen einsammelt. Dadurch wird bei größeren RDDs der Speicher nicht ausgehen.

Wenn möglich, sollten die Ergebnisse immer verteilt gespeichert werden. Die Methode `saveAsTextFile()` speichert die Ergebnisse eines Spark RDDs in das HDFS. Hierbei legt jeder Executor eine eigene Textdatei im HDFS an und speichert dort seinen Anteil der Ergebnismenge. Dadurch ist eine optimal verteilte Datenverarbeitung, auch bei großen Datenmengen, ohne Ressourcenengpass möglich.

5.5 Leistungsanalyse

Die hier entwickelte forensische Analyseplattform soll den Forensiker dabei unterstützen, die Daten schnell verarbeiten und analysieren zu können. Gerade die Dauer der Datenverarbeitung spielt eine wichtige Rolle. In diesem Kapitel soll daher getestet werden, wie lange die Datenaufbereitung dauert. Der gesamte Verarbeitungsprozess der Analyseplattform besteht einerseits aus dem Datenimport und andererseits aus der eigentlichen Datenverarbeitung. Wobei die reine Datenverarbeitung aus der Berechnung der Hashsummen und der Ermittlung der Medientypen besteht.

Da im Hadoop-Cluster mehrere Knoten im Verbund arbeiten und unterschiedliche Technologien eingesetzt werden, ist es sehr schwer, zuverlässige Testszenarien durchzuführen. Daher sollten die Ergebnisse dieser Testreihe vielmehr Anhaltspunkte liefern, in welchem groben Zeitraum wie viele Daten verarbeitet werden können.

Das hier genutzte Testcluster besteht aus 3 Knoten und bildet daher das kleinste mögliche Hadoop-Cluster mit der standardmäßigen dreifachen Datenreplikation. Die drei Knoten sind identisch und enthalten jeweils eine Intel Core i5-6500 Quad-Core CPU ohne Hyperthreading, 32 GB Arbeitsspeicher, eine 512 GB SSD und eine 2 TB große Magnetfestplatte. Als Betriebssystem wird CentOS 7 (Version 7.5.1804) genutzt. Darauf ist die Hortonworks Data Platform in der Version 2.6.5 installiert. Während das Betriebssystem jeweils auf der SSD installiert ist, werden die Daten aus dem HDFS auf den langsameren und größeren Magnetfestplatten gespeichert. Dadurch hat das HDFS eine maximale Gesamtkapazität von knapp 6 TB. Die Knoten kommunizieren in einem eigenen Netzwerk über Gigabit-Ethernet.

Tabelle 5.1 zeigt die Zeitspanne des Importvorgangs und der Datenverarbeitung. Das erste Datenträgerabbild ist knapp 10 GB groß und enthält eine Ubuntu Installation. Das zweite Datenträgerabbild ist ungefähr 155 GB groß und enthält eine Windows 10 Installation. Letzteres Abbild wird in unterschiedlichen Varianten importiert. Jeder Test wird dreimal durchgeführt. Aus den drei Durchläufen wird jeweils der Mittelwert gebildet.

| Datenträgerabbild | Dauer des Datenimports | Dauer der Datenverarbeitung |
|-----------------------------|------------------------|-----------------------------|
| Ubuntu Image 10 GB | 8 min 26 sec | 4 min 45 sec |
| Windows Image - 1. Variante | 4 h 32 min | 31 min 6 sec |
| Windows Image - 2. Variante | 3 h 20 min | 29 min 50 sec |
| Windows Image - 3. Variante | 1 h 22 min | 29 min 37 sec |

Tabelle 5.1: Zeitspanne der Datenaufbereitung

Der erste Testdurchlauf mit dem 10 GB großen Ubuntu-Datenträgerabbild ist in 13-14 Minuten abgeschlossen. Das Datenträgerabbild wird von einer SSD auf einem Cluster-Knoten ausgelesen und importiert. Die Zeitspanne von knapp 15 Minuten ist akzeptabel und kann noch optimiert werden.

Beim Datenimport des Windows-Datenträgerabbildes zeigen sich deutliche Geschwindigkeitsunterschiede. In der ersten Variante befindet sich das Datenträgerabbild auf einer herkömmlichen Festplatte mit Magnetscheiben, welche sich mit 5400 Umdrehungen pro Minute drehen können. Diese Festplatte wird via USB 3.0 mit einem Knoten des Clusters verbunden und die Daten werden importiert. Diese Variante entspricht einem realistischen Szenario, wenn beispielsweise die Festplatte eines Laptops sichergestellt wird und analysiert werden soll.

Allein der Datenimport benötigt mehr als 4,5 Stunden. Interessanterweise ist das Hadoop-Cluster nicht einmal annähernd voll ausgelastet. Über die Monitoring-Oberfläche des Clusters zeigt sich, dass die CPU- und Speicher-Auslastung nicht sonderlich hoch ist. Allerdings ist der Datendurchsatz von HBase sehr niedrig. Bei näherer Betrachtung zeigt sich, dass in HBase mehrere sogenannte *Region Splits* durchgeführt werden. Wie in Kapitel 3.5 beschrieben, wird eine HBase-Tabelle in Regions unterteilt. Wenn nun eine Region größer als 10 GB ist, dann teilt HBase diese Region in zwei neue kleinere Regions auf.²² Diese *Regions-Splits* benötigen viel Zeit, da die Daten umstrukturiert werden müssen.

In der zweiten Variante aus Tabelle 5.1 wird schon beim Anlegen der HBase-Tabelle angegeben, dass insgesamt 30 Regions in HBase erstellt werden sollen. Darüber hinaus wird der Zeilenschlüssel der einzelnen Einträge so modifiziert, dass HBase alle importierten Dateien gleichmäßig auf die 30 Regions verteilt. Wenn nun die Daten des Windows-Datenträgerabbildes importiert werden, dann reichen diese 30 Regions aus, um alle Daten in HBase zu speichern. Es werden keine zeitaufwendige Region-Splits durchgeführt. Dadurch kann die Zeitdauer des Importvorgangs um mehr als eine Stunde verringert werden.

Die dritte Variante, zum Importieren des Windows-Datenträgerabbildes, basiert auf der zweiten Variante. Dieses Mal ist das Datenträgerabbild auf einer SSD gespeichert und wird direkt von dieser SSD beim Importvorgang ausgelesen. Aufgrund der deutlich höheren Lesegeschwindigkeit von SSDs gegenüber klassischen HDDs mit Magnetscheiben, kann eine höhere Performanz erzielt werden. Daher benötigt der Datenimport in dieser Variante 1 Stunde und 22 Minuten. Hier zeigt sich, dass beim Optimieren der Verarbeitungsgeschwindigkeit die Software und auch die verwendete Hardware gleichermaßen betrachtet werden müssen.

Die bisher erzielte Verarbeitungsgeschwindigkeit ist akzeptabel. Sie kann aber noch deutlich verbessert werden. Beispielsweise ist die Parallelität beim Datenimport noch nicht optimal implementiert. So kann das Hochladen von großen Dateien in das HDFS und das Speichern der Metadaten in HBase vollständig parallelisiert werden.

Die Geschwindigkeit beim Datenimport ist auch abhängig von den genutzten Festplatten. Das HDFS im Testcluster ist so konfiguriert, dass die Daten auf die langsameren magnetischen Festplatten mit 7200 Umdrehungen pro Minute geschrieben werden. Hier kann die Performanz des Clusters weiter erhöht werden, wenn SSDs die Daten des HDFS speichern. Allerdings ist dieser Ansatz aus Kostengründen nicht immer realisierbar.

²²Die Standardkonfiguration von maximal 10 GB Größe kann über den Konfigurationsparameter `hbase.hregion.max.filesize` verändert werden.

Der Datendurchsatz wird auch erhöht, wenn mehrere Asservate parallel in das AnalyseSystem importiert werden. Damit kann eine optimale Auslastung des Hadoop-Clusters erreicht werden. Zumal bei forensischen Analysen oftmals mehrere Asservate sichergestellt werden und diese dann auch parallel verarbeitet werden sollen.

Andererseits macht es aus Anwendersicht keinen Sinn, zuerst das Asservat vollständig zu importieren und erst danach mit der Aufbereitung und Analyse zu beginnen. Die Daten können mit Spark auch schon verarbeitet werden, sobald die ersten Dateien im HDFS oder in HBase gespeichert werden. Durch diesen *Streaming-Modus* hat der Nutzer schon während dem Import die Möglichkeit, die ersten eingehenden Daten zu analysieren. Er müsste nicht warten bis der Import vollständig beendet ist. Auch die Datenindexierung kann schon während dem Importvorgang durchgeführt werden. Dieser Ansatz kann die Verarbeitungszeit nochmals deutlich senken und stellt dem Nutzer schon frühzeitig erste Teilergebnisse zur Verfügung. In einer zukünftigen Weiterentwicklung sollte daher der Datenimport und die Verarbeitung dahingehend überarbeitet werden.

6 Datenvizualisierung

Die Visualisierung von Ergebnissen ist ein wichtiger Aspekt einer Anwendung. Der Nutzer will die Ergebnisse einfach und schnell erkennen können. Dabei hängt die Art und Weise der Visualisierung sehr stark von den Daten und ihren Ergebnissen ab. Im forensischen Umfeld geht es um die Visualisierung von großen Datenmengen und dem Auffinden der sprichwörtlichen Nadel im Heuhaufen. Daher ist es wichtig, passende Werkzeuge bereitzustellen, um die Daten nach bestimmten Kriterien filtern zu können. Darüber hinaus muss es möglich sein, die Dateiinhalte (Bilder, Videos und Dokumente) schnell und zuverlässig anzeigen zu können.

Im Vergleich hierzu bietet die Referenzsoftware *Autopsy* eine gute Möglichkeit zur Datenvisualisierung. So können die Dateien einzelner Datenträger in einer hierarchischen Sicht betrachtet werden. Es existieren auch sogenannte *Views*, um alle Bilder oder alle gelöschten Dateien anzuzeigen. Ein wichtiger Aspekt ist auch die Analyse der Zeitstempel. Hierzu existiert eine eigene Ansicht mit einer Zeitleiste, um nach Ereignissen in einem bestimmten Zeitraum zu suchen. Kommunikationswege, auf der Grundlage von gesendeten E-Mails und besuchten Websites, können auch visualisiert werden. Autopsy bietet hier eine breite Auswahl, wie Daten gefiltert und angezeigt werden können.

Für die hier entwickelte forensische Analyseplattform wird die Datenvisualisierung als Web-Applikation implementiert. Der Zugriff auf die forensischen Rohdaten erfolgt über Apache Solr, wobei die indexierten Daten über eine REST-Schnittstelle angefordert werden.¹

In einer Testimplementierung wird eine rudimentäre Oberfläche zur Anzeige und Filterung der Metadaten entwickelt. Hierzu wird das Open-Source Projekt *Banana* genutzt, um die in Solr indexierten Daten zu visualisieren.² Banana basiert auf dem weit verbreiteten Analyse-Framework *Kibana*, welches die indexierten Daten von Elasticsearch visualisieren kann.³ Analog hierzu stellt Banana einzelne UI-Komponenten bereit, um die Daten aus Solr zu visualisieren. Obwohl das Projekt nicht mehr gepflegt wird, so zeigt es doch wie simpel und performant die Daten aus Solr über die REST-Schnittstelle abgefragt und visualisiert werden können.⁴ Abbildung 6.1 zeigt die Datenvisualisierung mit Banana.

Die Oberfläche ist in mehrere Komponenten aufgeteilt. Die erste Komponente ist die Volltextsuche, die es ermöglicht, in den Metadaten nach bestimmten Wörtern und Werten zu suchen. In der zweiten Zeile befinden sich diverse Statistiken, die bei jeder Filterung oder Suche aktualisiert werden. Im aktuellen Beispiel werden alle importierten Daten angezeigt.

¹Siehe auch Kapitel 3.7.

²Siehe Link: <https://github.com/lucidworks/banana>. Letzter Zugriff: 23.8.2018.

³Siehe Link: <https://www.elastic.co/products/kibana>. Letzter Zugriff: 24.9.2018.

⁴Der letzte Commit in das Github-Repository erfolgte im Juni 2017. Daher wird das Projekt sehr wahrscheinlich nicht mehr weiter gepflegt.

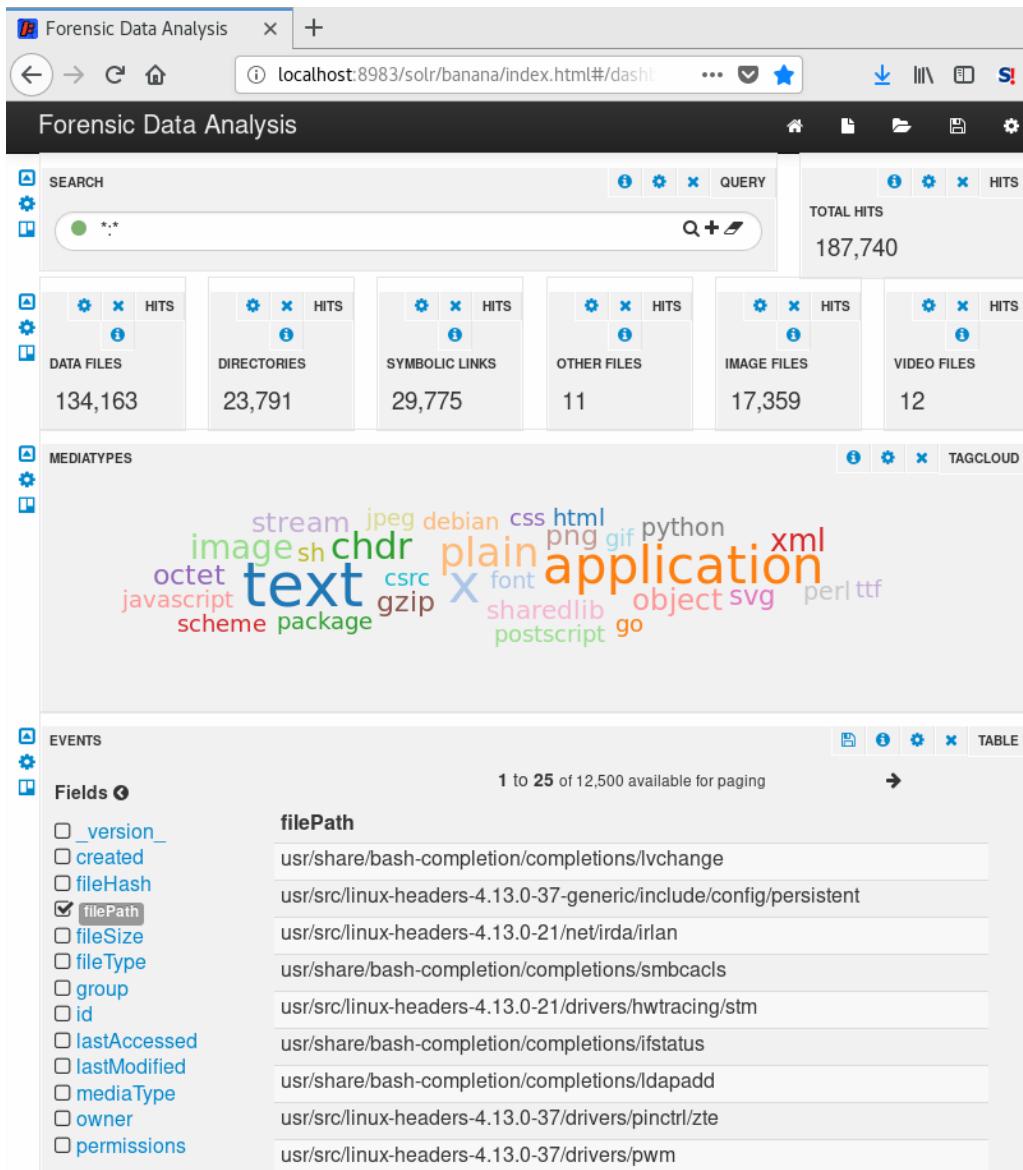


Abbildung 6.1: Visualisierungsbeispiel mit Banana

Dies sind insgesamt 187.740 Dateien. Darunter sind 134.163 Datendateien und 23.791 Verzeichnisse. In den Daten befinden sich 17.359 Bilder und 12 Videos. Diese Werte basieren auf der Erkennung der Medientypen, welche bei der Datenverarbeitung ermittelt werden.⁵

In der dritten Zeile werden die 30 häufigsten vorkommenden Medientypen in einer sogenannten *Word Cloud* angezeigt. In der vierten Zeile hingegen werden die Ergebnisse der Suchanfrage angezeigt. Im konkreten Fall werden die ersten beliebigen Dateien angezeigt. Sobald der Nutzer beispielsweise nach einem bestimmten Dateinamen sucht, werden alle Dateien mit diesem Namen in der Ergebnisliste ausgegeben. Zusätzlich können einzelne Attribute visualisiert werden. Mit Banana ist es auch möglich, die Dateizeitstempel auszuwerten und danach zu filtern.

⁵Siehe Kapitel 5.3.3.

Gerade auch im Open-Source Bereich existieren noch weitere Projekte, welche zukünftig für eine Datenvisualisierung genutzt werden können. So ist es möglich, komplexe Zusammenhänge in der Graphendatenbank *Neo4j* zu speichern und deren Graphenvisualisierung in die Web-Applikation zu integrieren.⁶ Zur Erstellung weiterer Datenvisualisierungen können auch die Projekte *Grafana*⁷ oder *Apache Superset*⁸ genutzt werden. Auch die JavaScript Bibliothek *D3.js* bietet dutzende Varianten zur Datenvisualisierung, welche im forensischen Umfeld bei großen Datenmengen genutzt werden können.⁹

⁶Siehe Link: <https://neo4j.com/>. Letzter Zugriff: 24.9.2018.

⁷Siehe Link: <https://github.com/grafana/grafana>. Letzter Zugriff: 24.9.2018.

⁸Siehe Link: <https://github.com/apache/incubator-superset>. Letzter Zugriff: 24.9.2018.

⁹Siehe Link: <https://d3js.org/>. Letzter Zugriff: 24.9.2018.

7 Weitere Aspekte

7.1 Plattform absichern

7.1.1 Allgemeines

Die forensische Analyseplattform muss besonders gegen unbefugten Zugriff gesichert werden, da bei forensischen Analysen unter anderem personenbezogene Daten, aber auch Geschäftsgeheimnisse aus dem kommerziellen Umfeld, verarbeitet werden. Hierbei ist es absolut untragbar, wenn Unbefugte die Daten lesen oder sogar modifizieren könnten.

Im Hadoop-Umfeld existieren bereits Lösungen, wie Daten vor unbefugtem Zugriff geschützt werden. Das Absichern des Clusters bezieht sich primär auf die Nutzung von Kerberos zur Authentifizierung. Es gibt einige weitere Projekte, wie beispielsweise Apache Ranger, Apache Atlas und Apache Knox, die zum Absichern des Clusters integriert werden können. Sie alle adressieren einen bestimmten Aspekt zur Verbesserung der Systemsicherheit. Nachfolgend soll die Authentifizierung mit Kerberos erklärt werden und Möglichkeiten zur Datenverschlüsselung aufgezeigt werden. Die hier entwickelte forensische Analyseplattform nutzt derzeit weder eine Authentifizierung noch eine Datenverschlüsselung. Allerdings können diese Aspekte in einer zukünftigen Weiterentwicklung implementiert werden.

7.1.2 Authentifizierung

Im Produktivbetrieb wird ein Hadoop-Cluster normalerweise in Kombination mit Kerberos verwendet, um einen allgemeinen Zugriffsschutz zu ermöglichen.[10] Nicht nur Apache Hadoop, sondern alle Komponenten aus dem Hadoop-Ökosystem müssen die Nutzung mit Kerberos unterstützen. Bei den hier genutzten Komponenten, wie Apache Spark, Apache HBase und Apache Solr wird daher darauf geachtet, dass sie mit Kerberos arbeiten können.

Kerberos ist ein kryptografisches Netzwerkprotokoll, welches den Authentifizierungsprozess gegenüber mehreren Servern vereinfachen soll. Dazu werden *Tickets* ausgestellt (*Ticket Single Sign-On*).[4, S. 425-429]

Das grundlegende Problem, welches dieses Protokoll löst, ist der erhöhte Verwaltungsaufwand bei der Authentifizierung gegenüber einer Systemlandschaft aus mehreren Servern. Prinzipiell besteht das Hadoop-Cluster aus mehreren Knoten, auf welchen unterschiedliche Services angeboten werden. Bei der forensischen Analyseplattform könnte der Nutzer Daten aus dem HDFS, HBase oder Solr auslesen, eine Datenverarbeitung mit Apache Spark ausführen oder die allgemeine Ressourcenauslastung des Systems anzeigen. Für all diese Aktionen sind unterschiedliche Services und Komponenten verantwortlich. Ist das System vollständig abgesichert, müsste sich der Nutzer vor jeder Nutzung bei jedem Service getrennt authentifizieren (beispielsweise mittels Nutzernamen und Passwort). Darauf

hinaus müssten sich auch die Komponenten untereinander authentifizieren, denn Apache Spark greift bei der Datenverarbeitung auf die Daten im HDFS zu und schreibt wiederum Daten in HBase. Um diesen Authentifizierungsaufwand zu verringern, wurde Kerberos entwickelt. Bei Kerberos existiert ein zentraler Authentifizierungsserver, gegenüber dem sich ein Nutzer authentifizieren muss. Dieser Server ermöglicht mithilfe sogenannter Tickets die temporäre Authentifizierung gegenüber allen anderen Services, auf welche der Nutzer zugreifen darf.[4, S. 425-429]

Abbildung 7.1 skizziert dieses Verfahren.

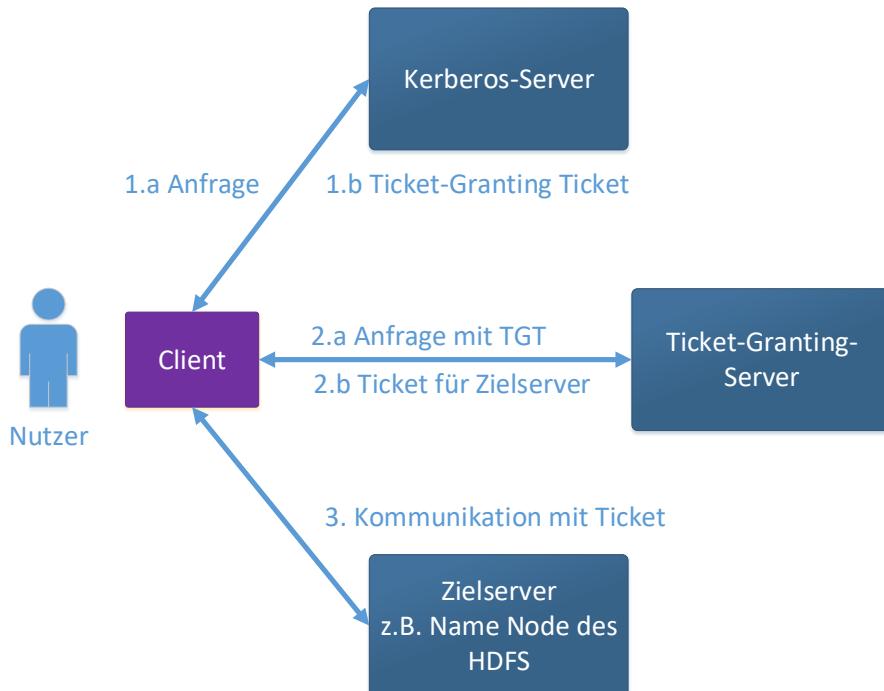


Abbildung 7.1: Authentifizierung mit Kerberos (Vgl. [4, S.426])

Zu Beginn sendet der Nutzer eine Anfrage an den Kerberos-Server zur Authentifizierung (zum Beispiel mit Nutzernname und Passwort). Danach erhält dieser vom Server ein sogenanntes *Ticket-Granting Ticket (TGT)*. Mithilfe des TGT kann er nun beim Ticket-Granting Server (TGS) Tickets für spezifische Zielserver und Services anfordern. Mit einem Ticket für einen konkreten Server oder Service kann der Client nun eine verschlüsselte Verbindung mit dem Zielserver öffnen.

Ein Ticket ist letztlich ein verschlüsselter Datensatz mit Nutzernname und Zugangsberechtigungen für einen spezifischen Server. Der Zielserver kann die für den Server erstellten Tickets vom Ticket-Granting-Server entschlüsseln und so sicherstellen, dass sich der Nutzer authentifiziert hat. Der Ticket-Granting-Server wird bei Kerberos genutzt, um das Schlüsselmanagement sicherer zu machen. Denn dieses Ticket-Granting Ticket ist nur für eine begrenzte Zeit gültig und muss dann wieder neu angefordert werden. Hierdurch ist es für einen Angreifer schwerer, dauerhaften Zugriff auf die Services zu erhalten, falls dieser den Sitzungsschlüssel des Ticket-Granting Tickets ermitteln kann.[4, S. 425-429]

7.1.3 Datenverschlüsselung

Zum Schutz der Daten im Hadoop-Cluster können diese verschlüsselt werden. Hierbei wird zwischen der *Persistenzverschlüsselung* und der *Transportverschlüsselung* unterschieden. Die Persistenzverschlüsselung kann auf unterschiedlicher Ebene durchgeführt werden. Es ist möglich, die Festplatten aller Knoten im Hadoop-Cluster auf Betriebssystemebene zu verschlüsseln. Dabei kann das sogenannte *Linux Unified Key Setup (LUKS)* auf Linux-basierten Betriebssystemen genutzt werden, um alle gespeicherten Daten zu verschlüsseln. Diese Art der Verschlüsselung ist unabhängig vom Hadoop-Ökosystem und sichert daher alle Daten auf den Knoten. Allerdings ist die Verwaltung aufwendig, da beim Ersetzen von Festplatten oder dem Hinzufügen neuer Knoten die Verschlüsselung nochmals durchgeführt werden muss. Darüber hinaus werden bei einem Neustart der Knoten die Passwörter zur Entschlüsselung benötigt. Hierzu gibt es spezifische Komponenten, die die Verwaltung der Schlüssel übernehmen. [10, S. 202-204]

Ein anderer Ansatz ist die Verschlüsselung der Daten auf Applikationsebene. Beim HDFS besteht die Möglichkeit, sogenannte *Verschlüsselungszonen (Encryption Zones)* zu nutzen. Dabei werden schon auf Anwendungsebene die Daten verschlüsselt im HDFS abgelegt. Darüber hinaus werden durch die Nutzung mehrerer Verschlüsselungszonen, die Daten innerhalb des HDFS nochmals gegen ungewollte Nutzerzugriffe gesichert. Dies kann beispielsweise die Sicherheit bei der Speicherung von Daten unterschiedlicher Firmen im gleichen HDFS erhöhen. Um die Daten zu entschlüsseln, wird bei dieser Variante ein unabhängiger Schlüsselserver benötigt, der einem Nutzer die entsprechenden Schlüssel abhängig von seinen Zugangsberechtigungen bereitstellt. Zusätzlich existiert ein sogenannter *Hadoop Key Management Server*, welcher die Kommunikation zwischen Client, HDFS und Schlüsselserver steuert. [10, S. 192-200]

Diese Variante zur Datenverschlüsselung bezieht sich allerdings nur auf das HDFS. Bei der Datenverarbeitung im Hadoop-Umfeld können die Daten aber auch temporär zwischengespeichert werden. Diese werden nicht von der Datenverschlüsselung im HDFS abgedeckt und sind ungeschützt auf den einzelnen Knoten im Cluster gespeichert. Hier zeigt sich, dass die Absicherung im Hadoop-Cluster immer auch spezifisch für die genutzten Komponenten geprüft werden muss.

Auch die Transportverschlüsselung im Hadoop-Cluster sollte betrachtet werden, da hier einerseits sensible Daten zwischen den Knoten aber auch von einzelnen Knoten zu den Rechnern der Nutzer transportiert werden müssen. Bei Webservices über HTTP sollte daher die Verschlüsselung mittels *Transport Layer Security (TLS)* durchgeführt werden. Darüber hinaus bietet Apache Hadoop weitere Möglichkeiten, um auch die Kommunikation zwischen den Knoten entsprechend zu verschlüsseln. Auch hier reicht es nicht aus, nur Apache Hadoop zu betrachten, sondern auch alle anderen Komponenten, die im Hadoop-Cluster arbeiten. [10, S. 207-216]

In der aktuellen Analyseplattform wird derzeit keine Datenverschlüsselung oder Transportverschlüsselung eingesetzt. Zumindest die Transportverschlüsselung sollte in einer zukünftigen Weiterentwicklung implementiert werden, um die Datensicherheit im Netzwerk zu erhöhen.

7.2 Datenlöschung

Das forensisch korrekte Löschen von Daten muss auch im Hadoop-Umfeld betrachtet werden. Bei einer forensischen Analyse werden die Asservate sichergestellt und für einige Zeit verwahrt. Die Computersysteme, mit welchen die Daten analysiert und verarbeitet werden, müssen bereinigt werden. Diese Bereinigung wird meistens durch das mehrmalige Überschreiben der persistenten Datenträger gewährleistet.

Im Hadoop-Umfeld ist dieses Vorgehen aufwendiger. Es ist zwar möglich, mit der hier entwickelten Datenimport-Anwendung aus Kapitel 4.7.3, die Daten aus dem HDFS und HBase zu löschen. Allerdings bedeutet dies nicht, dass sich danach keine Datenrückstände mehr auf den Festplatten der einzelnen Knoten befinden. Für gewöhnlich werden die Daten im HDFS über einen längeren Zeitraum gespeichert und müssen nicht forensisch korrekt gelöscht werden. Daher ist es nachvollziehbar, dass im Hadoop-Ökosystem dieser Aspekt bisher nicht ernsthaft betrachtet wurde.

Das Projekt *Secure Deletion-HDFS (SD-HDFS)* versucht, diesen Aspekt zu berücksichtigen und implementiert einen eigenen Mechanismus zum Löschen von Daten im HDFS.[12] Hierbei werden die allokierten Datenblöcke im HDFS auf den einzelnen Knoten überwacht. Die Datenblöcke, welche aus dem HDFS gelöscht wurden, werden mehrmals mit zufällig generierten Daten überschrieben.

Allerdings ist es fraglich, ob dieser Ansatz wirklich funktioniert. Denn je nach konkretem Speichertyp, ist durch das bloße Überschreiben auf Betriebssystemebene nicht gewährleistet, dass die Daten auch wirklich auf der Festplatte überschrieben werden. Dies ist zum Beispiel bei SSDs relevant, da dort der Speicher-Controller selbst entscheidet, in welchen Speicherblock neue Daten geschrieben werden.

Des Weiteren werden die Daten im Hadoop-Umfeld nicht ausschließlich im HDFS abgespeichert. Beispielsweise könnten Teile der Metadaten in Log-Dateien enthalten sein oder in temporären Dateien zwischengespeichert werden. So können bei Apache Spark nach Bedarf auch Zwischenergebnisse persistent auf die Festplatte ausgelagert werden.[22] Diese Daten werden bei dem Ansatz von SD-HDFS nicht berücksichtigt. Darüber hinaus wird dieses Projekt nicht mehr weiter verfolgt, da kaum Informationen zu dessen Einsatz bekannt sind.

Die derzeit einzige forensisch korrekte Lösung ist die vollständige Datenlöschung aller genutzten Datenträger innerhalb des Clusters. Dies hat jedoch auch die Neuinstallation des Analysesystems auf allen Knoten zur Folge. Aber nur dadurch kann sichergestellt werden, dass temporäre Datenfragmente gelöscht sind.

8 Zusammenfassung

Die Ergebnisse dieser Arbeit zeigen die Machbarkeit einer forensischen Auswertung von großen Datenmengen in einem Computer-Cluster auf Basis von Apache Hadoop. Um die Daten parallel zu verarbeiten, müssen diese in voneinander unabhängig verarbeitbaren Strukturen gespeichert werden. Hierzu bietet es sich an, die logischen Dateien aus den Datenträgerabbildern einzeln im Analysesystem abzuspeichern.

Ein kritischer Aspekt ist die Speicherung beliebig kleiner und großer Dateien für eine optimale Verarbeitung. Als Lösung werden die Vorteile unterschiedlicher Datenhaltungen kombiniert. So werden beliebig große Dateien direkt im verteilten Dateisystem von Apache Hadoop gespeichert. Kleine Dateien werden hingegen in der verteilten spaltenorientierten Datenbank HBase abgelegt. Dort können auch die Metadaten und Analyseergebnisse der Datenverarbeitung abgelegt werden. Derzeit benötigt der Datenimport in das Analysesystem aber noch viel Zeit und die Geschwindigkeit ist noch nicht zufriedenstellend.

Um mehrere Datenträgerabbilder in das System importieren zu können, existiert eine forensische Fallverwaltung. Diese speichert allgemeine technische und fachliche Daten zu den einzelnen importierten Asservaten.

Als Beispiele zur Datenverarbeitung wird die Berechnung von Hashsummen und das Ermitteln von Medientypen der einzelnen Dateien implementiert. Damit ist es bereits möglich Duplikate zu erkennen und nach Dateitypen zu filtern. Beispielsweise können damit alle Bilder der importierten Datenträger aufgelistet werden.

Ein interessanter Punkt zur performanten Analyse ist das Indexieren aller Metadaten und Dateiinhalte. Hierbei werden bereits alle Metadaten für eine performante Suche indexiert. Das Indexieren von Dateiinhalten ist prinzipiell auch möglich. Allerdings muss dafür die bereits existierende Implementierung zur verteilten Datenindexierung im Computer-Cluster nochmals überarbeitet und verbessert werden.

Zur Visualisierung der Daten existiert eine rudimentäre Web-Oberfläche, welche die indexierten Metadaten anzeigen kann. Bei der forensischen Analyse spielen aber auch noch weitere Aspekte, wie beispielsweise die Datensicherheit und Integrität der Beweismittelkette eine Rolle. Hierbei existieren theoretische Ansätze, wie die hier entwickelte Analyseplattform diese Anforderungen erfüllen könnte.

Letztlich bestätigt die hier entwickelte Analyseplattform die Möglichkeit zur verteilten Datenverarbeitung im forensischen Umfeld. Der hier entwickelte Ansatz liefert eine Basis und zeigt auf, wie die Analyseplattform zukünftig verbessert werden kann. Denn die aktuelle Implementierung bietet noch großes Potential, um die Daten zukünftig schneller aufbereiten und verarbeiten zu können.

9 Ausblick

Die hier entwickelte Analyseplattform bietet eine Grundlage zur verteilten Datenverarbeitung bei forensischen Auswertungen. Ausgehend von dieser Grundlage gibt es viele Möglichkeiten die Plattform zu erweitern und zu verbessern.

Bisher existiert für die Analyseplattform nur eine rudimentäre Web-Oberfläche zur Anzeige und Suche auf Basis der Metadaten. Hier müsste eine vollständig neue Oberfläche zur Datenvisualisierung erstellt werden. Ähnlich zu Autopsy sollte es möglich sein, Daten in einer Zeitachse zu visualisieren und Bilder, Videos oder Dokumente direkt anschauen zu können. Ein weiterer interessanter Ansatz wäre die Visualisierung der Beziehung zwischen den einzelnen Dateien in einer Graphenstruktur. Hier könnte die Graphendatenbank Neo4j und ihre Datenvisualisierung als Vorbild dienen. Es sollte auch entsprechende Möglichkeiten geben, die Daten zu verwalten, zu filtern und auch manuell Informationen hinzuzufügen.

Ein weiterer wichtiger Punkt ist die Optimierung der Verarbeitungsgeschwindigkeit. In der bisherigen Implementierung werden immer zuerst die Daten eines einzelnen Datenträgerabbildes in das System importiert. Dieser Datenimport kann zwar parallelisiert werden, jedoch erfolgt die eigentliche Datenverarbeitung immer erst nachdem der Datenträger vollständig importiert wurde. Diese Problematik könnte verbessert werden, indem die Plattform zukünftig jede logische Datei direkt nach ihrer Speicherung im Cluster auch verarbeitet (Streaming Data Modus). Damit könnte ein Nutzer schon während des Datenimports auf Teilergebnisse der bereits analysierten Daten zugreifen. Darüber hinaus wäre es dann auch sinnvoll, wenn die Datenimport-Anwendung versuchen würde fallrelevante Daten zuerst zu importieren. Beispielweise könnten bei Datenträgerabbildern mit installierten Betriebssystemen die nutzerspezifischen Verzeichnisse zuerst importiert werden, da diese im Normalfall für den Analyst einen höheren Mehrwert bieten, als betriebssystemspezifische Verzeichnisse.

Ein anderer Aspekt beim Datenimport ist das Mounten der Datenträgerabbilder. Wie in Kapitel 4.7.6 beschrieben, wird das Projekt *BindFS* genutzt, um dem Datenimport Zugriff auf alle Dateien zu geben. Dadurch ist es derzeit nicht möglich, den Besitzer und die Gruppe aus den Metadaten einer Datei korrekt auszulesen. Ein zukünftige Weiterentwicklung sollte diese Metadaten korrekt auslesen.

Auch die bisherige Datenverarbeitung muss noch erweitert werden. Beispielsweise wäre eine automatische Extraktion gefundener IP-Adressen, Web-Adressen, E-Mail-Adressen oder Positionsdaten sinnvoll. Darauf aufbauend wäre es möglich, Beziehungen zwischen mehreren Asservaten und deren Nutzern herzustellen. Die Extraktion spezifischer Nutzerdaten, wie beispielsweise der Browserhistorie oder E-Mails, wäre auch nützlich.

Die Implementierung einer Volltextsuche für alle Dateiinhalte wurde auch noch nicht zufrie-

denstellend gelöst. Bisher wird die Suche nur auf den Dateimetadaten angewendet. Wobei die Komponente zur Datenindexierung (Apache Solr) eigentlich die Möglichkeit bietet, ganze Dateien automatisiert zu indexieren. Allerdings muss hierzu das verwendete Projekt *Lily HBase Indexer* ausgetauscht werden, da diese Implementierung aktuell keine Binärdateien verarbeiten kann und es auch nicht mehr mit den neueren Versionen von HBase kompatibel ist. Hier müssten neue Lösungen gefunden werden, wie die Daten verteilt im Hadoop-Umfeld indexiert werden können.

Aber auch die querschnittlichen Aspekte bei der forensischen Analyse müssen in zukünftigen Implementierungen berücksichtigt werden. So muss die Analyseplattform entsprechend abgesichert werden. Hierzu könnte zur Nutzerauthentifikation Kerberos genutzt werden, da in der Theorie alle verwendete Komponenten auch die Integration von Kerberos unterstützen. Es wäre auch möglich die Daten auf den einzelnen Computer-Knoten zu verschlüsseln. Hierbei bietet das verteilte Dateisystem HDFS entsprechende Möglichkeiten. In diesem Kontext müsste auch ein passendes Rollenkonzept entwickelt werden.

Ein weiterer Aspekt ist die automatische Generierung der Beweismittelkette. Da das System automatisch die Nutzeraktionen protokolliert, könnten diese Informationen genutzt werden, um eine Beweismittelkette zu erstellen. Damit soll die Herkunft der Ergebnisse und die Integrität der zugrunde liegenden Daten sichergestellt werden.

Zuletzt müsste auch das forensisch korrekte Löschen von Daten nochmals praktisch analysiert werden. Denn nachdem ein Fall bearbeitet wurde, müssen die sensiblen Daten gelöscht werden und können nicht mehr weiterhin im Computer-Cluster verbleiben. Hierbei ist es zwar möglich die Daten im verteilten HDFS aus logischer Sicht zu löschen. Aber es muss auch garantiert werden, dass keine Rückstände auf den Festplatten der einzelnen Computer-Knoten vorhanden sind.

Literatur

- [1] Brian Carrier. *File System Forensic Analysis*. 1. Auflage. Addison Wesley, 2005.
- [2] Eoghan Casey. *Handbook of Digital Forensics and Investigation*. 1. Auflage. Academic Press, 2009.
- [3] Steffen Hartmann. *Solr-Suchserver in die Cloud skalieren*. entwickler.de. 17. Juni 2013. URL: <https://entwickler.de/online/solr-suchserver-in-die-cloud-skalieren-136486.html> (besucht am 02.08.2018).
- [4] Klaus Schmeh. *Kryptografie: Verfahren, Protokolle, Infrastrukturen*. 5. aktual. Auflage. dpunkt-Verl., 2013.
- [5] Jonas Freiknecht. *Big Data in der Praxis*. 1. Auflage. Hanser Verlag, 2014.
- [6] Saurav Haloi. *Apache zookeeper essentials: a fast-paced guide to using Apache ZooKeeper to coordinate services in distributed systems*. 1. Auflage. Packt Publishing, 2015.
- [7] Holden Karau u. a. *Learning Spark: Lightning-Fast Data Analysis*. 1. Auflage. O'Reilly, 2015.
- [8] Philip Polstra. *Linux Forensics*. 1. Auflage. Pentester Academy, 2015.
- [9] Dikshant Shahi. *Apache Solr: A Practical Approach to Enterprise Search*. 1. Auflage. Apress, 2015.
- [10] Ben Spivey und Joey Echeverria. *Hadoop Security: Protecting Your Big Data Platform*. 1. Auflage. O'Reilly, 2015.
- [11] Tom White. *Hadoop: The Definitive Guide*. 4. Auflage. O'Reilly, 2015.
- [12] B. Agrawal u. a. „SD-HDFS: Secure Deletion in Hadoop Distributed File System“. In: *2016 IEEE International Congress on Big Data (BigData Congress)*. 2016, S. 181–189.
- [13] Sam R. Alapati. *Expert Hadoop Administration*. 1. Auflage. Addison Wesley, 2016.
- [14] Benoy Antony u. a. *Professional Hadoop*. 1. Auflage. Wrox, a Wiley brand, 2016.
- [15] Krishna Sankar. *Fast Data Processing with Spark 2*. 3. Auflage. Packt Publishing, 2016.
- [16] André Arnes. *Digital Forensics*. 1. Auflage. Wiley, 2017.
- [17] o. V. *Apache Hadoop YARN*. Version 3.0.0. Apache Software Foundation. 8. Dez. 2017. URL: <https://hadoop.apache.org/docs/current/hadoop-yarn/hadoop-yarn-site/YARN.html> (besucht am 19.03.2018).
- [18] o. V. *HDFS Architecture*. Version 3.0.0. Apache Software Foundation. 8. Dez. 2017. URL: <https://hadoop.apache.org/docs/r3.0.0/hadoop-project-dist/hadoop-hdfs/HdfsDesign.html> (besucht am 17.03.2018).

- [19] Molly Galletto. *The HBase Side-Effect Processor and HBase replication monitoring*. NGDATA. 28. Juni 2018. URL: <https://www.ngdata.com/the-hbase-side-effect-processor-and-hbase-replication-monitoring/> (besucht am 09.09.2018).
- [20] Michael Kofler u. a. *Hacking and Security - Das umfassende Handbuch*. 1. Auflage. Rheinwerk Verlag, 2018.
- [21] o. V. *Apache Solr Reference Guide*. Version 7.4. Apache Software Foundation. 19. Juni 2018. URL: <https://archive.apache.org/dist/lucene/solr/ref-guide/apache-solr-ref-guide-7.4.pdf> (besucht am 10.10.2018).
- [22] o. V. *RDD Programming Guide*. Version 2.3.0. Apache Software Foundation. URL: <https://spark.apache.org/docs/2.3.0/rdd-programming-guide.html> (besucht am 10.09.2018).

Abbildungsverzeichnis

| | | |
|------|--|----|
| 1.1 | Analysevorgehen | 3 |
| 2.1 | Arbeitspakete der Masterthesis | 6 |
| 2.2 | Projektplan Teil A - Einarbeitung und Rohdatenspeicherung (siehe Kapitel A.2) | 7 |
| 2.3 | Projektplan Teil B - Datenanalyse (siehe Kapitel A.2) | 8 |
| 2.4 | Projektplan Teil C - Querschnittliche Aspekte und Visualisierung (siehe Kapitel A.2) | 9 |
| 2.5 | Komponenten der Entwicklungsumgebung | 10 |
| 3.1 | Apache Hadoop Ökosystem (Vgl. [5],[13]. Siehe Kapitel A.2) | 14 |
| 3.2 | HDFS - Datenspeicherung im Verbund (Vgl. [18],[13]) | 16 |
| 3.3 | Ressourcenverteilung mit YARN (Vgl. [17],[13]) | 18 |
| 3.4 | Spark Datenverarbeitung im Cluster | 21 |
| 3.5 | Schema-Beispiel einer HBase Tabelle (Vgl. [5]) | 23 |
| 3.6 | HBase Datenspeicherung im Cluster | 24 |
| 3.7 | Gespeicherte Informationen von HBase in ZooKeeper | 26 |
| 3.8 | Solr Cloud-Mode im Cluster | 28 |
| 3.9 | Solr-Suchanfrage via <i>curl</i> | 29 |
| 4.1 | Forensischer Analyseprozess für digitale Beweismittel (Vgl. [16, S.16]) | 30 |
| 4.2 | Erstellung eines neuen Falls mit Autopsy | 35 |
| 4.3 | Aufteilung der Daten des Datenträgerabildes im Hadoop-Cluster | 37 |
| 4.4 | HDFS - Dateieigenschaften | 39 |
| 4.5 | Datenspeicherung mit erweiterten Dateiattributen im HDFS | 41 |
| 4.6 | Sequence File Format (Vgl. [11, S. 134]) | 42 |
| 4.7 | Kumulierte Häufigkeit nach Dateigröße | 45 |
| 4.8 | Relativierte kumulierte Häufigkeit nach Dateigröße | 46 |
| 4.9 | Kumulierte Kategoriegröße nach Dateigröße | 47 |
| 4.10 | Relativierte kumulierte Kategoriegröße nach Dateigröße | 48 |
| 4.11 | Datenimport in HBase und HDFS | 49 |
| 4.12 | Datenimport-Ausführung in der Konsole | 51 |
| 4.13 | Datenmodell der forensischen Analyseplattform | 52 |
| 5.1 | Module zur automatischen Datenverarbeitung bei Autopsy | 56 |
| 5.2 | Datenfluss bei der Berechnung von Hashsummen | 60 |
| 5.3 | Datenfluss bei der Ermittlung von Medientypen | 61 |
| 5.4 | Indexierung von Daten aus HBase in Solr | 63 |

| | | |
|-----|--|----|
| 6.1 | Visualisierungsbeispiel mit Banana | 71 |
| 7.1 | Authentifizierung mit Kerberos (Vgl. [4, S.426]) | 74 |

Tabellenverzeichnis

| | |
|---|----|
| 5.1 Zeitdauer der Datenaufbereitung | 67 |
|---|----|

Listings

| | | |
|-----|--|----|
| 4.1 | Befehl zum Speichern einer Datei im HDFS | 39 |
| 4.2 | Befehl zum Hinzufügen und Auslesen von Metadaten | 40 |
| 4.3 | Befehl zum Setzen von Posix Capabilities | 54 |
| 4.4 | Nutzung von Bindfs zum Ändern von Dateirechten | 55 |
| 5.1 | Beispielimplementierung eines Spark RDDs | 59 |
| 5.2 | Lazy Loading bei Apache Spark | 65 |
| 5.3 | Anzeige der Ergebnisse eines Spark RDDs | 66 |
| B.1 | Minimale Konfiguration der Datei <i>hdfs-core.xml</i> | 90 |
| B.2 | Minimale Konfiguration der Datei <i>hbase-site.xml</i> | 90 |

Abkürzungsverzeichnis

ACL Access Control List

AFF Advanced Forensic Format

API Application Programming Interface

CAP Consistency, Availability, Partition tolerance

CC-BY-SA-4.0 Creative Commons Attribution Share Alike 4.0

CPU Central Processing Unit

CSV Comma-separated values

E01 EnCase Physical Format

EXIF Exchangeable image file format

FAT File Allocation Table

FoAm Forensische Analyseplattform

GDAL Geospatial Data Abstraction Library

HDFS Hadoop Distributed File System

HDP Hortonworks Data Platform

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

JAR Java Archive

JPEG Joint Photographic Experts Group

JRE Java Runtime Environment

JSON JavaScript Object Notation

JVM Java Virtual Machine

LUKS Linux Unified Key Setup

MD5 Message-Digest 5

NAS Network-attached Storage

NFS Network File System

NoSQL Not only SQL

NTFS New Technology File System

OCR Optical Character Recognition

ORC Optimized Row Columnar File

PDF Portable Document Format

PST Personal Storage Table

RC Record Columnar File

RDD Resilient Distributed Dataset

REST Representational State Transfer

SD-HDFS Secure Deletion-HDFS

SHA Secure Hash Algorithm

Solr Cell Solr Content Extraction Library

SQL Structured Query Language

SSD Solid State Disk

TAR Tape Archive

TGS Ticket-Granting Server

TGT Ticket-Granting Ticket

TLS Transport Layer Security

UTC Coordinated Universal Time

XML Extensible Markup Language

YARN Yet Another Resource Negotiator

A Allgemeines

A.1 Analyse ähnlicher Projekte und Produkte

Im Bereich der IT-Sicherheit und Incident Response für Unternehmensinfrastrukturen, existiert das Apache Projekt *Metron*, welches auf dem Hadoop-Ökosystem aufbaut.¹

Ziel dieses Projektes ist es, Sicherheitsvorfälle zu finden und zu analysieren. Hierbei kann Apache Metron auch mit Telemetriedaten umgehen.²

Eine entsprechende Abgrenzung zu diesem Projekt besteht aufgrund der unterschiedlichen Projektziele. Diese Thesis bezieht sich auf die forensische Analyse von Asservaten und informationstechnischen Systemen. Es ist nicht das Ziel, Sicherheitsvorfälle in unternehmenskritischen Infrastrukturen zu analysieren.

Das Open-Source Framework *Turbinia* ist ein weiteres Projekt, welches ähnliche Ziele verfolgt.³ Der Grundgedanke ist die Automatisierung und Skalierung forensischer Analysen in Computer-Clustern. Prinzipiell hat dieses Projekt das gleiche Ziel, wie diese Mastertesis. Aufwendige Analysen sollen parallelisiert prozessiert werden, um sie schneller zu verarbeiten. Das Projekt wird derzeit aktiv gepflegt.⁴ Allerdings ist es noch in einer frühen Alpha-Phase und daher noch nicht ausgereift. Dieses Projekt basiert auch auf einer Master-Client Architektur. Es bietet aber keine Nutzung auf Basis eines verteilten Dateisystems an. Es muss dafür gesorgt werden, dass jeder Knoten auf alle verfügbaren Daten, beziehungsweise Asservate, zugreifen kann.

Im Rahmen dieser Thesis hingegen, wird durch die Nutzung von Apache Hadoop, eine verteilte Speicherung von Daten unterstützt. Darüber hinaus wird die Datenverarbeitung dort ausgeführt, wo die Daten liegen und nicht umgekehrt.

Ein klassisches Analyse-Werkzeug in der Forensik ist *Autopsy*. Es basiert auf *The Sleuth Kit* und ist kostenlos.⁵ Mit dem Werkzeug können Hashsummen berechnet oder auch Multimediateile analysiert werden. Autopsy ist ein Single-Node Analyseprogramm und läuft vorzugsweise auf einem eigenen Analysecomputer pro Nutzer.

Es gibt auch die Möglichkeit, das Programm kollaborativ zu verwenden. Dabei gibt es einen zentralen Netzwerkspeicher, welcher alle Beweismittel enthält. Es ist möglich, mit mehreren Nutzern parallel am gleichen Fall zu arbeiten und Analyseergebnisse in Echtzeit zu teilen. Diese Art der verteilten Analyse zeigt Ähnlichkeiten zu dieser Thesis auf.

¹Siehe Link: <https://metron.apache.org/>. Letzter Zugriff: 5.3.2018.

²Siehe Link: <https://www.heise.de/developer/meldung/Cybersecurity-Apache-Metron-wird-Top-Level-Projekt-3695901.html>. Letzter Zugriff: 5.3.2018.

³Siehe Link: <https://github.com/google/turbinia>. Letzter Zugriff: 5.3.2018.

⁴Dies ist daran erkennbar, dass der letzte Commit in das Github-Repository am 4.10.2018 erfolgte (Letzter Zugriff: 6.10.2018).

⁵Siehe Link: <https://www.sleuthkit.org/autopsy/>. Letzter Zugriff: 5.3.2018.

Allerdings geht es bei diesem kollaborativen Ansatz vielmehr darum, an einem großen Fall mit mehreren Nutzern zu arbeiten und Ergebnisse einfacher zusammenzutragen. Einzelne Analysen finden nur auf einem konkreten Analyserechner statt. Eine parallele Verarbeitung mittels horizontaler Skalierung wird durch die Anzahl parallel arbeitender Nutzer geschaffen. Jedoch kann das System nicht automatisiert einzelne Analysen auf allen verfügbaren Knoten verarbeiten, wie es in dieser Thesis geplant ist.

Autopsy bietet keine Möglichkeiten, forensische Analysen im Cluster durchzuführen. Allerdings gibt es eine Variante des *The Sleuth Kits*, welche das gleiche Ziel verfolgt, wie in dieser Thesis. Hierbei wird die Funktionalität des *The Sleuth Kits* in einen Apache Hadoop Cluster übertragen.⁶ Das Projekt nutzt Apache Hadoop und auch Apache HBase zur Speicherung von Datenträgern im Cluster. Zur Prozessierung der Daten wird allerdings nicht Apache Spark genutzt, sondern das Hadoop interne Map-Reduce Verfahren. Darüber hinaus wird das Projekt seit 2012 nicht mehr gepflegt.⁷ Es ist nicht bekannt, aus welchen Gründen die Datenverarbeitung im Cluster eingestellt wurde.

A.2 Lizenzierungen in dieser Arbeit

Die dargestellten Gantt-Diagramme (siehe Abbildungen 2.2, 2.3, 2.4) wurden mit der JavaScript-Bibliothek *dhtmlxGantt* erstellt.⁸ Der Quellcode ist unter der *GNU GPLv2*-Lizenz lizenziert. Die aktuelle Bibliothek kann unter folgendem Link: <https://dhtmlx.com/docs/products/dhtmlxGantt/download.shtml> heruntergeladen werden (Letzter Zugriff: 21.3.2018).

Nachfolgend werden die Logos aufgelistet, welche in Abbildung 3.1 dargestellt werden. Die Logos der Projekte und die Projektnamen sind Handelsmarken der Apache Source Foundation.⁹ Sie dürfen in Publikationen genutzt werden.¹⁰

- Apache AmbariTM Logo von <https://ambari.apache.org/>. Letzter Zugriff: 21.3.2018.
- Apache Hadoop[®] Logo von <https://hadoop.apache.org/>. Letzter Zugriff: 21.3.2018.
- Apache SparkTM Logo von <https://spark.apache.org/>. Letzter Zugriff: 21.3.2018.
- Apache HBase[®] Logo von <https://hbase.apache.org/>. Letzter Zugriff: 21.3.2018.
- Apache HiveTM Logo von <https://hive.apache.org/>. Letzter Zugriff: 21.3.2018.
- Apache ZooKeeperTM Logo von <https://zookeeper.apache.org/>. Letzter Zugriff: 21.3.2018.

⁶Siehe Link: https://www.sleuthkit.org/tsk_hadoop/index.php. Letzter Zugriff: 6.10.2018.

⁷Siehe Link zum Source-Code Repository auf GitHub unter: https://github.com/sleuthkit/hadoop_framework. Letzter Zugriff: 6.10.2018.

⁸Siehe Link: <https://github.com/DHTMLX/gantt>. Letzter Zugriff: 20.04.2018.

⁹Siehe Link: <https://www.apache.org/>. Letzter Zugriff: 20.5.2018.

¹⁰Siehe Link: <https://www.apache.org/foundation/marks/>. Letzter Zugriff: 21.3.2018.

B Datenimport

B.1 Konfigurationsdateien

Nachfolgend werden die minimalen Konfigurationsdateien dargestellt, welche beim Datenimport angegeben werden müssen. Diese werden genutzt, um die Verbindung zum HDFS-Dateisystem und zur HBase-Datenbank zu definieren. Letztlich muss in beiden Konfigurationen der Service-Endpunkt konfiguriert werden.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
3 <!--
4   Following configuration describes how to connect to HDFS!-->
5 <configuration>
6   <property>
7     <name>fs.defaultFS</name>
8     <value>hdfs://localhost:9000</value>
9   </property>
10  </configuration>
```

Listing B.1: Minimale Konfiguration der Datei *hdfs-core.xml*

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
3 <!--
4   Following configuration describes how to connect to HBase!-->
5 <configuration>
6   <property>
7     <name>hbase.zookeeper.quorum</name>
8     <value>localhost</value>
9   </property>
10  <property>
11    <name>hbase.zookeeper.property.clientPort</name>
12    <value>2181</value>
13  </property>
14 </configuration>
```

Listing B.2: Minimale Konfiguration der Datei *hbase-site.xml*