INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Analyse von Werkzeugen der Computerforensik

Leonhard Bär

Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Peter Köllner (Bayerisches Landeskriminalamt)
	Helmut Reiser
Abgabetermin:	14. Januar 2005

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 14. Januar 2005

. . . .

(Unterschrift des Kandidaten)

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

Die allgegenwärtige Nutzung von digitalen Systemen wie Computer oder Mobiltelefonen, welche mittlerweile eine erhebliche Rechenleistung bieten, ist in unserer Gesellschaft nicht mehr wegzudenken. Fast jede Person besitzt und verwendet so ein digitales System oder hat zumindest ohne größere Probleme Zugriff auf ein solches. Dies ist zum Beispiel sehr gut an der Nutzung des Internets zu sehen, welches in diesem Jahr in Deutschland von mehr als der Hälfte der Einwohner regelmäßig verwendet wurde [Int04b].

Wie alle technischen und gesellschaftlichen Errungenschaften, werden auch digitale Systeme im täglichen Einsatz in kriminalistische Vorgänge involviert. Sei es, dass sie für die Planung und Durchführung „klassischer“ Verbrechen verwendet werden, zum Beispiel mittels Kommunikation über EMail, oder dass ganz neue Arten von Straftaten entstehen, wie etwa der exzessive Austausch von urheberrechtlich geschützten Dateien.

Die Folgen dieser allgegenwärtigen Nutzung von digitalen Systemen und kriminalistischen Energien, allgemein auch als Computerkriminalität bekannt, spiegelt sich auch in diversen Statistiken wieder. So nimmt die Zahl der beim Bundeskriminalamt gemeldeten Straftaten [Bun03a] in den letzten Jahren ständig zu (siehe Abbildung 1.1 auf der nächsten Seite[1]). Das Bundeskriminalamt zählt dabei nur Straftaten, für welche auch eine Anzeige eingegangen ist. Hier fehlen folglich eine Reihe von Fällen, bei denen auf diese Anzeige verzichtet wurde. Hierunter zählen insbesondere der Verzicht aus Prestigegründen, der sehr häufig auftritt, oder das Desinteresse an einer strafrechtlichen Verfolgung.

Bedingt durch den Anstieg der Verwendung digitaler Systeme bei der Ausführung von Straftaten, bildeten sich Mitte der 80er Jahre, vor allem in den USA, bei den staatlichen Ermittlungsbehörden vereinzelt Abteilungen, welche sich allgemein mit Computerkriminalität beschäftigten (z.B. Computer Analysis and Response Team (CART) des FBI). Bereits in den 90er Jahren wurden dann jährliche Konferenzen zum Thema Computerkriminalität abgehalten und es entstanden, auf Grund der großen Anzahl und Diversität der Straftaten, verschiedene Kategorien oder Forschungsteilbereiche beim Umgang mit solchen Straftaten. Eines dieser Gebiete ist die IT-Forensik, die sich allgemein mit der Sicherstellung von Beweisen in IT Systemen beschäftigt. Die zwei verbreitetsten Ausrichtungen der IT-Forensik sind dabei die Intrusion-Forensik und die Computerforensik. Erstere befasst sich insbesondere mit den Spuren, die beim Eindringen in ein Computersystem entstehen und ist eng mit dem Verfahren der Intrusion Detection Systemen

[1] Der Einbruch der Zahlen im Jahr 2002 ist die Folge eines geänderten Summenschlüssels. Betrugsdelikte mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten ohne PIN werden nicht mehr mit eingerechnet.

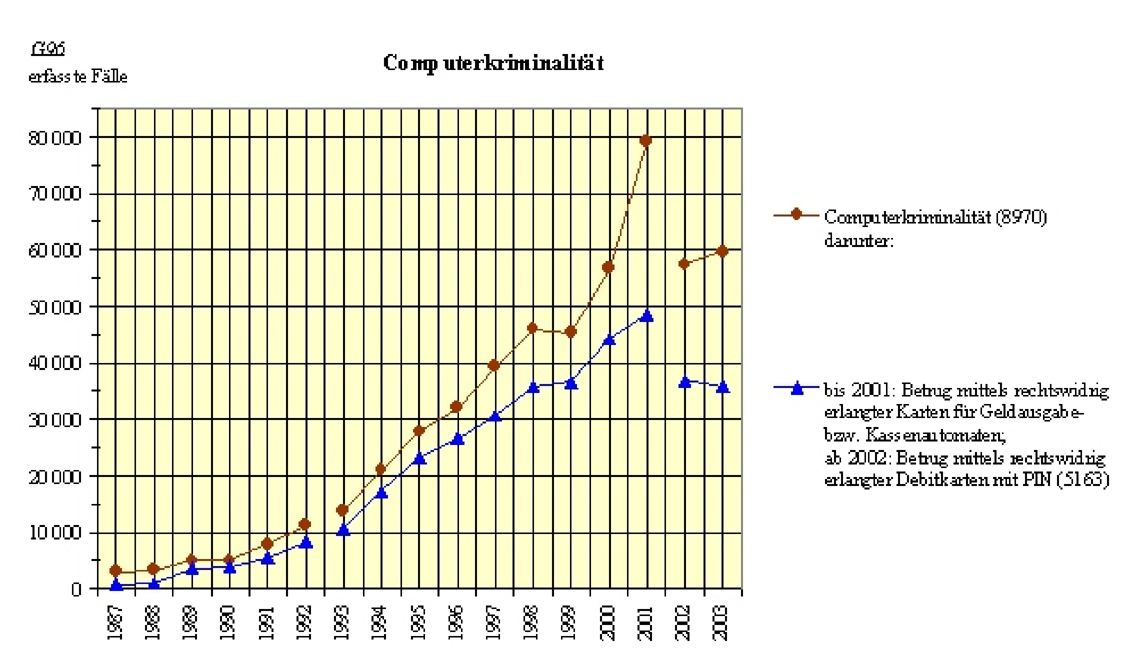

Abbildung 1.1: Erfasste Fälle von Computerkriminalität aus der PKS2003 [Bun03a] des Bundeskriminalamts.

(IDS) verbunden. Die Computerforensik hingegen, welche den Fachbereich der Diplomarbeit festlegt und deren genaue Bedeutung und Aufgabengebiet im folgenden Kapitel noch vorgestellt wird, behandelt vor allem die Analyse von bestehenden Daten auf den unterschiedlichsten Datenträgern.

Ebenfalls entstanden in den 90er Jahren erste Firmen (z.B. Vogon), welche sich auf die diversen Ausprägungen der IT-Forensik, so auch auf das der Computerforensik, spezialisierten und teilweise eng mit den staatlichen Ermittlungsbehörden zusammenarbeiteten. Das hierbei erworbene Wissen und die entwickelten Werkzeuge, welche einen bei einer (computerforensischen) Untersuchung unterstützen und auf welche der Fokus der vorliegenden Arbeit gerichtet ist, wurden dabei aus firmenpolitischen Gründen meist unter Verschluss gehalten.

Diese Situation hat sich in den letzten Jahren entscheidend verändert. Durch den oben erwähnten rasanten Anstieg der Computerkriminalität und deren Meldung in den Medien (z.B. Zerschlagung eines Kinderpornographierings), aber auch durch die Durchdringung von IT Systemen des alltäglichen Lebens und somit einer allgemeinen Präsenz auch in ganz „normalen“ Strafverfahren, ist das Interesse an der Computerforensik und deren Verwendung stark angewachsen. Dieses zeigt sich auch in der Wissenschaft und Wirtschaft. Die Zahl der englischen Publikationen und die Anzahl der verfügbaren Quellen im Internet nimmt kontinuierlich zu, und mit dem Buch „Computer Forensik“ von Alexander Geschonneck [Ges04] ist im Jahr 2004 das erste Deutsche Buch zu diesem

Thema herausgegeben worden, so dass in Zukunft wohl auch in Deutschland mit weiteren Arbeiten zum Thema gerechnet werden kann. Ähnlich verhält es sich auch mit den zur Verfügung stehenden Softwarewerkzeugen, welche einem bei einer computerforensichen Untersuchung unterstützen. Mittlerweile existieren hier sowohl leistungsfähige kommerzielle Tools [Sof04a], als auch auch umfassende open source Projekte [Car04a]. Im Vergleich zu anderen Softwaresparten sind die hier angesprochenen Werkzeuge jedoch noch relativ jung und unterliegen daher einer ständigen und sprunghaften Weiterentwicklung. Ebenfalls umfasst die Computerforensik ein sehr breites Gebiet an Aufgaben und Untersuchungsfeldern, so dass die Softwarewerkzeuge einen enormen Funktionsumfang zur Verfügung stellen, um den Forensiker in so vielen Situation wie möglich zu helfen. Diese zwei Punkte und die daraus resultierende Problematik, die Leistungsfähigkeit der einzelnen Produkte einzuschätzen und sie gegeneinander zu vergleichen, wird in der vorliegenden Diplomarbeit aufgegriffen und es wird ein Verfahren bereitgestellt, diese Problematik zu lösen.

1.2 Aufgabenstellung

Die Aufgabe der Diplomarbeit ist die Analyse und Bewertung von Werkzeugen der Computerforensik. Auf Grund des breiten Spektrums der Computerforensik sind bei dieser Analyse einige Einschränkungen vorgenommen worden. So werden bei den Werkzeugen nur die Eigenschaften untersucht, welche nötig sind, um eine forensische Analyse an einem Bitstream-Image[2] durchzuführen. Dies hat zum Einen den Vorteil, dass das Aufgabengebiet relativ klar umrissen ist und somit überschaubar bleibt. Zum Anderen ist die Analyse von Bitstream-Images einer der häufigsten Anwendungsfälle in der Kriminaltechnischen Abteilung des Bayerischen Landeskriminalamts, welche bei der Ausschreibung der Diplomarbeit beteiligt war und insbesondere bei der Betreuung und technischen Unterstützung entscheidend mitwirkte. Des Weiteren werden alle juristischen Aspekte, welche bei der Untersuchung eines kriminaltechnischen Vorfalls zwangsläufig auftreten, außen vorgelassen und nur dann erwähnt, wenn sie für die technische Ausprägung der Werkzeuge notwendig ist.

Für die Analyse der Werkzeuge bietet sich das Konzept des Kriterienkatalogs an, welches auch in früheren Arbeiten am Lehrstuhl Anwendung fand und dessen Methodik an die aktuelle Aufgabenstellung angepasst wurde. In einem Kriterienkatalog werden alle zu überprüfenden Eigenschaften eines Werkzeugs beschrieben und ein Verfahren gegeben, welches ermöglicht, die Werkzeuge objektiv zu bewerten und ihre Vor- und Nachteile aufzuzeigen.

Die Erstellung des Kriterienkatalogs ist folglich die Hauptaufgabe der Diplomarbeit. Hierfür ist es notwendig, Kriterien zu finden, welche das untersuchte Szenario genau beschreiben. Anschließend müssen diese Kriterien bewertet und ihre Abhängigkeiten untereinander festgelegt werden. Dies geschieht mittels Literaturrecherche, Anwendung der Werkzeuge und in Zusammenarbeit mit Mitarbeitern des Bayerischen Landeskriminalamts.

[2] Ein Bitstream-Image ist eine bitgenaue 1:1 Kopie des Originaldatenträgers in eine Datei.

Im zweiten Teil der Arbeit werden die Möglichkeiten des Kriterienkatalogs gezeigt, bestimmte Werkzeuge zu bewerten. Hierzu ist es notwendig, geeignete Testbedingungen festzulegen, mit deren Hilfe die Bewertung der einzelnen Kriterien für ein ausgesuchtes Werkzeug erfolgt.

1.3 Gliederung der Arbeit

In Kapitel 2 wird zunächst der Vorgang einer computerforensischen Untersuchung beschrieben. Hierbei wird gezeigt, bei welchen Schritten der Einsatz von Werkzeugen sinnvoll bzw. möglich ist.

Das Kapitel 3 vermittelt zunächst einen Einblick in die Thematik der Kriterienkataloge und stellt die bisherigen Ansätze zur Erstellung eines Kriterienkatalogs vor. Daraufhin wird für die vorliegende Aufgabe die geeignetste Methodik ausgewählt.

Das Erstellen des Kriterienkatalogs erfolgt in Abschnitt 4. Hierbei wird zunächst erläutert, wie die Anforderungen an die Werkzeuge der Computerforensik ermittelt werden. Anschließend werden die einzelnen Kriterien genauer beschrieben und ihre Beziehung untereinander dargestellt.

Die anschließende Anwendung des Kriterienkatalogs erfolgt in Kapitel 5. Das Ergebnis liefert einen Überblick über die Leistungsfähigkeit eines Produktes und wird an den drei Programmen *Encase Forensic Edition* [Sof04a], *The Sleuth Kit* [Car04a] und *ILook Investigator* [Ilo04] vorgeführt.

2 Computerforensik

2.1 Was ist Computerforensik?

Wie bereits in der Einleitung angemerkt, kann die Computerforensik als eine Kategorie oder als ein Forschungsgebiet beim Umgang mit Straftaten in der Computerkriminalität angesehen werden. Um diese Kategorie besser klassifizieren zu können, ist es sinnvoll, den Begriff der Forensik zunächst einmal genauer zu betrachten.

Die Forensik stützt sich als Wissenschaft auf die Tätigkeit der forensischen Untersuchung. Das aus dem Lateinischen stammende Wort *forensisch* bedeutet im ursprünglichen Sinn eigentlich *gerichtlich*, eine Übersetzung mit *kriminaltechnisch* ist in der aktuellen Zeit aber wohl zutreffender, was kurz erörtert werden sollte.

Zum Einen soll der Wortstamm „forensisch" den qualitativen Wert bzw. das qualitativ hochwertige Vorgehen einer Untersuchung verdeutlichen. Die Untersuchung soll also so ablaufen, dass ihre Ergebnisse vor Gericht als Beweise anerkannt werden und kein juristischer Zweifel an ihnen aufkommt. Dieses seriöse Vorgehen wird aber auch durch das oben angegebene „technische" wiedergegeben, welches ein wissenschaftliches und subjektives Vorgehen impliziert. Zum Anderen kennen sehr viele Leute den Begriff der Forensik nur im Zusammenhang mit der Gerichtsmedizin, welche aber nur einen Teil der Forensik ausmacht. Eine Übersetzung von forensisch mit gerichtlich würde diese Assoziation nur verstärken. Andere Gebiete der Forensik, wie die forensische Chemie oder die forensische Psychologie (Täterprofile), würden dabei aber weiter in den Hintergrund treten. Der Wortbestandteil „kriminal" ist hier wertneutraler, vermittelt aber weiterhin den Bezug zu einer Straftat, welche der eigentlich Anstoß zu einer forensischen Untersuchung ist.

Das Gebiet der Forensik kann also mit dem „Nachweis und der Aufklärung von strafbaren Handlungen und dem Auffinden von gerichtsverwertbaren Untersuchungsergebnissen" beschrieben werden. Es bleibt also noch die ursprüngliche Frage zu klären, welches Teilgebiet die Computerforensik abdeckt. Eine einfache, aber nicht zutreffende Lösung würde man erhalten, wenn man analog zu oben vorgeht, eine computerforensische Untersuchung betrachtet, und hiermit alle Untersuchungen bezeichnet, welche mit Hilfe eines Computers erfolgen. Da mittlerweile aber fast jede forensische Untersuchung, sei es die Suche nach Fingerabdrücken in einer Datenbank oder das Erstellen eines Täterprofils, mit Hilfe eines Computers erfolgt, würde man hiermit fast jede forensische Untersuchung bezeichnen können. Stattdessen hat sich ein anderes Aufgabengebiet etabliert, welches mit Computerforensik bezeichnet wird.

Die **Computerforensik** befasst sich mit dem Ermitteln, Sicherstellen, Analysieren und Dokumentieren von Beweismitteln im Bereich der Computerkriminalität. Der Fokus liegt hierbei auf der Untersuchung von Computersystemen, welche für die Ausübung einer Straftat verwendet wurden, und auf dem Finden von Beweisen für den Vollzug dieser Straftat.

2.2 Die computerforensische Untersuchung

Nachdem nun der Themenbereich, mit welchem sich die vorliegende Arbeit befasst, genauer vorgestellt wurde, ist noch zu klären, wo und wann die Werkzeuge der Computerforensik eingesetzt werden. Dieser Einsatz ist am besten nachzuvollziehen, indem eine computerforensische Untersuchung in ihren einzelnen Phasen nachvollzogen wird. Dies soll im vorliegenden Abschnitt kurz erfolgen, wobei insbesondere die Stellen hervorgehoben werden, welche den Aufgabenbereich der Diplomarbeit genauer festlegen.

Das Vorgehen bei einer computerforensischen Untersuchung ist von mehreren Faktoren abhängig. Zum Einen behandelt die Computerforensik ein sehr breites Spektrum unterschiedlichster Fälle, ein individuelles Vorgehen ist hier also notwendig. Zum Anderen ist das Vorgehen abhängig vom gewünschten Ziel der Untersuchung. Geht es also zum Beispiel darum, Beweise für eine Gerichtsverhandlung zu ermitteln, oder ist man nur am eigentlichen Ablauf der Straftat interessiert. Schließlich ist es noch wichtig, wer die Untersuchung durchführt. Trägt die Rolle des Ermittlers eine einfache Person (z.B. ein Systemadministrator, welcher den Vorfall aufklären soll), eine beauftragte Firma oder gar eine offizielle Ermittlungsbehörde, wie das Bayerische Landeskriminaltamt, welche sich alle an unterschiedliche rechtliche Vorgaben halten müssen. Das unten vorgestellte Vorgehen kann also nur den groben Verlauf einer Untersuchung wiederspiegeln und ist in keinster Weise vollständig. Dennoch vermittelt es einen guten Überblick über den Ablauf einer Ermittlung und ein ähnlich festgelegtes Vorgehensmodell wird in jeder professionellen Ermittlungsabteilung vorliegen, um die Seriösität einer Untersuchung zu gewährleisten.

Der Ablauf einer computerforensischen Untersuchung wird dabei grob durch die folgenden Punkte widergespiegelt. Die Punkte sind dabei als Phasen anzusehen, welche sich auch gegenseitig überlappen können, da eine wechselseitige Beeinflussung unumgänglich ist.

1. Dokumentation aller Vorgänge
2. Vorbereitung der Ermittlung
3. Sicherstellung der Beweismittel
4. Datenerfassung
5. Schutz der Beweismittel
6. Analyse
7. Auswertung und Präsentation

Die technische Bedeutung dieser Punkte ist schnell geklärt. Auf Grund des juristischen Umfeldes, welches bei der Computerforensik in irgendeiner Form immer vorliegt, ist es aber sinnvoll, zu jedem der Punkte zusätzlich noch einige Anmerkungen zu machen. Diese juristischen Aspekte sind zwar nicht Teil der vorliegenden Arbeit, und es besteht auch keine Anspruch auf Vollständigkeit der angesprochenen Punkte, dennoch sollte man sie im Hinterkopf behalten, da eine Ignorierung eventuell die gesamte forensische Untersuchung zunichte machen kann.

Des Weiteren ist noch der Bezug zwischen diesen Phasen und dem Thema der Diplomarbeit herzustellen. Für jede dieser Phasen existieren Werkzeuge der Computerforensik, die einen Ermittler unterstützen. Die für die Arbeit interessanten Werkzeuge entfalten ihre technischen Eigenschaften vor allem in Phase sechs und kommen dort noch einmal zur Sprache.

2.2.1 Dokumentation

Die vollständige und sofortige Dokumentation eines jeden Ermittlungsschrittes und Ergebnisses ist eine der wichtigsten Punkte im Laufe einer forensischen Ermittlung und erstreckt sich über alle hier angesprochenen Phasen. Es ist daher notwendig, eine lückenlose Informationskette über den Beweis vorzuweisen, damit er vor Gericht anerkannt wird. Diese erstreckt sich vom Ort der Sicherstellung, über sein Verweilen während der Untersuchung, bis hin zu seiner Präsentation. Für diese gerichtliche Anerkennung ist eventuell sogar eine spezielle Form der Dokumentation Voraussetzung. Ist die gerichtliche Verwendung kein Ziel der Untersuchung, bietet sich dieses Dokumentationsverhalten trotzdem an, um zu einen späteren Zeitpunkt die Untersuchung ohne größere Probleme nachvollziehen zu können. Die sofortige Dokumentation greift natürlich für beide Fälle, da sich in der Praxis immer wieder zeigt, dass anfallende Informationen gar nicht oder nur unvollständig erfasst werden, wenn sie nicht sofort dokumentiert werden.

Die Dokumentation ist somit auch ein zentraler Punkt für die Analysephase, welche im Kriterienkatalog durch ein eigenständiges Kriterium (Kriterium 3, Seite 52) repräsentiert wird.

2.2.2 Vorbereitung der Ermittlung

Dies ist ein Punkt der Untersuchung, dessen nichttechnischer Bereich vor allem von privaten Ermittlern unterschätzt wird, die nicht in irgendeiner Form in einer forensischen Abteilung organisiert sind, sondern auf eigene Faust ermitteln.

Auf der technischen Seite ist hier zum Einen das forensische Labor zu nennen, in welchen die spätere Analyse der Daten erfolgt. Dies sollte sich aus Zeit- und Kompatibilitätsgründen auf dem aktuellen Stand der Technik befinden, um ein zügiges und reibungsloses Arbeiten zu ermöglichen. Falls das Labor mit mehreren Computern ausgestattet ist, sollte es aus Sicherheitsgründen über ein separates Netzwerk kommunizieren und nicht mit dem Firmennetzwerk oder gar dem Internet verbunden sein (siehe hierzu den fünften Punkt *Schutz der Beweismittel*). Zum Anderen sind hier noch die für die Untersuchung verwendeten Speichermedien und Programme zu nennen, welche sich in einem „sterilen“ Zustand befinden müssen. Für Speichermedien bedeutet dies, dass sie komplett von nicht mehr gebrauchten Daten bereinigt und in Bezug auf Virenbefall und Funktionstüchtigkeit überprüft wurden. Die verwendeten Programme dürfen nicht aus dubiosen Quellen stammen und falls möglich, sollte ihr Originalzustand, zum Beispiel mittels der Bildung von Hashwerten (MD5), sichergestellt werden.

Da bei der Untersuchung eines Vorfalls sehr schnell auch personenbezogene Daten, zum Beispiel die des Täters oder Opfers, eingesehen und analysiert werden, sind unbedingt die Persöhnlichkeits- und Datenschutzrechte zu beachten. Um hier dennoch vernünftig, dass heißt ohne Ausklammerung von eventuell untersuchungsrelevanten Daten, und im rechtlichen Rahmen eine Ermittlung zu führen, ist eine entsprechende Genehmigung von einer Geschäfts- oder Organisationsleitung (z.B. Betriebsrat oder eine zugehörige polizeiliche Dienststelle) einzuholen. Des Weiteren sollten der Auftrag und das Ziel der Ermittlung so schnell und so genau wie möglich von einer autorisierten Person festgelegt und unterzeichnet werden, um sowohl die Ermittler, als auch die in der Untersuchung involvierten Personen vor unangebrachten Handlungen (z.B. Verletzung der Privatsphäre) zu schützen.

2.2.3 Sicherstellung der Beweismittel

Dies ist vor allem ein kriminaltechnischer Vorgang, welcher bei jeder Ermittlung in ähnlicher Form abläuft und im Falle der Computerforensik sehr eng mit der nächsten Phase der Untersuchung, der Datenerfassung, verzahnt ist. Als Resultat erhält man einen Tatortbefund, der möglichst alle Informationen enthält, welche für die spätere Untersuchung von Bedeutung sein können. Hierunter fallen insbesondere:

- **Der Fundort**
  und die genaue Position, wo die einzelnen Beweise sichergestellt wurden, um eventuell eine genaue Zuordnung zwischen Täter und Beweismittel zu ermöglichen.

- **Die Zeit,**
  welche auf den sichergestellten Systemen eingestellt ist, und eventuelle Abweichungen von der am Tatort aktuellen Zeitzone. Dies wird benötigt, um in der Analysephase eventuell den genauen zeitlichen Ablauf eines Tatvorganges rekonstruieren zu können.

- **Der Zustand**
  des sichergestellten Systems (z.B. der Betriebszustand), welcher sowohl die weitere Sicherstellung (siehe unten), als auch die nächste Phase der forensischen Untersuchung beeinflusst.

Ist kein Vorgehen am Tatort möglich, zum Beispiel wenn eine Ermittlung von einem anderen ausführenden Organ übernommen wurde oder Teile der Ermittlung an dritte weitergegeben wird, ist in jedem Fall zusätzlich die genaue Situation der Übergabe der Beweise festzuhalten.

Wie bereits angedeutet sind bei der Sicherstellung noch einige Besonderheiten zu beachten. Auf Grund des digitalen Charakters der Beweismittel wird in der Regel der zugehörige Datenträger sichergestellt, auf welchem sich die verdächtigen Daten befinden. Bei einer Privatperson ist dies durch die Beschlagnahme des Computers und aller vorgefundenen Datenträger eventuell noch möglich. Bei einer größeren Firma (z.B. einem Internetprovider) könnte dieses Vorgehen aber zu einem erheblichen logistischen Problem werden, das im Vorraus abgeklärt werden sollte.

Ein weiterer wichtiger Punkt ist der Zustand eines Systems und hier insbesondere der Betriebszustand. Trifft man auf ein laufendes System, ist vor dessen Sicherstellung unbedingt noch ein Teilprozess der Datenerfassung notwendig (siehe Online-Erfassung weiter unten), um alle flüchtigen Informationen zu sichern, die ansonsten nicht rekonstruierbar sind. Ob anschließend ein kontrolliertes Herunterfahren des Systems oder eine Trennung vom Stromnetz angebracht ist, hängt von dem vorliegenden System ab und ist im Einzelfall von den Personen vor Ort zu entscheiden.

Aber auch der physische Zustand eines Systems kann von Interesse sein. Sind Manipulationen feststellbar? Wurde versucht, zum Beispiel mittels Feuer oder Wasser, Beweise zu vernichten? Dies sind nur einige Fragen, die hier zu klären sind, welche aber für die spätere Ermittlung eventuell von Bedeutung sein können.

Insgesamt ist bei dieser Phase darauf zu achten, möglichst präzise und vollständig zu arbeiten, da durch die einfache Manipulationsmöglichkeit und Dynamik der digitialen Daten, eine Konservierung, und somit ein späteres Wiederaufsuchen des Tatorts, meist nicht möglich ist.

2.2.4 Datenerfassung

Diese Phase der Ermittlung dient dazu, alle Untersuchungsrelevanten Informationen zusammenzutragen und in einem, für die Ermittlungsabteilung einheitlichen, Format so bereitzustellen, dass während einer späteren Analyse ohne Probleme auf diese Informationen zurückgegriffen werden kann. Insbesondere sollte am Ende dieser Phase eine Trennung zwischen den am Tatort sichergestellten Systemen und Daten, und den später zu analysierendem Material bestehen. Gewährleistet wird dies, indem nur Kopien der Originaldaten zur Verfügung gestellt werden. Dies ist zum Einen aus rechtlichen Gründen notwendig (siehe nächste Phase), zum Anderen hilfreich für die Ermittler, da so parallel mehrere Analysen auf verschiedenen Kopien, oder auch destruktive/manipulative Analysen, möglich sind.

Grundsätzlich sind zwei Arten der Datenerfassung zu unterscheiden, welche vom aktuellen Betriebszustand des Systems abhängen. Zum Einen die schon erwähnte Online-Erfassung, welche auf Grund der Erfassung von flüchtigen Informationen schon während der vorherigen Phase im laufenden Betrieb am Tatort stattfinden muss. Zum Anderen die Offline-Erfassung, auch bekannt als *imaging*, also der Erstellung eines Bitstream-Image[1] von einem Datenträger, was auch zu einem späteren Zeitpunkt unabhängig vom Tatort erfolgen kann.

Bei einer Online-Erfassung werden alle Daten in der Reihenfolge ihrer Vergänglichkeit (Flüchtigkeit) gesichert. Zuerst der Hauptspeicher, dann der aktuelle Zustand des

[1] Ein Bitstream-Image ist eine bitgenaue 1:1 Kopie des Original Datenträgers in eine Datei.

Netzwerkes und laufende Prozesse. Des Weiteren nicht persistente Daten, welche zu den laufenden Prozessen gehören und nur während deren Laufzeit existieren, und temporäre Daten, welche beim Herunterfahren des Systems vom Betriebssystem oder anderen Programmen gelöscht werden. Die hierfür verwendeten Werkzeuge (z.B. `dd` und `netcat` im Unix/Linux Bereich), bzw. die Funktionalität in diesem Bereich, sind für die vorliegende Arbeit aber nicht weiter von Belang.

Bei der offline-Erfassung werden die nichtflüchtigen Daten von Massenspeichern (Festplatten, CD-ROMs, ...) gesichert. In der Regel wird hierzu ein Bitstream-Image erstellt, auf welchem diverse Analysen, zum Beispiel die Wiederherstellung von gelöschten Dateien (siehe Kriterium 4.2.1 Seite 61), vollzogen werden können. Genau diese Fähigkeiten der forensichen Werkzeuge, Analysen auf einem Image durchzuführen, sind der Untersuchungsgegenstand für die vorliegende Diplomarbeit und finden inhärent Einzug in den Kriterienkatalog (Kapitel 4), um die Werkzeuge der Computerforensik zu bewerten. Für die Erstellung des Image existieren diverse Tools (z.B. `dd`) und auch ein großer Teil der Werkzeuge, welche ein solches Image analysieren können, sind in der Lage, Bitstream-Images zu erzeugen. Genau wie bei der Online Erfassung sind diese Fähigkeiten kein Teil der Arbeit. Weitere Informationen und eine sehr ausführliche Bewertung dieser imaging Tools finden sich unter [CFT04].

Nachdem alle untersuchungsrelevanten Daten erfasst wurden, ist es noch notwendig, diese dem Ermittler in geeigneter Weise und entsprechend dem Umfeld in aufbereiteter Form zur Verfügung zu stellen. Für den „Gelegenheitsermittler“ reicht es eventuell, alle fallrelevanten Daten in einem Verzeichnis oder auf einem externen Datenträger abzulegen und auf einem dafür vorgesehenen Rechner zu untersuchen. Im professionellen Einsatz bietet sich hingegen ein dedizierter Server mit eigener Netzwerk Infrastruktur an, so dass für die Untersuchungsrechner ein effizienter Zugriff auf die untersuchten Daten möglich ist.

2.2.5 Schutz der Beweismittel

Der Schutz der Beweismittel und hier insbesondere der Schutz vor Manipulation ist vor allem im Hinblick auf die Gerichtsverwertbarkeit eine wesentliche Bedeutung zuzuschreiben. Zum Schutz sichergestellter Hardware ist im professionellen Bereich die im strafrechtlichen Umfeld übliche Asservatenkammer vorgesehen. Für (firmen-) interne Untersuchungen, die nicht auf eine strafrechtliche Verfolgung hin arbeiten, bietet sich der Firmensafe oder ein ähnlicher Ort an, zu dem nur ausgewählte Personen Zugang haben.

Insbesondere die erfassten Daten sind auf Grund ihrer digitalen Eigenschaft besonders zu schützen, da eine Manipulation relativ schnell und einfach erfolgen kann (z.B. ein einfacher schreibender Zugriff). Um hier die Unverfälschtheit der Beweise sicherzustellen und damit die Zulassung vor Gericht nicht zu gefährden, ist die Anfertigung von Prüfsummen unumgänglich. Aus dem gleichen Grund sollte die Analyse der Daten auch immer auf Kopien erfolgen, um die original Daten vor versehentlicher Manipulation zu schützen.

Der Schutz der Beweismittel erstreckt sich aber noch über weitere Gebiete: zum Beispiel der Schutz vor dem Zugriff von unberechtigen Personen, Schutz der Untersuchungsumgebung und Betriebsmittel vor Manipulation oder der allgemeine Datenschutz, wie er im Gesetzt verankert ist. Diese rechtlichen Aspekte sind aber nicht Bestandteil der vorliegenden Arbeit, da ihr Einbezug den Rahmen der Arbeit bei weitem sprengen würde, außerdem fehlt die juristische Grundlage, um hier fundierte Aussagen treffen zu können.

2.2.6 Analyse

Die Analyse der erfassten Daten ist eine der wichtigsten Phasen im Verlauf einer computerforensischen Untersuchung und für die vorliegende Arbeit die interessanteste. Ziel der Analyse ist es, so viele untersuchungsrelevante Daten wie möglich zu ermitteln und daraus Beweise für die Durchführung einer bestimmten Handlung abzuleiten. Es wird also versucht, die klassischen Fragen einer Ermittlung: „Wer hat was, wo, wann getan; und wie oder womit hat er dies bewerkstelligt" weitgehendst zu klären.

Um diese Fragen effizient zu beantworten, ist eine Kombination aus diversen Analysetechniken und fallorientiertem Vorgehen notwendig. Die unterschiedlichen Analystechniken (z.B. Nutzungsverhalten verschiedener Dienste, Sichtung von multimedia Dateien, Wiederherstellung von gelöschten Dateien) werden hier nur kurz erwähnt, da sie durch die Kriterien des entwickelten Kriterienkatalogs charakterisiert werden und dort eingehend besprochen werden. Für einen Überblick der Analysemöglichkeiten empfiehlt sich hier entweder die graphische Darstellung des Kriterienkatalogs auf Seite 34 oder die tabellarische Darstellung auf Seite 36. Im Folgenden soll also nur ein grober Überblick gegeben werden, welche Techniken zu welchem Zeitpunkt eventuell zum Einsatz kommen können.

Als erstes sind hier die bereits sichergestellten und erfassten Daten zu nennen. Allein bei der Untersuchung eines Computers können sich hier auf Grund aktueller Festplattengrößen[2] und Verfügbarkeit billiger Datenträger[3] weit über hundert Gigabyte an Daten ansammeln. Diese zu untersuchen würde einen immensen Zeitaufwand erfordern. Es sind daher Verfahren und somit der Einsatz von bestimmten Werkzeugen notwendig, diese Datenmengen zu verkleinern und den Umgang mit ihnen zu automatisieren. Eine Reduzierung des Ausgangsmaterial kann zum Beispiel durch das Ausblenden aller Dateien erfolgen, welche zum Betriebssystem oder bekannten Anwendung gehören (Kriterium 2.3 Seite 49). Aber auch eine Konzentration auf bestimmte, fallrelevante Dateien (z.B. multimedia Dateien, bei einem Fall von Kinderpornographie, oder anwendungsspezifischer Dokumente, bei Industriespionage) ist denkbar.

Ein weiterer Punkt ist die Analyse der Nutzung des Systems. Diese fängt bei der Ermittlung der verwendeten Betriebssysteme und installierten Anwendung an, welche zu weiteren system- und anwendungsabhängigen Untersuchungen führen. So unterscheidet sich die Analyse eines Windows und Linux Systems dadurch, dass unterschiedliche Dateisysteme verwendet werden (Kriterium 4.1.2 Seite 58) oder unterschiedliche Anwendungen, zum Beispiel unterschiedliche Browser und EMail Clients bei der Nutzung des Internets (Kriterium 4.5 Seite 87), Verwendung finden.

---

[2] 100GB und mehr sind in aktuellen Computern mittlerweile standardmäßig vorzufinden.

[3] Beschreibbare CD-Rs ($\sim$ 700MB) kosten weniger als 0,30 €, beschreibbare DVD±Rs ($\sim 4,7$GB) weniger als 1.– €.

Schließlich besteht die Sicherung von Beweismittel zum großen Teil auch aus dem Auffinden (Kriterium 4.3 Seite 71) und der Sichtung von unterschiedlichen Daten, welche insbesondere textuellen Charakter aufweisen (z.B. Office Dokumente, Notizen, Protokolldateien, usw.). Es ist also notwendig, alle Quellen zu berücksichtigen, welche untersuchungsrelevante Daten beinhalten können (Kriterium 4.2 Seite 60).

Die Analyse umfasst also ein sehr breites fachliches Gebiet und kann sich je nach Datenumfang, Anzahl der Spuren und äußeren Einflüssen durchaus über einen Zeitraum von mehreren Tagen oder Wochen erstrecken (z.B. wenn erst ein Passwort für einen speziellen Zugriff ermittelt werden muss, oder auf Grund großer Datenmengen eine Suche mehrere Stunden dauert). Der Verlauf und Ausgang der Untersuchung ist dabei inhärent von der Erfahrung des Ermittlers abhängig. Dieser braucht einerseits die „richtige Nase“, um auf eine ergiebige Spur zu stoßen, andererseits genügend Wissen, um diese auch verfolgen und anschließend richtig deuten zu können.

2.2.7 Auswertung und Präsentation

Dies ist die abschließende Phase einer forensischen Untersuchung. In ihr werden alle Ergebnisse der vorangegangen Analyse zusammengefasst und auf ihre Verwertbarkeit in Bezug auf den untersuchten Vorgang überprüft. Es ist also die Aufgabe des Ermittlers diejenigen Ergebnisse auszuwählen und aufzubereiten, welche eine beweiskräftige Aussage über den untersuchten Vorgang liefern.

Eine Auswahl ist deswegen notwendig, da viele Ergebnisse nur eine Spur oder Verdachtsmomente liefern, aber keine sichere Aussage über ein Ereignis ermöglichen. Ausschlaggebend sind aber nur die Ergebnisse, die einen bestimmten Vorgang auch beweisen und nicht nur erahnen lassen. Eine Aufbereitung der Beweise ist notwendig, da der Auftraggeber einer Untersuchung (z.B. die Firmenleitung oder eine gerichtliche Instanz) in der Regel nicht die fachlichen Kompetenzen in Bezug auf das untersuchte Computersystem besitzt. Der Ermittler muss die Beweise also so darstellen, dass sie von den entsprechenden Instanzen verstanden und nachvollzogen werden können, um eine qualifizierte Aussage oder ein gerechtes Urteil über den untersuchten Vorgang abgeben zu können. Hierzu gehört neben den Beweisen an sich, auch die Nennung der verwendeten Werkzeuge und eingesetzten Vorgehensweise, um das (kriminaltechnisch) korrekte Vorgehen der Untersuchung zu zeigen.

2.3 Notwendigkeit von Werkzeugen

Generell werden Werkzeuge dafür verwendet, die Erledigung von Aufgaben effizienter durchzuführen oder gar erst zu ermöglichen. Bei der Aufgabe einer computerforensischen Untersuchung ist dies nicht anders und viele der Notwendigkeiten ergeben sich bereits aus den beschriebenen Punkten, welche im Zusammenhang mit einer computerforensischen Untersuchung bis jetzt genannt wurden. An dieser Stelle folgt also nur noch eine gebündelte Aufstellung dieser Notwendigkeiten.

Bereits in Kapitel 1 wurde die Entstehung der Computerforensik mit der alltäglichen Durchdringung des Lebens mit digitalen Systemen und der ansteigenden Zahl von Fällen im Bereich der Computerkriminalität begründet. Auf die steigende Zahl von Fällen und der durchzuführenden Untersuchungen kann natürlich mit gesteigertem Personalaufwand reagiert werden. Als Alternative bieten sich Werkzeuge an, die die Durchführung einer Untersuchung effizienter gestalten, und es damit einem Ermittler ermöglichen, in gleicher Zeit eine größere Anzahl von Untersuchungen durchzuführen.

Der stark anwachsende Umfang an Daten, welcher pro Fall untersucht werden muss, wurde ebenfalls bereits erwähnt. Fielen früher nur wenige Megabyte an Daten an (z.B. ein Stapel Disketten), so sind heutige Datenträger im hohen Gigabyte Bereich anzusiedeln. Eine effiziente Bewältigung dieser Datenmengen ist ebenfalls nur noch mit Werkzeugen beizukommen.

Als weiterer Punkt ist der begrenzte Wissensstand zu nennen, welcher sich ein Ermittler aneignen kann. Die Zahl der unterschiedlichen digitalen Systeme steigt ständig weiter an, zum Beispiel Windows und Linux Betriebssysteme, welche regelmäßig in neuen Versionen erscheinen. Für jedes dieser Systeme ist aber in der Regel spezielles und systemgebundenes Wissen notwendig, zum Beispiel die Besonderheiten der Dateisysteme, um bestimmte Aufgaben der Sicherstellung von Beweisen durchzuführen. Eine Aneignung dieses Wissens kann aber nur selektiv erfolgen, da ansonsten keine Zeit mehr für die Untersuchung übrig bleibt. Ein Werkzeughersteller hingegen kann dieses Expertenwissen sammeln, in seinem Produkt bündeln und dem Ermittler zu Verfügung stellen. Dem Ermittler ist es somit möglich, sich auf bestimmte Vorgänge einer Untersuchung zu konzentrieren und diese transparent, ohne Expertenwissen über das untersuchte System, durchzuführen (z.B. die Wiederherstellung und Untersuchung von gelöschten Dateien, ohne genaue Kenntnisse über das Dateisystem).

Schließlich ist noch der juristische Charakter einer computerforensischen Untersuchung zu beachten. Die gefunden Beweise sollen ja vor Gericht als solche akzeptiert werden. Dazu gehört auch, dass der Ermittler die Herkunft und Erfassung der Beweise darlegt und versichert, dass diese korrekt und im juristischen Sinne erfolgt ist. Hier kann der Ermittler sein Analysemethoden Schritt für Schritt erklären und so seine Kompetenz und die Korrektheit seines Vorgehens aufzeigen. Einfacher gestaltet es sich aber, wenn man auf die Verwendung eines Werkzeugs verweisen kann, dessen juristische Eignung bereits zu einem früheren Zeitpunkt festgestellt wurde.

3 Methodik zur Erstellung des Kriterienkatalogs

Dieses Kapitel beschreibt das in der Diplomarbeit verwendete Verfahren des Kriterienkatalogs, um Werkzeuge der Computerforensik zu analysieren. Diese Verfahren wurde unter anderem bereits in der Diplomarbeit von Scheiter [Sch99] verwendet und erfuhr später in den Arbeiten von Giemsa [Gie00] und Brenner [Bre02] einige Verbesserungen, auf welche auch in dieser Arbeit zurückgegriffen werden.

Nach einer Einführung über die Komponenten und Eigenschaften eines Kriterienkatalogs werden kurz die Anforderungen beschrieben, welche ein Kriterienkatalog zu erfüllen hat (Abschnitt 3.2, Seite 17). Anschließend werden die bisherigen Verfahren und die jeweils geleisteten Verbesserungen vorgestellt (Abschnitt 3.3, Seite 20). Abgeschlossen wird das Kapitel mit einer Beschreibung, der in der Arbeit verwendeten Methodik (Abschnitt 3.4, Seite 24).

3.1 Einführung

Es existieren unterschiedliche Methoden, um eine effiziente, objektive und umfassende Analyse von komplexen Szenarien zu erhalten (z.B. Benchmarking [SK02]). Die Erstellung und Anwendung eines Kriterienkatalogs, wie sie in dieser Diplomarbeit durchgeführt wird, sind nur eine, wenn auch sehr mächtige, Ausprägung einer solchen Methode. Als Ergebnis erhält man ein Konzept, mit dessen Hilfe ein Szenario (im Falle der Diplomarbeit ein Analysewerkzeug der Computerforensik) schnell und unkompliziert bewertet werden kann.

Für die Erstellung eines Kriterienkatalog liegt kein standardisiertes oder normiertes Verfahren vor. Bei der Entwicklung eines Katalogs ist es daher sinnvoll, sowohl den Aufbau als auch die Methodik zur Erstellung eines Kriterienkatalogs, genauer zu beschreiben und gegebenenfalls anzupassen.

Grundsätzlich enthält ein Kriterienkatalog folgende Komponenten:

- Eine Menge von Kriterien, welche das Szenario vollständig beschreiben und dieses in einzelne Kategorien aufteilt. Ein Kriterium enthält, neben einer vollständigen Beschreibung eines jeden Teilaspektes dieser Kategorie, noch weitere Attribute, mit deren Hilfe das Kriterium bewertet werden kann (z.B. Erfüllungsgrad oder Wichtigkeit des Kriteriums).

- Eine Beschreibung der Beziehung von Kriterien untereinander (z.B. „Kriterium A *ist abhängig von* oder *beeinflusst* Kriterium B“).

- Ein Berechnungsverfahren, welches die Bewertungen und Beziehungen der einzelnen Kriterien zusammenfasst und ein verwertbares Ergebnis für das untersuchte Szenario liefert.

Aus den Beziehungen der Kriterien zueinander entsteht die Struktur des Kriterienkatalogs.

In Abhängigkeit von den Beziehungen der Kriterien untereinander, können mehrere Arten von Kriterien unterschieden werden. Des Weiteren spiegelt sich diese Unterscheidung auch in der Art der Bewertung der einzelnen Kriterien wider. Insgesamt können die Kriterien in folgenden drei Ausprägungen erscheinen:

1. **Basiskriterien**
   Diese Kriterien bilden die Basis des Kriterienkatalogs (ähnlich den Blättern in Baumstrukturen). Mit Hilfe der Beschreibung und der zusätzlichen Attribute, die jedes Kriterium beinhaltet, kann sofort eine Bewertung des Kriteriums erfolgen. Im Idealfall beeinflussen sich die Basiskriterien untereinander nicht (haben also keine Beziehung zueinander), sondern wirken sich nur auf übergeordnete Hauptkriterien aus.

2. **Hauptkriterien**
   Komplexere Kriterien (ähnlich den Knoten in Baumstrukturen), welche von mehreren Kriterien abhängig sind und andere Hauptkriterien beeinflussen. Sie repräsentieren ganze Teilbereiche des Szenarios. Ihre Auswertung erfolgt unter Verwendung des eingesetzten Berechnungsverfahrens. Die Eingabe für dieses Berechnungsverfahren besteht aus den Ergebnissen der Kriterien, von denen das Hauptkriterium abhängt.

3. **Wurzelkriterium**
   Ist ein spezielles Hauptkriterium, welches in jedem Kriterienkatalog nur einmal existieren darf. Von diesem Kriterium sind zum Einen keine weiteren Kriterien abhängig, zum Anderen beeinflusst es auch keine. Die Auswertung dieses Kriteriums entspricht der Auswertung des untersuchten Szenarios.

Um die Abhängigkeit der Kriterien untereinander zu beschreiben, werden die zwei Begriffe *Teilkriterium von* und *Oberkriterium von* verwendet. Alle Kriterien, die einem Hauptkriterium zugeordnet sind, bezeichnet man als *Teilkriterien von* diesem Hauptkriterium. Entsprechend ist ein Hauptkriterium ein *Oberkriterium von* einem bestimmten Teilkriterium. Demzufolge ist ein Basiskriterium immer ein *Teilkriterium von* einem zugehörigen Hauptkriterium. Die Wurzel nimmt immer die Rolle eines Oberkriteriums ein. Die restlichen Hauptkriterien können je nach Position im Kriteriumkatalog sowohl die Rolle eines Teilkriteriums, als auch eines Oberkriteriums annehmen (siehe Abbildung 3.1 auf der gegenüberliegenden Seite).

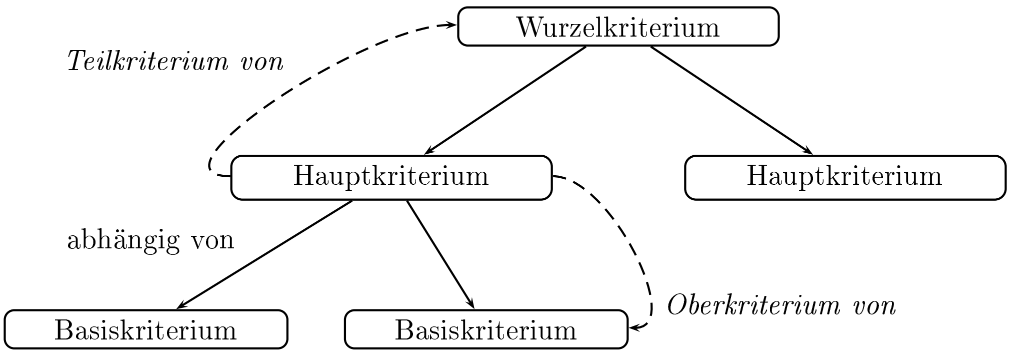

Abbildung 3.1: Beispiel für die Rollen und Beziehungen von Kriterien

3.2 Anforderungen an den Kriterienkatalog

Obige Eigenschaften spiegeln nur den grundsätzlichen Aufbau eines Kriterienkatalogs wieder, geben aber keinerlei Richtlinien vor, wie dieser erstellt werden soll oder welchen Anforderungen der Katalog genügen sollte. Damit die Erstellung und Anwendung des Kriterienkatalogs aber mit vertretbaren Aufwand erfolgt und vergleichbare Ergebnisse liefert, ist es notwendig, ein bestimmtes Vorgehen bei der Erstellung und Anwendung des Katalogs einzuhalten und auch gewisse Anforderungen an den Katalog zu stellen.

3.2.1 Vorgehen bei der Erstellung des Kriterienkatalogs

Die Erstellung eines Kriterienkatalogs kann auf verschiedene Weisen erfolgen. In den meisten Fällen werden aber die folgenden drei Phasen bearbeitet werden, welche bei der Entwicklung eines Kriterienkatalogs eine große Rolle spielen.

1. **Erstellung der Methodik**
   In dieser Phase werden die Regeln des Kriterienkatalogs festgelegt. Hierunter fallen z.B. der Aufbau der Kriterien oder ihr Bewertungsschema. Insbesondere die Festlegung der erlaubten Beziehungen, der Kriterien untereinander, und die Erläuterung des verwendeten Berechnungsverfahren, zur Ermittlung eines Gesamtergebnisses, sind hier notwendige Arbeitsschritte. Für die vorliegende Arbeit ist diese Phase im Abschnitt 3.4 (Seite 24) genauer beschrieben.

2. **Erstellung des Kriterienkatalogs**
   In diese Kategorie fällt alles, was mit der oben beschriebenen „Menge von Kriterien“ zu tun hat. Dies beinhaltet das eigentliche Ermitteln der Kriterien, deren genaue Beschreibung und Klassifizierung, so dass das untersuchte Szenario vollständig und schematisch untersucht werden kann. Des Weiteren werden hier die Attribute der einzelnen Kriterien und deren Beziehungen untereinander festgelegt. Das gesamte Kapitel 4 (Seite 29) beschäftigt sich mit diesem Teil der Entwicklung.

3. **Anwendung des Katalogs**
   Neben evtl. kleinen Anpassungen des Katalogs an das zu untersuchende Szenario, bestimmt vor allem die Auswertung der (Basis-)Kriterien und die anschließende Berechnung des Gesamtergebnisses diese Phase.

Obige Reihenfolge sollte nur begrenzt die zeitliche Abfolge vorgeben, in welcher der Kriterienkatalog entwickelt wird. Eine Interaktion zwischen den einzelnen Phasen ist jederzeit möglich und sogar gewünscht, um ein optimales Ergebnis zu erhalten. So können zum Beispiel bei der Anwendung des Katalogs Ereignisse eintreten, welche die Änderung eines Kriteriums nach sich ziehen (z.B. wenn die Bewertung eines Kriteriums zu aufwändig ist). Diese sollten mit einer erneuten Anwendung der zweiten Phase in den Kriterienkatalog eingearbeitet werden.

3.2.2 Anforderungen an die Methodik

Da die Methodik das Grundgerüst des Kriterienkatalogs darstellt, ist es notwendig, bei der Definition der einzelnen Bestandteile gewisse Vorgaben festzulegen. Dies gewährleistet später eine einfache und effektive Anwendung der Methodik, um unterschiedlichste Kriterienkataloge zu entwerfen. Neben dem Berechnungsverfahren und den Eigenschaften für die Form und Beziehung der Kriterien, sind hier auch Änderungen an der Struktur des Katalogs zu beachten.

Kriterienform und Bewertungsmaßstab

Bei der Anwendung des Kriterienkatalogs fällt ein großer Teil der Arbeit auf die Auswertung der Kriterien. Damit diese Auswertung schnell und reibungslos erfolgen kann, sollten die Form der Kriterien und ihrer erlaubten Attribute einheitlich festgelegt sein. Dies vereinfacht einerseits die Erstellung der Beschreibung der einzelnen Kriterien, da ein festes Muster bei der Beschreibung verwendet werden kann. Andererseits trägt es zur Übersichtlichkeit bei, da sich der Wiedererkennungswert der einzelnen Kriterien erhöht und so ein einfacheres Zurechtfinden in den Kriterien möglich ist.

Beim Festlegen eines Bewertungsmaßstabs ist ein Mittelweg zwischen Genauigkeit und Aussagekraft einzuhalten. Zwar wäre eine sehr feine Diskretisierung bei der Einschätzung eines Kriteriums (z.B. in Prozent) wünschenswert, oft kann diese Genauigkeit aber nicht erreicht werden. Dies liegt zum Einen daran, dass ein Vorgang, welcher von einem Kriterien beschrieben wird, in vielen Fällen nicht auf einer Skala normiert ist, wie es zum Beispiel bei Längen- oder Gewichtsangaben der Fall ist. Der Bewertungsmaßstab eines Kriteriums entspricht aber einer Schablone, welche auf dieser Skala aufsetzt. Für die Bewertung wäre es also notwendig eine eigene Skala für den Vorgang anzulegen, was aber meist nur mit wenigen Abstufungen möglich ist (z.B. Vorgang wird nicht/kaum/mittelmäßig/gut/vollständig erfüllt). Hieraus einen feineren Bewertungsmaßstab abzuleiten, zum Beispiel in Prozentangaben, wäre aber nicht nachvollziehbar und somit nicht sonderlich aussagekräftig. Zum Anderen erfordert eine solch fein granulare Bewertung, falls sie möglich ist, in den meisten Fällen einen nicht zu vertretbarem (zeitlichen) Aufwand. Eine Reduzierung der Bewertungsskala (z.B. auf nicht/im mittlerem Umfang/vollständig erfüllt) ist in solchen Fällen angebracht, da sie aussagekräftiger und meist effizienter zu ermitteln ist.

Beziehungseigenschaften und Struktur

Die Anzahl und Art der erlaubten Beziehungen zwischen den Kriterien, geben die Struktur (z.B. eine Baumstruktur) des Kriterienkatalogs vor. Aus Gründen der Übersichtlichkeit und Nachvollziehbarkeit der Abhängigkeiten ist eine Einschränkung auf einige wenige Beziehungen sinnvoll. Hier ist besonders darauf zu achten, dass keine Zyklen in den Abhängigkeiten entstehen, da ansonsten die Bewertung eines Kriteriums von seiner eigenen Bewertung abhängig ist.

Die Zyklenfreiheit kann zum Beispiel mittels einer abgewandelten Breitensuche (breadth depth first) durch den Graph erfolgen, welche beim Wurzelkriterium startet und alle Pfade entlang der Abhängigkeiten überprüft. Wird bei dieser Suche ein Kriterium doppelt angetroffen, so liegt ein Zyklus vor.

Berechnungsverfahren

Das Berechnungsverfahren liefert als Ergebnis die Bewertung des untersuchten Szenarios. Da die weiteren Entscheidungen über das Szenario von diesem Ergebnis abhängen und oftmals die genaue Auswertung nicht mehr betrachtet wird, sollte das Berechnungsverfahren deshalb folgenden Anforderungen genügen:

- **Aufwand**
  Die Berechnung sollte nachvollziehbar und für alle Kriterienarten (Basis- und Hauptkriterien) auf die gleiche Weise erfolgen, so dass sie insgesamt mit einem vertretbarem Aufwand durchführbar ist.

- **Ergebnis**
  Als Ergebnis muss ein sinnvoller und vergleichbar Wert geliefert werden. Kleine Änderungen in der Bewertung der Kriterien sollten auch nur zu kleinen Änderungen im Ergebnis führen.

- **Robustheit**
  Auch nach Anwendung der nachfolgend angesprochenen Anpassungsmöglichkeiten der Methodik sollten die oberen zwei Punkte noch erfüllt sein.

Anpassungsmöglichkeiten

Im Idealfall wird zur Bewertung eines Szenarios ein Kriterienkatalog erstellt und anschließend angewendet. In der Praxis enstehen dennoch immer wieder Situationen, in denen es nötig ist die Aufgabenstellung oder das Szenario leicht anzupassen (z.B. wenn neue Versionen eines Werkzeugs mit einem neuen Funktionsumfang herausgegeben werden, welcher bis jetzt noch nicht beachtet wurde). Für diese Situationen ist es notwendig, dass die Methodik einige Mechanismen zur Verfügung stellt, diese Anpassungen zu erlauben. Insbesondere Strukturänderungen wie das Entfernen oder Hinzufügen von Kriterien, sollten berücksichtigt werden und unkompliziert durchzuführen sein.

3.2.3 Anforderungen an die Kriterienwahl

Die Wahl der Kriterien erfordert ähnliche Überlegungen wie bei der Kriterienform. Da die Kriterien das Szenario beschreiben und klassifizieren, muss bei ihrer Wahl ein Kompromiss zwischen Genauigkeit und Handhabbarkeit erfolgen. Es ist zwar interessant, jeden einzelnen Teilaspekt eines Szenarios zu untersuchen, dies kann aber zu einer nicht mehr überschaubaren Anzahl von Kriterien führen und somit eine kosteneffektive Auswertung des Szenarios verhindern.

Eine weitere Gegebenheit, die oft bei einer zu hohen und feingranularen Kriterienanzahl auftritt, besteht darin, dass ihre Auswertung für die meisten untersuchten Szenarios unverändert bleibt und nur in Spezialfällen zutrifft. Die Aussagekraft eines solchen Kriteriums ist somit in den meisten Fällen relativ gering und steht in keinem Verhältnis zum verursachten Auswertungsaufwand.

Insgesamt sollte also darauf geachtet werden, dass die Kriterien zum Einen mittels ihrer Beschreibungen und Attribute leicht identifizierbar und bewertbar bleiben. Zum Anderen sollten sie so gewählt werden, dass mittels ihrer Beziehungen untereinander die Zusammenhänge im Szenario deutlich zum Vorschein kommen.

3.3 Bisherige Methodik für Kriterienkataloge

Folgender Abschnitt soll einen kurzen Überblick über die bereits verwendeten Methodiken geben. Hierbei wird nur kurz auf die Interessanten Aspekte der im letzten Abschnitt aufgeführten Anforderungen eingegangen. Insbesondere beim Berechnungsverfahren werden nur die Probleme und deren Lösung präsentiert.

3.3.1 Struktur

Sowohl bei Scheiter [Sch99] als auch bei Giemsa [Gie00] ist alleinig die Baumstruktur für den Kriterienkatalog zulässig. Die Basiskriterien entsprechen dabei den Blattknoten, die Hauptkriterien den inneren Knoten des Baumes. Die einzig erlaubte Beziehung ist hier also die schon oben angesprochene Beziehung zwischen Teil- und Oberkriterium, wobei jedes Teilkriterium nur einem Oberkriterium zugeordnet werden darf. Jedes Basiskriterium besitzt weiterhin die zwei Attribute Bewertung b und Gewicht g (siehe unten), welche die Grundlage für das verwendete Berechnungsverfahren sind. Die Methodik von Brenner [Bre02] verwendet hingegen ein Konzept mit gerichteten Graphen (siehe Abbildung 3.2).

Bewertung der Kriterien

Für die Bewertung der Kriterien wurde ein sehr einfacher Schlüssel verwendet, der nur wenige Abstufungen (5-6) beinhaltet. Besonderem Interesse gilt hierbei der Vergabe der

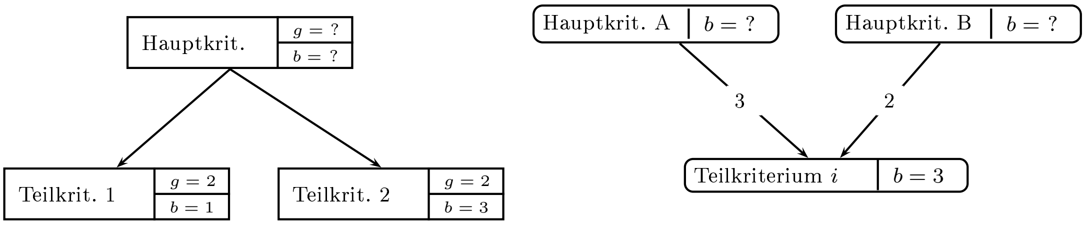

Abbildung 3.2: Beispielstrukturen für Kriterienkataloge (Giemsa/Scheiter und Brenner)

schlechtesteten Bewertung.

Am unteren Ende ist hier bei Giemsa und Scheiter die Nichterfüllung von k.o.-Kriterien aufgeführt. K.o.-Kriterien sind Kriterien, deren Erfüllung für das untersuchte Szenario obligatorisch ist. Diese werden entweder gesondert in einem k.o.-Katalog behandelt (Giemsa) oder ziehen bei Nichterfüllung auch die Nichterfüllung ihres Oberkriteriums nach sich (Scheiter). In beiden Fällen wird dabei zu einem Abbruch der Bewertung und dem Verwerfen des untersuchten Szenarios geraten.

In der Methodik von Brenner existieren keine k.o.-Kriterien, da in dessen Arbeit „nur ein einzelnes Szenario bewertet wird“ und deswegen ein „automatische[r] Ausschluss einer untersuchten Alternative nach Nichterfüllung eines k.o.-Kriteriums keinen Sinn“ ergibt ([Bre02] Seite 30). Ähnliche Überlegungen gelten auch für die vorliegende Arbeit. Da hier Werkzeuge bewertet werden sollen, welche eine umfangreiche Funktionalität in einem weiten Aufgabengebiet anbieten sollen, ist ein Ausschluss eines Kriteriums, aufgrund der Nichterfüllung eines Teilgebietes, nicht sinnvoll. Das Werkzeug ist für dieses Teilgebiet dann einfach nicht geeignet. Aus diesem Umstand eine Nichtbenutzung des ganzen Werkzeugs abzuleiten, wäre nicht nachvollziehbar. Auf das Konzept von k.o.-Kriterien wird daher im Folgenden auch nicht weiter eingegangen.

Gewichtung der Kriterien

Das Gewicht eines Kriteriums ist sowohl bei Giemsa, als auch bei Scheiter ein Attribut des aktuellen Kriteriums, das auf vier Abstufungen beruht. Die Gewichtungen werden dabei gemäß ihres Einflusses auf das Gesamtergebnis vergeben. Dies hat vor allem Auswirken, wenn Anpassungen am Katalog (z.B. Streichung von Kriterien) vorgenommen werden (siehe 3.3.3).

Bei Scheiter erfolgt die Gewichtung nicht mehr als Attribut innerhalb des Kriteriums, sondern wird als Teil der Beziehung zwischen den Kriterien angesehen. Das Gewicht eines Kriteriums wird dabei als Attribut des zugehörigen Oberkriteriums abgelegt. Somit ist es möglich, dass ein Teilkriterium nicht nur ein Oberkriterium beeinflussen kann, sondern die Beeinflussung von mehreren Oberkriterien mit jeweils spezifischer Gewichtung möglich ist. Die strikte Baumstruktur wird also aufgebrochen, und eine Graphenstruktur ist möglich. Die Vergabe der Gewichtung erfolgt dabei für jedes Hauptkriterium in Abhängigkeit davon, wie groß der Einfluss des jeweiligen Teilkriteriums für seine Erfüllung ist.

3.3.2 Berechnungsverfahren

Das Berechnungsverfahren wird eingesetzt, um aus den Bewertungen der einzelnen Teilkriterien, eine Bewertung für das Oberkriterium (bzw. das Wurzelkriterium) zu berechnen. Liegt für ein Teilkriterium noch keine Bewertung vor, so wird das Berechnungsverfahren zunächst auf dieses Teilkriterium angewandt (Dieses rekursive Vorgehen terminiert, da Basiskriterien per Definition unabhängig ausgewertet werden können). Allen drei Methoden ist dabei gemeinsam, dass das zugehörige Gewicht multiplikativ auf die Bewertung des Kriteriums Einfluss nimmt. Bei der weiteren Berechnung gehen die Methoden aber unterschiedliche Wege.

Da sowohl bei Scheiter als auch bei Giemsa, das Gewicht g und die Bewertung b ein Teil des Kriteriums sind, wird für jedes Teilkriterium zunächst eine Punktzahl $p = b \cdot g$ vergeben.

Bei Scheiter werden diese Punktzahlen der Teilkriterien zunächst aufsummiert und anschließend durch die Anzahl der Teilkriterien n dividiert. Hieraus ergibt sich die neue Bewertungszahl b des Oberkriteriums. Analog wird das neue Gewicht g durch die normierte Summe der Gewichte der Teilkriterien g_i berechnet (wobei g_i, b_i, p_i die Attribute des i-ten Teilkriteriums kennzeichnen). Für die Bewertung b und das Gewicht g eines Oberkriteriums ergibt sich also:

$$b = \frac{\sum p_i}{n} \qquad g = \frac{\sum g_i}{n}$$

Hierbei können unerwünschte Effekte auftreten, wenn die Teilkriterien sowohl aus Basiskriterien, als auch aus zusammengesetzten Hauptkriterien bestehen [Gie00], da so Basiskriterien mit gleicher Gewichtung aber unterschiedlicher Tiefe im Baum, einen unterschiedlichen Einfluss auf das Gesamtergebnis haben. Diesen Umstand berücksichtigt Giemsa, und er aggregiert stattdessen die Punktzahlen aller Basiskriterien des Katalogs und mittelt diese. Das Ergebnis ist hier also nur noch von den Bewertungen und Gewichten der Blattkriterien abhängig. Aus logischer Sicht besitzt ein Kriterienbaum aber nur noch die Höhe eins, und weder die Struktur noch die inneren Knoten haben einen Einfluss auf die Auswertung. Dadurch wird der Katalog aber sehr unflexibel, wenn sich die Bewertung für Teilbereiche des Katalogs ändern soll (siehe nächsten Abschnitt). Eine genauere Analyse dieser Berechnungsverfahren findet sich in Kapitel 4.3.5 von [Bre02].

Bei dem Verfahren von Brenner treten diese Effekte nicht auf, da es unter Berücksichtigung dieser Aspekte entwickelt wurde. Wie bereits erwähnt, ist die Gewichtung jetzt als Eigenschaft der Beziehungen zwischen Kriterien definiert. Sie stehen also bereits vor dem Start der Berechnung für alle Kriterien zu Verfügung. Für die Bewertung b_H eines Hauptkriteriums H mit n Teilkriterien wird zunächst analog wie oben die Punktzahlen der einzelnen Teilkriterien berechnet und aufsummiert ($g_{i \to H}$ entspricht dabei der

Gewichtung der Beziehung). Anschließend wird dieser Wert noch mit der Summe der Gewichte normiert und man erhält folgendes Berechnungsverfahren:

$$b_H = \frac{\sum\limits_{i=1}^{n} b_i g_{i \to H}}{\sum\limits_{i=1}^{n} g_{i \to H}}$$

3.3.3 Anpassungsmöglichkeiten

Die Anpassung des Katalogs auf bestehende Szenarios ist eine Anforderung an die Methodik. Insbesondere das Hinzufügen und Weglassen von Kriterien sollte dabei erlaubt sein. Bei diesen Anpassungen zeigen aber sowohl das Verfahren von Scheiter als auch das von Giemsa Schwächen, was auf die Position des Gewichts innerhalb der Kriterien und dem Berechnungsverfahren zurückzuführen ist. Diese werden bei [Bre02] in Abschnit 4.3.5 ausführlich an einem Beispiel erklärt, so dass hier die Ergebnisse nur zitatweise aufgeführt werden.

Zwar sind diese Anpassungsmöglichkeiten grundsätzlich erlaubt, dennoch treten dabei unerwartete Ereignisse auf. Wird zum Beispiel bei dem Verfahren von Scheiter bei der „Berechnung eines Hauptkriteriums ein unterdurchschnittlich wichtiges Teilkriterium herausgenommen [($g_i < g$ in der obigen Berechnung)], so erhöht sich automatisch die Gewichtung des Hauptkriteriums“. Dieser Vorgang setzt sich dann natürlich fort und hat Auswirkungen auf die benachbarten und übergeordneten Kriterien, insbesondere auch auf das Wurzelkriterium. Analog verringert das Hinzufügen eines solchen Kriteriums das Gewicht. Bei Anpassungen mit überdurchschnittlich bewerteten Teilkriterien kehrt sich dieser Effekt um.

Ein ähnlicher Effekt ist auch bei Giemsa zu beobachten. Da hier das „Endergebnis als gewichteter Wert ausgegeben wird, hat das Durchschnittsgewicht aller Kriterien unmitelbaren Einfluss auf das Endergebnis“. Das Hinzufügen eines Kriteriums mit geringen Gewicht führt also zu einer Verschlechterung des Endergebnisses, auch wenn es mit sehr gut bewertet wird.

Bei beiden Verfahren ist es also nach dem Hinzufügen oder Entfernen eines Kriteriums notwendig, die Bewertungen der meisten bzw. aller Kriterien zu überprüfen und gegebenenfalls an die neue Situation anzupassen, da sich ihre Wichtigkeit im Bezug zueinander verändert hat. Auch dieses Problem wird mit dem Verfahren von Brenner umgangen. Durch die Wahl eines geeigneten Berechnungsverfahren und die Verlegung des Gewichts in die Beziehung ist bei einer Anpassung immer nur das aktuelle Oberkriterium und dessen Teilkriterien betroffen. Eine Streichung eines Kriteriums beeinflusst nun keine anderen Gewichte mehr. Beim Hinzufügen eines Kriteriums müssen lediglich die Gewichte der benachbarten Teilkriterien beachtet werden, um eine sinnvolle Einordnung des neuen Kriteriums zu ermöglichen.

Erreichter Erfüllungsgrad		vergebene Bewertung b
Kriterium wird **voll**	erfüllt	4
Kriterium wird **zum größten Teil**	erfüllt	3
Kriterium wird **in mittlerem Umfang**	erfüllt	2
Kriterium wird **kaum**	erfüllt	1
Kriterium wird **nicht**	erfüllt	0

Tabelle 3.1: Abstufungen für den Erfüllungsgrad einzelner Kriterien

3.4 Eingesetzte Methodik

Dieser Abschnitt beschreibt die in der Arbeit verwendete Methodik zu Erstellung eines Kriterienkatalogs. Diese stützt sich zum großen Teil auf die Arbeiten von [Bre02] und wurde an das aktuelle Szenario angepasst. Wie in den Abschnitten zuvor wird zunächst die Struktur des Katalogs, also der Aufbau der Kriterien und ihrer erlaubten Beziehungen zueinander, beschrieben. Anschließend folgt die Festlegung des Berechnungsverfahrens und der erlaubten Anpassungsmöglichkeiten des Katalogs.

3.4.1 Struktur

Bewertung der Kriterien

Das einzig zulässige Attribut für ein Kriterium ist der Erfüllungsgrad. Für dieses zur Bewertung der Kriterien notwendige Attribut wird die in Tabelle 3.1 gezeigte Skala verwendet. Diese Skala spiegelt die maximale Differenzierung der Bewertung da, um den in Abschnitt 3.2.2 angesprochenen Anforderungen zu genügen. Das heißt, dass eine weitere Verfeinerung in unterschiedliche Erfrüllungsgrade nicht erlaubt ist. Falls ein Kriterium nicht so differenziert bewertet werden kann, ist hingegen eine sinnvolle Kürzung der Skala ohne weiteres möglich (z.B. Kriterium wird voll/in mittlerem Umfang/nicht erfüllt).

Beziehung der Kriterien

Für die Beziehungen des Kriterienkatalogs werden folgende Einschränkungen festgesetzt:

- Die Zuordnung eines Teilkriteriums zu einem Oberkriterium (und umgekehrt) ist die einzig erlaubte Beziehung.
- Der Kriterienkatalog muss zyklenfrei sein.
- Bis auf das Wurzelkriterium sind alle Kriterien Teilkriterien eines anderes.

Punkt eins ermöglicht es relativ einfache Graphen zu erstellen, da „komplizierte“ Beziehungen (z.B. mit Bedingungen verknüpft) nicht zulässig sind. Dennoch bleibt die Möglichkeit, dass bestimmte Teilkriterien Einfluss auf mehr als ein Hauptkriterium haben, was in einer reinen Baumstruktur nur durch redundantes Vorhalten bestimmter Kriterien möglich wäre. Punkt zwei gewährleistet, dass die Auswertung eines Kriteriums nicht von

Relevanz des Kriteriums		Gewichtung g
Kriterium ist **äußerst wichtig**	für die Erfüllung des Hauptkriteriums	4
Kriterium ist **sehr wichtig**	für die Erfüllung des Hauptkriteriums	3
Kriterium ist **wichtig**	für die Erfüllung des Hauptkriteriums	2
Kriterium ist **weniger wichtig**	für die Erfüllung des Hauptkriteriums	1

Tabelle 3.2: Abstufungen für die Gewichtung von Teilkriterien

der eigenen Auswertung abhängig ist. In Verbindung mit Punkt drei stellt dies einerseits sicher, dass ein zusammenhängender Graph und kein Wald vorliegt. Andererseits wird dadurch gewährleistet, dass genau ein ausgezeichnetes Kriterium existiert, welches am Ende das Ergebnis des Kriterienkatalogs beinhaltet.

Gewichtung der Kriterien

Der unterschiedliche Einfluss der einzelnen Teilkriterien auf ihr Oberkriterium wird als Gewicht der Beziehungen modelliert. Die hierfür zulässigen Werte werden in Tabelle 3.2 angegeben. Die Verteilung der Gewichte erfolgt dabei topdown von der Wurzel aus, wobei für jedes Hauptkriterium bestimmt wird, wie groß der Einfluss jedes seiner Teilkriterien auf seine Erfüllung ist.

Die Gewichtung der einzelnen Teilkriterien wird in der Erklärung des zugehörigen Hauptkriterium angegeben und motiviert. Des Weiteren wird der Wert in der graphischen Darstellung (Abbildung 4.4/4.2 Seite 34/35) als Gewicht der Kanten eingetragen.

Aufbau eines Kriteriums

Der Aufbau der einzelnen Kriterien ist prinzipiell immer gleich und genügt folgendem Schema (siehe Abbildung 3.3 Seite 26):

1. Titel des Kriteriums.
2. Pfad von der Wurzel zum Kriterium und, falls vorhanden, die Angabe der Teilkriterien mit ihren Gewichten.
3. Ist das Kriterium ein Basiskriterium, so folgt hier eine detaillierte Beschreibung des Kriteriums, um es genau zu bestimmen und von den anderen Kriterien abzugrenzen. Ist das Kriterium ein Hauptkriterium, folgt hier ein Überblick über das entsprechende Themengebiet und die Gewichtung der Teilkriterien.
4. Anforderungen an das Werkzeug, die es leisten soll.
5. Mögliche Erscheinungsformen des Kriteriums.
6. Maßstab für die Bewertung des Kriteriums.

Die Punkte 4-6 sind nur bei Basiskriterien vorhanden.

Kriterium 1.2.4
TITEL DES BEISPIELKRITERIUMS

Kriterium	Gewicht
Oberkriterium XYZ	
Titel des aktuellen Beispielkriteriums	
Teilkriterium 1	4
Teilkriterium 2	1
Teilkriterium 3	2

Ist das Kriterium ein Basiskriterium, so folgt hier eine detaillierte Beschreibung des Kriteriums, um es genau zu bestimmen und von den anderen Kriterien abzugrenzen. Ist das Kriterium ein Hauptkriterium, folgt hier ein Überblick über das entsprechende Themengebiet und die Gewichtung der Teilkriterien.

Anforderungen:

- Das Werkzeug sollte die Funktion XYZ unterstützen.
- Das Werkzeug sollte die Funktion ABC unterstützen
- Das Werkzeug sollte die Funktion OPQ unterstützen.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Ein Teil der Punkte wird erfüllt.

C Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	im mittlerem Umfang erfüllt	2
C	nicht erfüllt	0

Abbildung 3.3: Beispielaufbau eines Kriteriums

3.4.2 Berechnungsverfahren

Sei $g_{(i \to H)}$ das Gewicht der Beziehung zwischen einem Teilkriterium i und seinem Oberkriterium H (einem Hauptkriterium). Die Bewertung b_H eines Hauptkriteriums wird in Abhängigkeit der Bewertungen b_i der Teilkriterien mit folgendem Berechnungsverfahren ermittelt:

$$b_H = \frac{\sum\limits_{i=1}^{n} b_i g_{(i \to H)}}{\sum\limits_{i=1}^{n} g_{(i \to H)}} \tag{3.1}$$

Da die Gewichte der Beziehungen bei der Erstellung des Kriterienkatalogs festgelegt werden, reicht es für die Bewertung eines Hauptkriteriums aus, die Bewertungen der einzelnen Teilkriterien festzustellen.

Die Bewertung des Wurzelkriteriums und somit die Auswertung des Kriterienkatalogs, wird also folgendermaßen rekursiv für jedes Hauptkriterium berechnet:

1. Liegen alle Bewertungen der Teilkriterien vor, kann mit Hilfe der Berechnungsformel (3.1) die Bewertung ausgerechnet werden.
2. Falls für ein Teilkriterium keine Bewertung vorliegt, ist zunächst eine Bewertung des Teilkriteriums notwendig.

Dieses rekursive Vorgehen terminiert, da Basiskriterien per Definition unabhängig ausgewertet werden können Es werden also zunächst alle Hauptkriterien ausgewertet, deren Teilkriterien nur aus Basiskriterien bestehen. Mit diesen bewerteten Hauptkriterien können dann sukzessiv weitere Hauptkriterien und schließlich das Wurzelkriterium ausgewertet werden.

3.4.3 Anpassungsmöglichkeiten

Um auf Veränderungen in den Untersuchten Szeanrios reagieren zu können, sind die gängigen Anpassungsmöglichkeiten der Struktur des Katalogs möglich. Das Herausnehmen von einzelnen Kriterien erfolgt unkompliziert und geschieht durch einfache Streichung des entsprechenden Kriteriums. Unvorhergesehenen Seiteneffekte wie sie in 3.3.3 beschrieben wurden, treten nicht auf. Das Hinzufügen von Kriterien ist ohne weiteres möglich. Die Zuordnung einer Gewichtung ist dabei in Abhängigkeit der bereits bestehenden Teilkriterien vorzunehmen. Durch die verwendete Methodik besteht dabei kein Unterschied, ob diese Operation nur mit einzelnen Kriterien oder ganzen Teilbäumen erfolgt.

4 Kriterienkatalog zur Bewertung forensischer Werkzeuge

Wie bereits in der Aufgabenstellung beschrieben soll mit Hilfe des Kriterienkatalogs die Bewertung von Werkzeugen der Computerforensik erfolgen. Der Fokus der Werkzeuge wurde dabei auf den Bereich der Analyse von Bitstream-Images eines Datenträgers eingeschränkt. Für den Bewertungsvorgang und damit die spätere Anwendung des Kriterienkatalogs galt es, neben den Leistungen die ein Kriterienkatalog von der Methodik her liefert, noch weitere Bedingungen zu erfüllen, welche einige Auswirkungen auf die Erstellung des Kriterienkatalogs ausübten.

Eine der Bedingungen gab vor, dass nicht nur einzelne Funktionen des Werkzeugs bewertet werden, sondern möglichst dessen volles Leistungsspektrum. Eventuell vorhandene Schwachstellen des Werkzeugs sollten dabei ebenfalls aufgezeigt werden. Hierfür war es notwendig, nahezu den kompletten Funktionsumfang eines Werkzeugs mittels Kriterien abzudecken. Dies gelang durch eine umfangreiche Kriteriensammlung, auf welche in Abschnitt 4.1 genauer eingegangen wird. Hierbei entstanden rund 30 Kriterien, welche eine umfassende Charakterisierung der Werkzeuge ermöglichen. Um bei dieser Anzahl nicht den Überblick zu verlieren, wurde der Kriterienkatalog einer gewissen Struktur unterworfen (Abschnitt 4.2). Des Weiteren sollte die Bewertung möglichst ohne lange Einarbeitungszeit in das Werkzeug durchführbar sein. Es musste also ein Vorgehen gefunden werden, welches erlaubt, die Bewertung zusammen mit dem erstem Umgang des Werkzeugs durchzuführen. Die Lösung hierfür wird im Abschnitt 4.3 dargelegt. Abgeschlossen wird das Kapitel mit den Beschreibungen der einzelnen Kriterien.

4.1 Erfassung der Kriterien

Zu Beginn der Erstellung des Kriterienkatalogs galt es zunächst Kriterien zu finden, welche die Analysefähigkeit der computerforensischen Werkzeuge charakterisieren. Hierzu wurden im wesentlichen Quellen aus zwei verschiedenen Bereichen verwendet: Literaturrecherche (Fachliteratur, Verfügbare Dokumente im Internet, Bedienungsanleitungen der Werkzeuge) und Anwendung des Analysewerkzeugs, wobei hier inhärent auf das Wissen von Mitarbeitern des Landeskriminalamts Bayern zurückgegriffen wurde, welche täglich mit diesen Werkzeugen arbeiten.

Die Bedienungsanleitungen und Leistungsbeschreibungen der Werkzeuge sind innerhalb der Literaturrecherche eine der Hauptquellen für die grundlegenden Funktionen der Werkzeuge gewesen (z.B. das Benutzerhandbuch von EnCase [Sof04a], Sleuthkit [Car04a]). Die Funktionen zur Analyse von Festplatten-Images wurden dabei thematisch gebündelt, um sie in Kriterien zusammenzufassen. Hieraus ergab sich ein Grundstock an Kriterien, der es ermöglichte die Analysefähigkeit aktueller Werkzeuge zu bewerten.

Die weitere Literaturrecherche anhand von Fachbüchern und verfügbaren Artikeln im Internet (siehe Literaturverzeichnis) lieferte vor allem Hintergrundwissen in Bezug auf das Thema Computerforensik und den bereits aus den Funktionsbeschreibung ermittelten Kriterien. Zusätzliche Kriterienpunkte wurden hierbei nicht ermittelt, die Bestehenden konnten aber verfeinert und genauer klassifiziert werden. Dass hier keine weiteren Kriterien ermittelt werden konnten, ist auf zwei Gründe zurückzuführen: Auf die Quantität der vorhandenen Fachliteratur und auf das Publikationsverhalten der einzelnen Firmen, welche im Bereich der Computerforensik arbeiten. Die vorhandene Fachliteratur ist derzeit bemüht, vor allem einen umfassenden Überblick über das Thema Computerforensik zu geben [Ges04], wie es in ähnlicher und gekürzter Weise in Kapitel 2 erfolgt ist. Eine Konzentration auf die einzelnen Phasen bzw. Bereiche der Computerforensik liegt aber noch nicht vor. Ähnlich sieht es mit den Publikationen der einzelnen Firmen in diesem Bereich aus. Viele sind bedacht, ihr eigenes Wissen zu schützen, da es Teil ihrer angebotenen Dienstleistungen ist. Die Publikationen beschränken sich daher meist auf das eigene Produkt, auf Fallstudien, welche die Leistungsfähigkeit des Produkts zeigen, oder auf allgemeine Themen, wie sie auch in der Fachliteratur erörtert werden.

Die restlichen Kriterienpunkte wurden unmittelbar aus dem Umgang mit den einzelnen Werkzeugen abgeleitet. Einerseits durch Anwendung der Werkzeuge auf zur Verfügung gestellte Testfälle aus dem Internet [Car04b], [Hon04] oder selbst erstellte Images, um den Umgang mit dem Werkzeug zu erlernen. Andererseits wurde auf den Erfahrungsschatz und das Wissen von Herrn Köllner vom Landeskriminalamt Bayern gesetzt, dessen Arbeitsbereich in der Analyse von Festplatten-Images liegt. Anhand den Schilderungen des täglichen Umgangs mit den Analysewerkzeugen und den dabei auftretenden Anforderungen, Funktionswünschen und Problemen, wurden weitere Punkte für die Bewertung der Werkzeuge abgeleitet und zu Kriterien zusammengefasst.

Während dieser Zeit der Erfassung ergaben sich immer wieder Kriterien, die für die allgemeine Bewertung eines Werkzeugs oder für ein spezielles Aufgabengebiet der Computerforensik sehr interessant wären, aber dennoch nicht Einzug in den Kriterienkatalog fanden bzw. nicht in den Bewertungsvorgang mit aufgenommen wurden. Dies waren vor allem Kriterien, die nur sehr subjektiv oder mittels eines sehr großen Testumfangs bewertet werden können (z.B. ob die Bedienung eines Werkzeugs „intuitiv“ erfolgt oder nicht). Diese nicht aufgenommen Kriterien werden im Abschnitt 4.5 auf Seite 99 kurz aufgeführt und besprochen.

4.2 Struktur des Kriterienkatalogs

Nach der Erfassung der Kriterien wurden diese thematisch geordnet und zu Gruppen zusammengestellt. Abhängig von dieser Thematik wurde aus den einzelnen Gruppen der Kriterienkatalog zusammengesetzt. Unter Berücksichtigung der in Abschnitt 3.4 (Seite 24) angegebenen Methodik ergab sich so ein Kriterienbaum, welcher in Abbildung 4.4 und 4.2 (Seite 34/35) graphisch dargestellt wurde. Bei der Erstellung des Kriterienkatalogs sind dabei folgende Strukturierungsmerkmale eingehalten worden.

Die Grobstruktur des Katalogs lässt sich durch zwei Teilbereiche beschreiben. Einerseits die Kriterien, welche eine Funktion des Werkzeugs bewerten, die direkt mit der Analyse des Festplatten-Images zusammenhängt. Andererseits alle Kriterien, die den Umgang mit dem Werkzeug beschreiben. Auf dieser Einteilung beruht auch die zweiseitige Darstellung des Kriterienkatalogs.

Innerhalb dieser zwei Bereiche wurde versucht, eine weitere Abstufung vorzunehmen. Aus hierarchischer Sicht befinden sich die obersten Teilkriterien[1] der beiden Bereiche auf gleicher Ebene. Führt man auf diese Bereiche einen postorder-Durchlauf[2] durch, so ergibt sich die in der graphischen Darstellung angedeutete vertikale Abstufung der Kriterien. Bei den allgemeinen Kriterien wurde hier versucht eine Konzentration von eher allgemein gültiger Kriterien, hin zu den speziellen (Analyse-) Kriterien zu verfolgen, welche den Schwerpunkt der Untersuchung bilden. Bei den Analyse-Kriterien wurde versucht, eine Abstrahierung zu modellieren, welche zunächst die Kriterien behandelt, welche sehr grundlegende Funktionen bewerten bzw. sehr nahe am untersuchten Image und dessen Daten liegen (z.B. Dateisystemunterstützung). Je weiter der vertikalen Abstufung nach unten gefolgt wird, desto mehr erfolgt eine Interpretation der Daten bzw. Dateien durch das Analysewerkzeug.

Schließlich besteht noch innerhalb der Gruppierung der einzelnen Basiskriterien eine weitere Strukturierung. Hier wurde die Abfolge so aufeinander abgestimmt, dass die Beschreibung der Kriterien aufeinander aufbauen kann, um die Verständlichkeit der einzelnen Kriterien zu erhöhen.

4.3 Gewichtung und Bewertung der Kriterien

Die Gewichtung der einzelnen Kriterien gestaltete sich schwierig, da kein Standard existiert, an welchem die Wichtigkeit der einzelnen Kriterien im Vergleich zueinander abgeschätzt werden könnte. Desweiteren ist die Wichtigkeit oder Notwendigkeit der einzelnen Kriterien, und damit der bewerteten Funktionen, inhärent vom spezifischen Fall abhängig. In vielen Fällen wird die volle Funktionalität eines Werkzeugs gar nicht benötigt, ein Teil der Kriterien ist also für diesen Fall nicht von Bedeutung (z.B. die Analysefähigkeit von Mailboxen, wenn sich gar keine Mailanwendung auf dem untersuchten Image befindet). Deswegen sind diese Kriterien aber nicht weniger wichtig, nur weil sie aktuell nicht benötigte Funktionen bewerten.

Als Grundlage für die Gewichtung wurde daher zum Einen das aus der Fachliteratur angeeignete Wissen verwendet. Kriterien, die relativ häufig Verwendung finden oder grundlegende Eigenschaften für eine Untersuchung zu Verfügung stellen (z.B. Wiederherstellung gelöschter Dateien in Kriterium 4.2.1 auf Seite 61), wurden höher bewertet als solche, die eher unterstützende Wirkung besitzen und auch auf anderem Weg, wenn

[1] Zur Semantik der Baumstruktur siehe Kapitel[3]

[2] Bei der Betrachtung einer Baumstruktur, wird bei einem postorder-Durchlauf zunächst die Wurzel betrachtet. Anschließend der komplette Teilbaum, welcher sich am weitesten rechts befindet und danach in Reihenfolge die Teilbäume, welche sich links davon befinden.

auch umständlicher, erreicht werden könnten (z.B. die Aufbereitung von Daten oder die Bereitstellung verschiedener Suchalgorithmen). Zum Anderen wurde hier wiederum auf die Erfahrung von Herrn Köllner zurückgegriffen, dessen Einschätzung der Kriterien beim täglichen Umgang mit dem Werkzeug, einen entscheidenden Teil ausmachte.

Bei der Erstellung der Bewertungsmaßstäbe für die Kriterien mussten zwei Bedingungen beachtet werden, welche konträr zueinander stehen. Einerseits wird von einem Kriterium erwartet, dass es den bewerteten Vorgang umfassend beschreibt und alle Aspekte zu seiner Charakterisierung berücksichtigt, so dass durch die Bewertung ein aussagekräftiges Ergebnis, über die Leistung des untersuchten Vorgangs, vorliegt. Andererseits war es eine Prämisse des Kriterienkatalogs, eine einfache und schnelle Möglichkeit zu liefern, die Werkzeuge der Computerforensik zu analysieren, ohne sich vorher lange mit ihnen zu beschäftigen.

Eine umfassende Bewertung eines Kriteriums, oder anders ausgedrückt, eine qualitative Aussage, wie gut ein Analysewerkzeug einen Vorgang erfüllt (hierzu gehört auch das Ergebnis des Vorgangs), ist aber nur mit zahlreichen Testfällen und genauer Beobachtung des Vorgangs zu erreichen. Diesen Ansatz befolgt zum Beispiel das Computer Forensics Tool Testing Project (CFTT) [CFT04], welches einen Rahmen vorgibt, der zur Erstellung von Bewertungen für Werkzeuge vorgesehen ist. Dieser ist aber so umfangreich, dass allein die Bewertung einer Funktion, welche im vorliegenden Katalog in etwa einem Kriterium entspricht, den Umfang einer eigenen Fallstudie annimmt (z.B. umfasst eine dort angebotene Studie, welche die Fähigkeit Bitstream-Images zu erstellen bewertet, über 50 Tests).

Für die vorliegende Arbeit wurde daher ein anderer Weg der Bewertung eingeschlagen, welcher eher einen quantitativen Charakter beinhaltet. Jedes Kriterium wird zunächst eingehend beschrieben, um den Anwender des Katalogs mit der entsprechenden Gebiet der forensischen Analyse vertraut zu machen. Anschließend werden ein, oder mehrere (kriterienspezifische) Eigenschaften aufgeführt, die das analysierte Werkzeug unterstützen sollte. Der Bewertungsmaßstab ist also davon abhängig, wie viele solcher (sinnvollen) Eigenschaften pro Kriterium gefunden wurden. Die Bewertung eines Kriteriums erfolgt dann in Abhängigkeit von der Anzahl der erfüllten (kriterienspezifischen) Eigenschaften. Dies ermöglicht eine schnelle und einfache Bewertung der Kriterien, da anhand der Beschreibungen des Kriteriums, in den meisten Fällen die nötigen Informationen im Benuterhandbuch zu finden sind und anschließend an einem Test-Image verifiziert werden können (siehe Kapitel 5 Seite 101).

Das Verfahren ermöglicht auf relativ einfache Weise die Fähigkeiten eines Werkzeugs der Computerforensik zu analysieren und eine Aussage über das entsprechende Werkzeug abzuleiten. Ist eine qualitative Aussage über die Leistungsfähigkeit und Ergebnisse der einzelnen Funktionen oder gar des ganzen Werkzeugs gewünscht, bleibt hingegen nur die Möglichkeit des oben erwähnten Computer Forensics Tool Testing Projects. Dies wäre aber mit einem sehr großen Kriterienkatalog und einer dementsprechend längeren und aufwändigeren Beurteilung verbunden.

4.4 Beschreibung der Kriterien

Die einzelnen Kriterien werden in der Reihenfolge eines postorder-Durchlaufs des Kriterienbaumes (Abbildung 4.4 und 4.2 auf der nächsten Seite) aufgeführt. Für ein schnelles Auffinden der einzelnen Kriterien wird dieser Durchlauf ebenfalls in tabellarischer Form angegeben (Tabelle 4.1 Seite 36).

Wurzelkriterium
WERKZEUGE DER COMPUTERFORENSIK

Kriterium	Gewicht
Werkzeug Computerforensik	
Anwender Support	2
Bedienung des Werkzeugs	3
Protokollierung	2
Analyse	4

Die Werkzeuge der Computerforensik werden anhand der Gebiete *Anwender Support, Bedienung des Werkzeugs, Protokollierung* und *Analyse* bewertet. Die *Analyse* ist hierbei der wichtigste Bereich, da von ihr die Ergebnisse der forensichen Untersuchung abhängen. Die *Bedienung des Werkzeugs* wird als sehr wichtig eingestuft, da aussagekräftige Ergebnisse nur mit dem sachgemäßem Umgang des Werkzeugs möglich sind, welches den Anwender so gut es geht unterstützt.

In der Bewertung des Kriterienkatalogs findet der *Anwender Support* nur dann eine Anwendung, wenn ein Problem mit dem Werkzeug auftritt. Geht man von einem funktionierenden und durchdachten Werkzeug aus, sollte dieser also nur bei einem Fehler im Programm kontaktiert werden und daher eher selten gebraucht werden. Des Weiteren wird beim Gebrauch von allgemein verfügbarer Software in vielen Fällen der Support nicht kontaktiert, sondern eine Fehlfunktion als gegeben hingenommen. In diesem Zusammenhang wird der *Anwendung Support* als wichtig eingestuft.

Ähnliche Überlegung gelten für die *Protokollierung*, welche ebenfalls als wichtig eingestuft wird, da hier nur zusätzliche Leistungen (z.B. eine automatische Protokollierung) bewertet werden. Es wird davon ausgegangen, dass die einzelnen Funktionen der Analyse ein entsprechendes Ergebnis liefern, welches zum Beispiel auch von Hand in einen Bericht übernommen werden könnte.

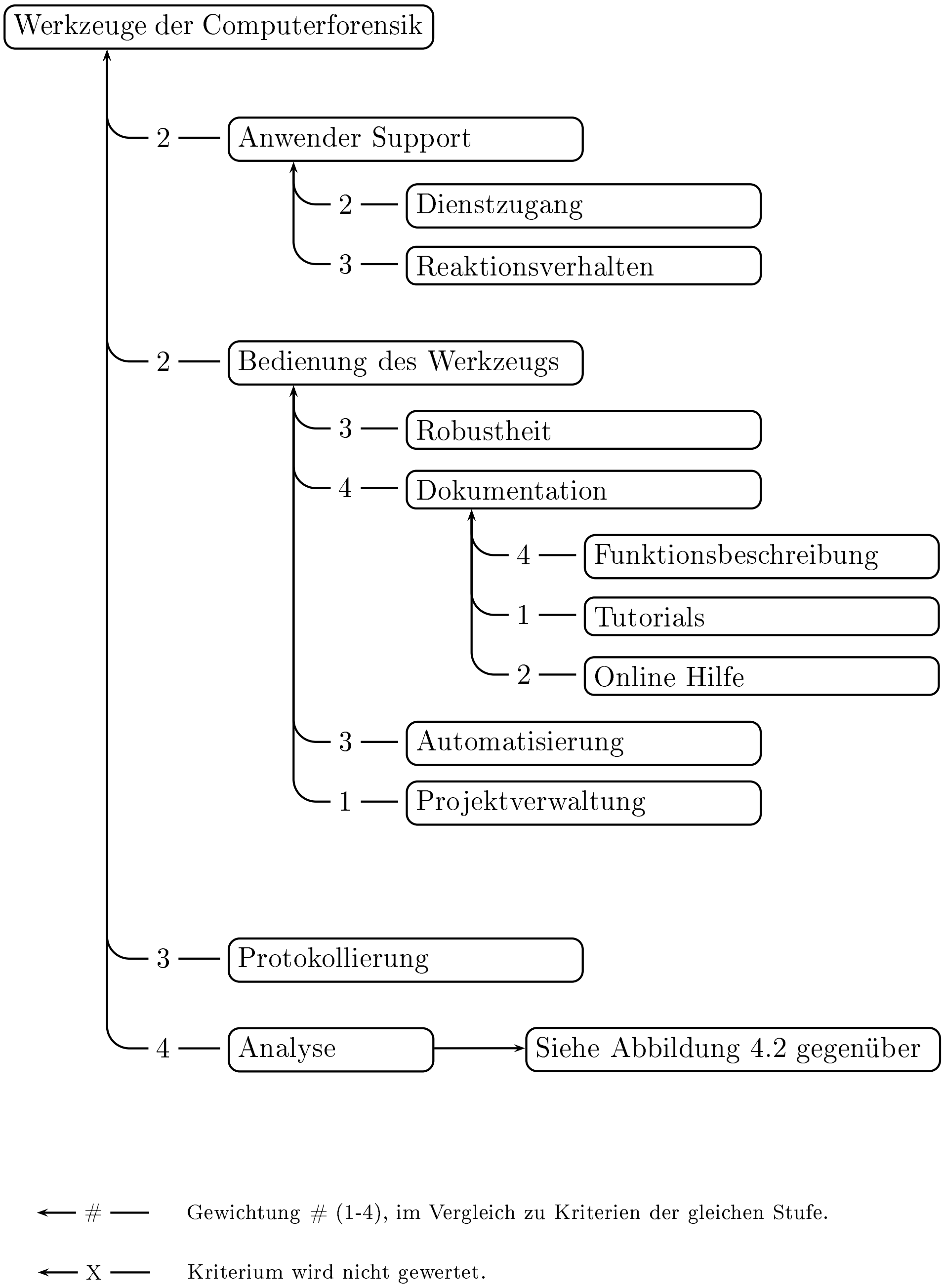

Abbildung 4.1: Kriterienkatalog (Allgemeine Kriterien)

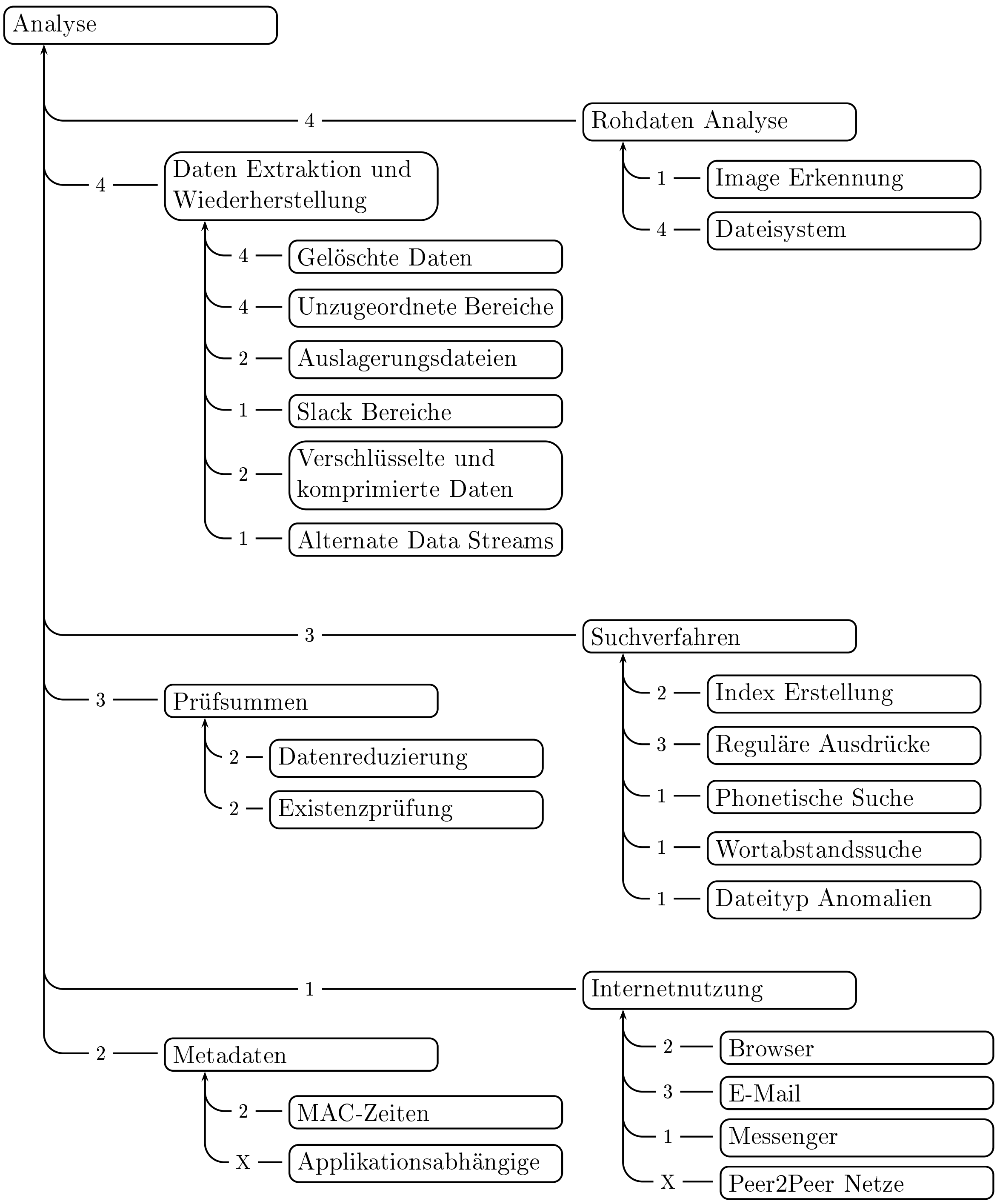

Abbildung 4.2: Kriterienkatalog (Analyse Kriterien)

Kriterium	**Titel**	**Seite**
1	Anwender Support	37
1.1	Dienstzugang	37
1.2	Reaktionsverhalten	38
2	Bedienung des Werkzeugs	40
2.1	Robustheit	41
2.2	Dokumentation	43
2.2.1	Funktionsbeschreibung	44
2.2.2	Tutorials	46
2.2.3	Online Hilfe	47
2.3	Automatisierung	49
2.4	Projektverwaltung	50
3	Protokollierung der Untersuchung	52
4	Analyse	54
4.1	Rohdaten Analyse	56
4.1.1	Image Erkennung	56
4.1.2	Dateisystem Unterstützung	58
4.2	Daten Extraktion und Wiederherstellung	60
4.2.1	Gelöschte Daten	61
4.2.2	Nicht zugeordnete Bereiche	63
4.2.3	Slack Bereiche	64
4.2.4	Auslagerungsdateien und Swap-Partitionen	66
4.2.5	Verschlüsselte und komprimierte Daten	68
4.2.6	Alternate Data Streams	69
4.3	Suchverfahren	71
4.3.1	Index Erstellung	71
4.3.2	Reguläre Ausdrücke	75
4.3.3	Phonetische Suche	77
4.3.4	Wortabstandssuche	79
4.3.5	Dateityp Anomalien	80
4.4	Prüfsummenbildung	82
4.4.1	Datenreduzierung	84
4.4.2	Existenzprüfung	85
4.5	Internet Benutzung	87
4.5.1	Internetbrowser	88
4.5.2	E-Mail Anwendung	90
4.5.3	Messenger	92
4.5.4	Peer to Peer Netze	93
4.6	Metadaten	95
4.6.1	MAC-Zeiten	96
4.6.2	Applikationsabhängige Metadaten	98

Tabelle 4.1: Tabellarische Übersicht der Kriterien

Kriterium 1
ANWENDER SUPPORT

Kriterium	Gewicht
Anwender Support	
Dienstzugang	2
Reaktionsverhalten	3

Der Anwender Support als Teilgebiet des IT Service Management ist ein umfangreicher Bereich, welcher unter anderem die Interaktion zwischen Anwender und Dienst Anbieter beschreibt. Es existieren diverse Standards (z.B. IT Infrastructure Library (ITIL) [ITI04], enhanced Telecom Operation Map (TOM) [Int04a]), die den Aufbau und die Leistungen des Anwender Supports genauer spezifizieren. Diese sind in der Regel sehr umfassend, und eine darauf basierende Bewertung entspricht durchaus dem Umfang eines eigenständigen Kriterienkatalogs bzw. einer Diplomarbeit, wie es zum Beispiel in [Bre02] erfolgt ist. Des Weiteren wäre eine Beurteilung des Supports ohne Kenntnisse und Beobachtungen der inneren Struktur des Dienstanbieters kaum möglich, da diese inhärenter Bestandteil des Dienstes ist.

Bei der vorliegende Arbeit reicht es hingegen aus, nur einen kleinen Teil des Anwender Supports zu betrachten. Aus der Sicht eines Benutzers, welcher den „Anwender Support“ in Anspruch nimmt, lässt sich die Bewertung dieses Dienstes auf zwei Punkte reduzieren. Zum Einen, welche Kommunikationsmöglichkeiten bestehen, den Dienst zu erreichen (*Dienstzugang*). Zum Anderen, wie das Reaktionsverhalten des Supports auf eine Anfrage ist. Die Verfügbarkeit wird dabei als wichtig angesehen, da sie dafür entscheidend ist, wie dieser Dienst genutzt wird. Im Vergleich dazu ist das *Reaktionsverhalten* als sehr wichtig anzusehen, da beim Vorhandensein eines Dienstes erwartet wird, dass dieser ein Ergebnis liefert. Die Art der Kontaktaufnahme (EMail, Telefon, usw.) wird also im Verhältnis zur Leistung des Supports herabgestuft.

Kriterium 1.1
DIENSTZUGANG

Kriterium	Gewicht
Support	
Dienstzugang	

Ein Hersteller hat die unterschiedlichsten Möglichkeiten, dem Benutzer Zugang zum Anwender Support zu gewähren. Die klassische Variante wäre das Einrichten einer Hotline, die einen direkten und persönlichen Kontakt erlaubt. Alternativen wie EMail, welche eine asynchrone, aber dennoch persönliche Kommunikation, bietet, oder ein Web-Forum, welches einer öffentlichen Diskussionsrunde entspricht, sind mittlerweile ein fast obligatorisch angebotener Dienst. Für die Bewertung des Kriteriums ist nur die Anzahl der

Möglichkeiten des Dienstzugangs ausschlaggebend, welche vom Hersteller für die Kontaktaufnahme zum Support zu Verfügung gestellt werden.

Anforderungen:

- Eine telefonische Hotline wird angeboten.
- Die Kontaktaufnahme mittels EMail wird angeboten.
- Eine öffentliche Diskussionsrunde wird angeboten.
  (z.B. Web-Forum, Mailing-Liste, Newsgroup)
- Ein Servicevertrag mit speziellen Leistungen (z.B. 24h-Vor-Ort Service, persönliche Ansprechpartner, etc.) wird angeboten.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 1.2
REAKTIONSVERHALTEN

Kriterium	Gewicht
Support Reaktionsverhalten	

Das Reaktionsverhalten des Anwender Support lässt sich grob durch zwei Merkmale charakterisieren: erstens wie lange man auf eine Reaktion warten muss, zweitens wie diese ausfällt.

Beide Punkte lassen sich aber nur sehr schwer bewerten. Insbesondere ist die Art der Antwort für den Anfragenden interessant. Bei ihrer Beurteilung spielen aber die unterschiedlichsten Punkte eine Rolle, zum Beispiel ob die Antwort verständlich war, ob sie weitergeholfen hat oder ob das Problem grundsätzlich gelöst wurde oder nur ein ein „Workaround“ gefunden wurde. Das Testen dieser qualitativen Merkmale ist aber äußerst problematisch. Hierfür müssten diverse Testanfragen an den Support gestellt werden und die entsprechenden Antworten beurteilt werden. Mit diesem Verfahren können aber nur Antworten auf Standardfragen getestet werden, weil neue Anfragen bezüglich einer Fehlfunktion einerseits sehr schwer gefunden werden und andererseits in der Regel nur einmal gestellt werden können. Dies beruht darauf, dass eine einmal gestellte Frage dem Support bekannt sein sollte (es ist also eine Standardfrage) bzw. die Fehlfunktion nach dieser behoben wird und somit das Problem nicht mehr besteht.

Die Überprüfung mittels Standardfragen ist aber auch aus einem weiteren Grund nicht für den Katalog geeignet. Die Anfrage und das Warten auf eine Antwort kostet natürlich seine Zeit und verhindert so eine zügige Beurteilung des Kriteriums. Hier bieten sich als Quelle die in der Regel öffentlich verfügbaren Diskussionsrunden an, welche die unterschiedlichsten Anfragen beinhalten und so einen guten Überblick über das bisherige Reaktionsverhalten liefern. Die Frage nach der Qualität der Antwort besteht aber weiterhin. Hierfür müsste ein Bewertungsschlüssel gefunden werden, mit welchem die Qualität dieser Antworten eingeordnet wird. Dieser Bewertungsschlüssel wäre aber sehr umfangreich, da unterschiedliche Merkmale (z.B. Verständlichkeit, Umfang) bei der Qualität einer Antwort eine Rolle spielen und auch die Bedeutung für den Anfragenden individuell verschieden ist (z.B. ist eine Aussage „kommt in der nächsten Version“ für den einen ausreichend, für jemand anderen aber nicht tragbar). Auf die Frage wie eine Reaktion ausfällt, kann im Zuge der vorliegenden Arbeit also nicht genauer eingegangen werden.

Es bleibt also noch die Beurteilung der Reaktionszeit, welche mit Hilfe der oben erwähnten öffentlichen Diskussionsrunden relativ leicht ermittelbar ist. Auch hier sollten einige Punkte beachtet werden. Einerseits die Zeiterintervalle, die für den Maßstab verwendet werden. Aufgrund des internationalen Charakters der Diskussionsrunden ist eine eventuell vorhandene Zeitverschiebung zu berücksichtigen. Die Skala sollte also nicht allzu fein ausfallen. Andererseits halten sich in öffentlichen Diskussionsrunden häufig fachkundige Personen auf, die nicht zum offiziellen Support Team gehören, aber dennoch qualifizierte Antworten geben. In vielen Diskussionsrunden hat es sich eingebürgert, dass korrekte Antworten nicht extra vom Support bestätigt werden (sondern nur falsche korrigiert). Bei einer Beurteilung sollten diese Antworten also mitgerechnet werden, da bei einer nicht Beantwortung durch dritte, sehr wahrscheinlich der offizielle Support reagiert hätte.

Für eine genaue Auswertung wäre es notwendig, alle vorhanden Fragen zu betrachten und sich die Reaktionszeiten zu notieren. Diese würde je nach Größe der Diskussionsrunde aber wieder einen erheblichen zeitlichen Aufwand erfordern. Des Weiteren existieren natürlich immer wieder Anfragen, die aus unterschiedlichen Gründen aus der Reihe fallen (z.B. Spassanfragen, Fragen welche gar nichts mit dem Werkzeug zu tun haben, Fragen die doppelt gestellt worden sind, usw.). Diese würden ein Ergebnis stark verfälschen, und es müsste wiederum ein eigens System zur Bewertung dieser Fragen gefunden werden. Im Sinne einer einfachen Beurteilung des Kriteriums wurde der Bewertungsmaßstab deswegen so gewählt, dass das allgemeine Reaktionsverhalten des Supports bewertet wird.

Für eine Beurteilung ist es also ausreichend, sich einen Überblick der entsprechende Diskussionsrunde zu verschaffen und dann eine passende Kategorie auszuwählen.

Erscheinungsformen:

A Eine Reaktion erfolgt in der Regel innerhalb von 24 Stunden.

B Eine Reaktion erfolgt innerhalb von 3 Tagen.

C Eine Reaktion erfolgt innerhalb einer Arbeitswoche.

D Es ist nur ein sporadisches Reaktionsverhalten ersichtlich, d.h. nicht alle Anfragen werden beantwortet.

E Es ist kein Reaktionsverhalten ersichtlich.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 2
BEDIENUNG DES WERKZEUGS

Kriterium	Gewicht
Bedienung des Werkzeugs	
Robustheit	3
Dokumentation	4
Automatisierung	3
Projektverwaltung	1

Unter der Bedienung des Werkzeugs fällt die gesamte Interaktion zwischen Anwender und Software. Dies ist ein umfassendes Gebiet, dass in vielen Teilgebieten durch subjektive Eindrücke geprägt wird. Hierunter fällt zum Beispiel die intuitive Bedienung, also die Möglichkeit die Funktionalität des Programmes aufgrund des eigenen Erfahrungsschatzes zu nutzen, ohne vorher die Bedienungsanleitung zu lesen. Ähnlich verhält es sich mit Punkten wie der Übersichtlichkeit und Bedienbarkeit, also der effizienten Nutzung des Werkzeugs, wenn man seine Funktionalität beherrscht. Diese Kriterien sind, wenn überhaupt, nur mittels umfangreicher (Anwender-) Tests zu bewerten. Für den vorliegenden Kriterienkatalog wurde daher auf die Bewertung dieser überwiegend subjektiven Kriterien verzichtet. Es wurden nur Kriterien ausgewählt, deren Bewertung objektiv durch den Anwender des Kriterienkatalogs erfolgen kann.

Die *Robustheit* beschreibt das wohldefinierte Verhalten des Werkzeugs auf Benutzer- oder Programmeingaben. Dieses ist im Vergleich zu den anderen Punkten sehr wichtig, da ansonsten ein zuverlässiges Arbeiten am Fall nicht möglich ist. Die *Dokumentation* des Werkzeugs ist entscheidend dafür, in wie weit der Anwender die Fähigkeiten des Werkzeugs ausschöpft und sich mit diesen auseinandersetzt. Sie ist daher als äußerst wichtig anzusehen. Die *Automatisierung* von Untersuchungsschritten wird als sehr wichtig eingestuft, da sie eine der Hauptaufgaben für die Verwendung von Werkzeugen ist und eine erhebliche Reduzierung des Arbeitsaufwandes ermöglicht.

Die *Projektverwaltung* gestaltet den Verlauf einer Untersuchung übersichtlicher, da es die einzelnen Bitstream-Images verwaltet und die Ergebnisse geordnet ablegt. Das Teilkriterium wird dennoch als weniger wichtig im Vergleich zu den anderen Kriterien gewertet, da es zwar eine Erleichterung beim Arbeitsaufwand bietet, die gleiche Funktionalität aber ohne weiteres auch manuell mit einem entsprechendem Ablagekonzept machbar wäre.

Kriterium 2.1
ROBUSTHEIT

Kriterium	Gewicht
Bedienung des Werkzeugs	
Robustheit	3

Ein Programm heißt robust, wenn es in Ausnahmefällen in einen definierten Zustand übergeht. Ausnahmefälle bezeichnen hier Situationen, welche nicht ausdrücklich in der Programmspezifikation angegeben sind. Diese können zum Einen durch das Ausführen von Operationen auftreten, die auf den aktuell vorliegenden Daten oder Ergebnissen nicht anwendbar sind (z.B. die Interpretation von beliebigen Binärdaten als Bilddatei). Zum Anderen durch fehlerhaften Programmcode, der Seiteneffekte hervorruft, die nicht sinnvoll weiterverarbeit werden können (z.B. die Übergabe eines ungültigen Parameters).

Zu beachten ist, dass dieses Kriterium nicht bewertet, ob und wie viele solcher Situationen während der Anwendung auftreten, sondern nur wie die Reaktion auf solch eine Situation ist! Hierfür wäre ansonsten ein eigenes Kriterium notwendig (z.B. Vorhandensein von Bugs).

Der Übergang in einen definierten Zustand kann unterschiedlichen Auflagen genügen. Am wichtigsten ist hier, dass das Auftreten eines Ausnahmefalls, zu keinem unkontrolliertem Abbruch („Absturz“) oder Einstellung der Reaktion („Aufhängen“) des Programms führt. Des Weiteren sollte der Benutzer dabei so weit wie möglich über die verursachenden Probleme informiert werden und wenn möglich Lösungen angeboten bekommen, um diese zu vermeiden und vernünftig weiterarbeiten zu können. Treten hierbei Inkonsistenzen im Datenbestand auf, zum Beispiel wenn nur ein Teil der Daten manipuliert wurde, sollte dies dem Benutzer ausführlich mitgeteilt werden, da unter diesen Umständen ein Wiederaufnehmen der Untersuchung eventuell nicht sinnvoll ist.

Um solche Ausnahmefälle zu rekonstruieren und das entsprechende Verhalten zu bewerten, bieten sich mehrere Quellen an: zum Beispiel eine eventuell vorhandene Diskussionsrunde innerhalb des Supports (siehe Kriterium 1), eine vom Hersteller entsprechend zu Verfügung gestellte Liste von Fehlerverhalten (Bugliste) und Recherche im Internet (z.B. „Name des Programms + Fehler“ oder „+ Absturz“ bzw. die entsprechenden englischen Ausdrücke bug, error, crash usw.). Sind keine solchen Ausnahmefälle bekannt bzw. treten keine auf, obliegt es dem Anwender des Kriterienkatolgs hier eine Einschätzung vorzunehmen. Ist der Beobachtungszeitraum ausreichend lang und ist eine Einsicht in das System und die Arbeitsweise des Werkzeugs möglich (z.B. Open Source Projekt), so kann hier eventuell Punkt A oder B vergeben werden. Ist diese Einschätzung nicht möglich oder zu unsicher, ist das Kriterium zu streichen.

Erscheinungsformen:

D Ein robustes Verhalten ist nicht zu erkennen. Bei einer nicht erlaubten Aktion beendet sich das Programm ohne Vorwarnung oder reagiert nicht mehr.

C Vor dem Übergang in einen undefinierten Zustand gibt das Werkzeug eine Fehlermeldung aus, welche bei einer Diagnose des Vorgangs und einer evtl. möglichen Vermeidung hilfreich sein können.

B Das Programm verhält sich robust. Beim Auftreten eines Fehlers wird dies angezeigt und die entsprechende Operation abgebrochen. Danach ist ein normales Weiterarbeiten möglich. Bereits ermittelte Teilergebnisse dieser Operation gehen verloren oder werden nicht gemeldet.

A Wie B, aber bereits ermittelte Teilergebnisse der Operation gehen nicht verloren, sondern stehen zur Ansicht zu Verfügung.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	kaum erfüllt	1
D	nicht erfüllt	0

Kriterium 2.2
DOKUMENTATION

Kriterium	Gewicht
Bedienung des Werkzeugs	
Dokumentation	
Funktionsbeschreibung	4
Tutorials	1
Online Hilfe	2

Die Dokumentation ist ein wesentlicher Teil jedes Softwarepakets und beinhaltet alle Informationen, welche dem Benutzer eines Produkts zur Verfügung gestellt werden. Für die Bewertung des Analysewerkzeugs sind dabei zwei Punktes besonders hervorzuheben: zum Einen ist die Dokumentation notwendig, um die Bedienung des Programms zu erlernen. Dies beruht darauf, dass die Computerforensik einerseits ein sehr neues Themengebiet ist, andererseits einen vielschichtigen und breiten Bereich einer Wissenschaft abdeckt und somit die zugehörigen Werkzeuge sehr umfangreich sind. Ein Erlernen, zum Beispiel durch „learning by doing“ oder eine intuitive Bedienung, wie es in etwa bei einer Textverarbeitung durchaus üblich ist, ist daher kaum oder fast gar nicht möglich. Zum Anderen, ist eine Dokumentation notwendig, um im laufenden Betrieb über bestimmte Arbeitsweisen des Programms zu recherchieren, da aus oben genannten Gründen eine vollständige Beherrschung des gesamten Funktionsumfanges eines Werkzeugs in den meisten Fällen nicht bzw. erst nach langer Einarbeitungszeit möglich ist.

Die Dokumentation umfasst dabei folgende Gebiete, welche als eigenständige Teilkriterien behandelt werden:

- Funktionsbeschreibung
  Beschreibung und Auswirkungen aller Programmfunktionen.
- Tutorials
  Schritt für Schritt Erklärungen grundsätzlicher Vorgehensweisen.
- Online Hilfe
  Vom Werkzeug zur Verfügung gestellte Hilfeleistungen zu den einzelnen Programmfunktionen.

Die Funktionsbeschreibung wird dabei als äußerst wichtig angesehen, da sie sowohl zum Erlernen des Programms und seiner Funktionen als auch zum späteren Nachschlagen unumgänglich ist. Das Vorhandensein von Tutorials wird im Vergleich dazu als weniger wichtig eingestuft, da sie vor allem in der Anfangsphase eine schnelles Erlernen der Funktionsweise ermöglichen. Zu einem späteren Zeitpunkt werden sie aber in der Regel nicht mehr gebraucht. Des Weiteren gestaltet sich ihre Bewertung im Vergleich zu den anderen Kriterien ein wenig undifferenziert (siehe Kriterienbeschreibung). Die Online Hilfe wird als wichtig eingestuft, da sie während der Arbeit unterstützenden Charakter bietet, den Arbeitsfluss aufrecht erhält und so ein zügiges und konzentriertes arbeiten ermöglicht.

Die eigentliche Bewertung der einzelnen Teilkriterien gestaltet sich schwierig, da die Einschätzung einer Dokumentation oft von persönlichen Vorlieben (z.B. ob das Handbuch in gedruckter Form oder als elektronisches Dokument vorliegt) oder dem Wissensstand des Anwenders abhängt. Eine vollständig objektive Bewertung der Dokumentation würde aber den Rahmen dieser Arbeit sprengen und zu einem eigenständigen Kriterienkatalog führen. Dieser könnte aber ohne Probleme an dieser Stelle in den aktuellen Kriterienkatalog eingehängt werden (siehe Abschnit 3.4.3 Seite 27).

Um die Bewertung der einzelnen Kriterien übersichtlich zu halten, werden deshalb nur die wichtigsten Aspekte einer Dokumentation untersucht. Für die drei Teilkriterien sind dabei folgende gemeinsame Punkte zu berücksichtigen.

- Verfügbarkeit
  Ist überhaupt eine Dokumentation vorhanden und wenn ja, ist der Zugriff auf diese ohne Probleme möglich. Liegt sie also zum Beispiel dem Produkt bei oder ist sie nur auf Umwegen zu erlangen. Falls sie in elektronischer Form vorliegt, werden auch die entsprechenden Darstellungsprogramme mitgeliefert oder müssen diese separat beschaffen werden.

- Vollständigkeit
  Alle in der Dokumentation beschriebenen Funktionen oder Verfahren finden sich im Programm wieder und zeigen die beschriebene Wirkung. Umgekehrt sollten alle Funktionen des Werkzeugs auch in seiner Dokumentation beschrieben sein.

- Ergiebigkeit
  Die einzelnen Funktionen oder Verfahren sind ausreichend beschrieben und es werden die häufigsten Fragen zu diesem Thema beantwortet. Schwierige Sachverhalte werden mittels Beispielen verdeutlicht.

- Struktur
  Die einzelnen Punkte sind leicht aufzufinden, zum Beispiel mittels verschiedener Inhaltsverzeichnisse oder Indizes, und übersichtlich und einheitlich dargestellt. Themenverwandte Gebiete werden auch zusammenhängend präsentiert.

Weitere spezifische Punkte werden in den Beschreibungen der Teilkriterien behandelt.

Kriterium 2.2.1
FUNKTIONSBESCHREIBUNG

Kriterium	Gewicht
Bedienung des Werkzeugs	
Dokumentation	
Funktionsbeschreibung	4

Die Funktionsbeschreibung (oder auch Benutzerhandbuch) ist ein essentieller Bestandteil der Dokumentation. Sie liefert eine Beschreibung für die korrekte Bedienung eines Werkzeugs und soll dem Benutzer den Umgang mit diesem Werkzeug auf einfache Weise vermitteln. Generell ist es ein zusammenhängender Text, welcher zuerst die allgemeinen Funktionsweisen des Werkzeugs beschreibt und anschließend auf die einzelnen Teilgebiete genauer eingeht.

Für die Bewertung des Kriteriums sind insbesondere die im Oberkriterium genannten Punkte in Bezug auf Verfügbarkeit, Vollständigkeit, Ergiebigkeit, und Struktur zu überprüfen. Ist die Verfügbarkeit noch relativ einfach zu ermitteln und somit eine Beurteilung durchzuführen, so gestaltet sich die anderen Punkte ein wenig schwieriger.

Die Beurteilung der Struktur der Dokumentation wird der Einschätzung des Anwenders überlassen, da diese einerseits vom verwendeten Medium (gedrucktes Buch, Hypertext Dokument) abhängig ist, andererseits aber auch sehr subjektiven Kriterien unterliegt. Es wird daher nur überprüft, ob eine einigermaßen passable Struktur der Dokumentation vorliegt. Anhaltspunkte hierfür wären ein Index und/oder ein Inhaltsverzeichnisses, die übersichtliche Darstellung, eine leichte Navigation, oder die Zusammenfassung themenverwandter Gebiete.

Bei der Vollständigkeit der Dokumentation stellt sich die Frage, wie man diese feststellen kann. In der Regel wird die Bewertung eines Analysewerkzeugs ja vor dessen Einsatz oder während eines Testbetriebes ermittelt. Hier auf Diskrepanzen zwischen der Beschreibung und der Programmfunktion zu stoßen, wäre eine Sisyphusarbeit oder Glücksache. Ähnlich sieht es mit der Ergiebigkeit aus, welche sich oft erst bei einem konkreten Problem zeigt.

Als Lösung bietet sich der Analyse Teil des vorliegenden Kriterienkatalogs an. Alle dort aufgeführten Kriterienpunkte sollten sich in der Funktionsbeschreibung des Werkzeugs wiederfinden, sofern sie vom Werkzeug unterstützt werden. Dies bedeutet natürlich auch, dass man für die Anwendung des Kriterienkatalogs nicht alleine auf das Handbuchs zurückgreifen kann, sondern zusätzliche Quellen hinzuziehen muss (z.B. Fachliteratur, den Support oder Personen, die bereits mit dem Produkt arbeiten). Die Beschreibung sollte dann ausreichend sein, um das Kriterium nachvollziehen und größtenteils bewerten zu können. Für die Ergiebigkeit bietet es sich eventuell zusätzlich an, gewisse Szenarios oder Aufgaben (Abschnitt 5.2 Seite 103) durchzuspielen.

Anforderungen:

- Eine zusammenhängende Funktionsbeschreibung ist verfügbar, zum Beispiel in Buchform mitgeliefert, auf der Webseite zum Herunterladen und Ausdrucken bereitgestellt, als Hypertext Dokument beim Programm mitgeliefert.
- Die Beschreibung der einzelnen Funktion ist ausreichend, um diese nachzuvollziehen und eine Bewertung des entsprechenden Kriteriums durchzuführen. (Ergiebigkeit)
- Die Funktionsbeschreibung ist übersichtlich strukturiert (siehe Text).
- Alle Kriterien des Katalogs werden in der Dokumentation beschrieben, sofern sie vom Werkzeug unterstützt werden. (Vollständigkeit)

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 2.2.2
TUTORIALS

Kriterium	Gewicht
Bedienung des Werkzeugs	
Dokumentation	
Tutorials	1

Ein Tutorial (im engl. als HowTo zu finden) ist eine Schritt-für-Schritt Anleitung, welche anhand von Beispielen erklärt, wie grundlegendes arbeiten mit dem Werkzeug vollzogen oder bestimmte Ergebnisse erzielt werden können. In der Regel wird hierbei jede Aktion und deren Ergebnis genau erklärt und durch zusätzliche Medieninhalte (z.B. Bilder, Filme, Sprache) verdeutlicht.

Hieraus ergibt sich auch eine Einschränkung bei dem im Oberkriterium genannten Punkten, welche ein Kriterium erfüllen muss. Durch die Schritt-für-Schritt-Vorgabe ist die Struktur streng vorgegeben, und ein bestimmte Funktion wird vollständig und eingehend beschrieben, da dies ja gerade der Sinn eines Tutorials ist. Somit wäre auch die Ergiebigkeit abgehakt. Hier ließe sich natürlich über die Qualität des Tutorials streiten, welche aber zumeist nur subjektiv bewertet werden kann. Hierzu einen objektiven Maßstab zu finden (z.B. ob eine kurze prägnante Angabe der durchzuführenden Aktionen „qualitativ hochwertiger“ ist, als ein Film, der diesen Vorgang zeigt) ist aber eine aufwändige Angelegenheit, die im Rahmen der vorliegenden Arbeit nicht durchgeführt werden kann. Die Qualität wird daher nicht in der Bewertung aufgenommen.

Bleibt also noch, die Vollständigkeit und Verfügbarkeit im Bezug auf Tutorials zu klären. Tutorials werden in der Regel nur für die grundlegenden Vorgehensweisen angelegt. Es besteht also gar nicht die Intention, dass für alle Funktionen eines Werkzeugs ein Tutorial vorliegt. Zumal ab einem gewissen Erfahrungsgrad die reine Beschreibung der Funktion meist völlig ausreichend ist, und eine Schritt-für-Schritt-Anleitung eher hinderlich bzw. zu zeitaufwändig ist. Die Vollständigkeit in Bezug auf die grundlegenden Funktionen ist aber genauso wenig sinnvoll, da keine Vorgaben existieren, was eine grundlegende Funktion ist. Eine Bewertung anhand der Vollständigkeit (in Bezug auf die Abdeckung der Analysefunktionen) kann für Tutorials also nicht gegeben werden.

Als einziges Bewertungskriterium ist also die Verfügbarkeit von Tutorials zu ermitteln. Da Tutorials für eine Software in der Regel in elektronischer Form vorliegen, bietet sich die Herstellerwebseite oder eine Internetrecherche als Quelle an. Intuitiv würde man für den Bewertungsmaßstab der Verfügbarkeit die Anzahl der verfügbaren Tutorials verwenden. Die Überlegungen zur Vollständigkeit greifen aber auch hier, so dass keine Obergrenze angegeben werden könnte, an welcher man den Maßstab ausrichten könnte. Für die Bewertung kann also nur das Vorhandensein an sich gezählt werden. Hier ist also wieder die Abschätzung des Kataloganwenders gefordert, ob genügend Tutorials vorhanden sind oder nicht. Als Entscheidungshilfe kann dazu wiederum der Analysebereich des Kriterienkatalogs benutzt werden. Sind für einen Teil der dort beschriebenen Themengebiete Tutorials vorhanden, so sollte das vorliegende Kriterium positiv bewertet werden.

Erscheinungsformen:

A Es stehen ausreichend viele Tutorials der grundlegenden Funktionen zu Verfügung.

B Es stehen nicht genügend oder gar keine Tutorials zu Verfügung.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	nicht erfüllt	0

Kriterium 2.2.3

ONLINE HILFE

Kriterium	Gewicht
Bedienung des Werkzeugs	
Dokumentation	
Online Hilfe	2

Die Online Hilfe ist der Teil eines Werkzeugs, welcher dem Benutzer während der Benutzung auf Wunsch oder selbsttätig Informationen über den Gebrauch des Werkzeugs liefert oder Wege aus Fehlersituationen aufzeigt. Der Hauptvorteil dieser Art von Hilfe besteht darin, dass der Benutzer die Online Hilfe sofort und ohne Wechsel des Arbeitsmediums nutzen kann. Der Arbeitsfluss wird also nicht unterbrochen. Des Weiteren beansprucht sie keinen physischen Raum (Arbeitsplatz) und kann, im Gegensatz zu den gedruckten Medien, einfach und kostengünstig mittels Software updates aktuell gehalten werden.

In [Kau03] wird das Thema Online-Hilfe ausführlich behandelt. An dieser Stelle sollen nur die wichtigsten Arten der Online Hilfe zitiert werden, um einen Überblick dieser Techniken zu geben und eine Bewertung des Kriteriums zu erleichtern.

- **Hilfe zu Oberflächen-Elementen**
  Diese wird entweder durch Verweilen auf dem Oberflächen-Element mit der Maus (Tooltips) oder durch Betätigen eines Schalters und Anklicken des entsprechenden Oberflächen-Elements ausgelöst (Windows: Point&Click-Hilfe, Macintosh: Balloon-Help). In einem kleinen Fenster wird dann ein meist kurzer Hilfetext zu dem Oberflächenelement angezeigt. Die Balloon-Help des Macintosh-Betriebssystems ermöglicht es sogar, sich alle Hilfetexte auf einmal anzeigen zu lassen.

- **Aufgabenorientierte Hilfe**
  Diese Art der Hilfe unterstützt den Benutzer bei der Erledigung einer spezifischen Aufgabe. Bei der bekanntesten Form, den sogenannten Assistenten oder Wizards, wird der Benutzer schrittweise durch die Aufgabe geführt. Dabei wird er mit allen wichtigen Informationen für das Bewältigen der einzelnen Schritte versorgt. Er hat die Möglichkeit einzelne Schritte zu widerrufen und rückgängig zu machen.

- **Kontextsensitive Hilfe**
  Kontextsensitive Hilfe ist durch ein spezielles Oberflächen-Element oder eine spezielle Hilfe-Taste verfügbar und bietet Hilfe zum aktuellen Kontext der Anwendung. Im allgemeinen bezieht sie sich auf das aktuelle Fenster oder den aktuellen Dialog.

Des Weiteren kann die Funktionsbeschreibung in elektronischer Form als Online-Hilfe angesehen werden, wenn diese in das Werkzeug integriert ist (z.B. als Menüpunkt, oder man-page). Ein „einfaches“ vorliegen der Funktionsbeschreibung in elektronischer Form (z.B. Word Dokument, PDF Datei) sollte nicht als Online-Hilfe gewertet werden.

Dies stellt nur eine Auswahl der verbreitetsten Ausprägungen von Online-Hilfen da und ist keineswegs vollständig. Bietet das Werkzeug eine weitere sinnvolle Art der Online-Hilfe, so sind gegebenenfalls der Bewertung anzupassen, indem ein entsprechender Punkt der Anforderungen ausgetauscht wird. Dies sollte dann aber für alle untersuchten Werkzeuge erfolgen, um die Vergleichbarkeit der Ergebnisse zu gewährleisten. Zu beachten ist, dass diese Hilfekonzepte nicht eindeutig voneinander getrennt sind, eine Vermischung der Funktionalität ist durchaus denkbar und sinnvoll.

Anforderungen:

- Die Funktionsbeschreibung ist innerhalb der Online-Hilfe integriert.
- Es existiert eine Hilfe zu Oberflächen-Elementen.
- Es stehen Verfahren zur aufgabenorientieren Hilfe zu Verfügung.
- Eine Form der kontextsensitiven Hilfe ist implementiert.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 2.3
AUTOMATISIERUNG

Kriterium	Gewicht
Bedienung des Werkzeugs	
Automatisierung	3

Dieser Kriterienpunkt beinhaltet alle Möglichkeiten, die einem das Werkzeug bietet, Standardaufgaben zu automatisieren und autonom ablaufen zu lassen. Hierunter fallen zum Beispiel die wiederholte und mehrfach miteinander verkettete Anwendung unterschiedlicher Filter und Suchfunktionen, um nur Dateien einer ganz bestimmten Kategorie zu erhalten.

Im Idealfall können alle Vorgänge, welche ein Anwender durch Benutzereingaben erreichen kann, auch durch einen Automatismus ersetzt werden. Hierzu ist es notwendig, dass das Werkzeug eine Schnittstelle bereitstellt, welche einen einfachen Zugriff auf die einzelnen Funktionen des Werkzeugs bietet. Dies kann zum Beispiel durch die Aufzeichnung der Benutzereingaben (Makroaufzeichnung) und der Möglichkeit, diese zu einem späteren Zeitpunkt abzuspielen, gegeben sein. Eine weitere Variante wäre die zu Verfügungstellung einer Programmiersprache, welche den einfachen Zugriff auf die einzelnen Programmfunktionen mittels eines Schnittstelle (Application Programming Interface (API)) bietet.

Anforderungen:

- Die Ergebnisse einer Funktion/Analysemethode können ohne Probleme als Eingabe für die nächste Funktion verwendet werden. Es ist keine explizite Zwischenspeicherung notwendig.

- Das Werkzeug bietet eine Aufzeichnungsmöglichkeit der durchgeführten Aktionen an (Makrofunktion)
- Es existiert eine Programmiersprache und eine API, welche den vollen Zugriff auf die Funktionen des Werkzeugs erlauben.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Zwei der genannten Punkte werden erfüllt.

C Nur einer der genannten Punkte wird erfüllt.

D Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 2.4
PROJEKTVERWALTUNG

Kriterium	Gewicht
Bedienung des Werkzeugs	
Projektverwaltung	1

Die Projektverwaltung bezeichnet die umfassende Unterstützung eines Ermittlers bei der Verwaltung einer Untersuchung. Eine Untersuchung umfasst dabei unter Umständen mehrere Festplatten-Images und alle zugehörigen Informationen, welche bei der Analyse der Images erfasst werden. Es ist also Aufgabe der Projektverwaltung die untersuchten Images und (Teil-) Ergebnisse der Analyse (z.B. einer Suche) strukturiert darzustellen und ihren Bezug zueinander zu gewährleisten. Weiterhin sollte die Möglichkeit gegeben werden, untersuchungsbezogene Notizen (z.B. mit Verweis auf eine bestimmte Datei) an entsprechenden Stellen abzulegen.

Das Werkzeug sollte also die komplette Verwaltung aller anfallenden Daten übernehmen und den Zugriff darauf für den Anwender transparent gestalten. Das Anlegen einer eigenen Verzeichnis- bzw. Datenstruktur, für die Ablage der anfallenden Informationen und Ergebnisse, sollte also komplett vom Werkzeug übernommen werden. Im Idealfall reicht es also für den Anwender aus, den Ort der untersuchten Images und ein Arbeitsverzeichnis zu Verfügung zu stellen.

Anforderungen:

- Die Darstellung eines untersuchten Bitstream-Images ist in einer übersichtlichen Weise möglich.
- Die Ergebnisse der einzelnen Analyseschritte werden übersichtlich dargestellt.
- Die Verwaltung mehrere Bitstream-Images in einer Instanz des Werkzeugs ist möglich.
- Es wird die Möglichkeit gegeben, eigene Notizen zu den einzelnen Dateien oder Untersuchungsergebnissen anzulegen.
- Die Verwaltung der Daten erfolgt transparent durch das Werkzeug.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Vier der genannten Punkte werden erfüllt.

C Drei der genannten Punkte werden erfüllt.

D Zwei einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 3
Protokollierung der Untersuchung

Die Sicherstellung von Beweisen ist der zentrale Bestandteil der Computerforensik. Damit Beweise später vor Gericht oder einem ähnlichem Gremium anerkannt werden bzw. deren Sicherstellung von einer dritten Person nachvollzogen werden kann, ist es notwendig, dass keine Zweifel an der Herkunft, Sicherstellung und Integrität der Beweise bestehen.

Dies kann dadurch erreicht werden, dass jede Information, welche über den Beweis zu Verfügung steht, und jede Aktion, welche in Bezug auf den Beweis stattfindet, genauestens dokumentiert wird. Folgende Informationen sind dabei festzuhalten:

- Eine genau Beschreibung des Beweises sowie sein Fundort innerhalb des Bitstream-Images, damit dessen Identität und Herkunft gesichert ist.
- Für jede Person, die bei der Sicherstellung des Beweises involviert war, die Personalien, der Zeitpunkt und die Art des Zugriffs, sowie der Grund, warum dieser Zugriff durchgeführt wurde.
- Das verwendete Untersuchungswerkzeug bzw. das verwendete Teilprogramm inklusive Versionsnummer.

Ziel ist eine lückenlose und nachvollziehbare Dokumentation der Untersuchung, so dass keine Fragen in Bezug auf die (gerichtliche) Verwertbarkeit der Beweise offen bleiben. Für die unmittelbare Analyse von Bitstream-Images ist hierbei nur der erste Punkt interessant. Bei den anderen beiden Punkten reicht es, innerhalb des angefertigten Untersuchungsprotokol diese einmal anzugeben, da sie normalerweise keiner oder nur geringer Änderungen unterworfen sind.

Für die Bewertung des Kriteriums kann davon ausgegangen werden, dass die Anwendung einer Analysefunktion ein Ergebnis liefert und dieses dem Benutzer präsentiert. Neben dem Ergebnis sollte zusätzlich die Information bereitgestellt werden, welche verwendete Funktion zu diesem Ergebnis geführt hat, ob eventuell zusätzliche Optionen eingestellt waren (z.B. per Kommandozeilenparameter oder in sonstigen Einstellungen) und zu welchem Zeitpunkt sie ausgeführt wurde. Des Weiteren sollte die Datenquelle, auf welche die Analysefunktion angewandt wurde, genauer spezifiziert werden (z.B. eine bestimmte Datei, ein Verzeichnis, Dateien mit bestimmten Eigenschaften, das verwendete Image usw.). Diese Informationen beinhalten alles nötige, um einen Beweis (innerhalb des vorgegebenen Rahmens) ausreichend zu beschreiben. Sie könnten in dieser Form also ohne weiteres in ein geführtes Untersuchungsprotokol aufgenommen werden (z.B. per copy&paste).

Da diese Protokollierung aber für jeden gefundenen bzw. verwendeten Beweis nötig ist, sollte hierfür ein Automatismus zu Verfügung stehen. Dabei können zwei Vorgehensweisen unterschieden werden. Erstens die automatische Protokollierung jeder Aktion und jedes Ergebnisses. Dies hat den Vorteil, dass man sich nicht weiter um die Protokollierung kümmern muss und am Ende einer Untersuchung über ein vollständiges Protokoll verfügt. Nachteil dieser Methode ist natürlich der dabei entstehende enorme Umfang an unbrauchbaren Daten, da hier natürlich auch Analyseschritte protokolliert werden, die keine Beweise liefern und eventuell später (z.B. aus Gründen der Übersichtlichkeit) wieder manuell entfernt werden müssen. Die zweite Möglichkeit besteht darin, nur die notwendigen Protokolle eines Analyseschritts innerhalb des Werkzeugs zu sichern (z.B. mittels eines Knopfdrucks, welcher bei der Anzeige des Ergebnisses bereitgestellt wird) und am Ende einer Untersuchung gesammelt auszugeben. Hierbei müsste man sich dann natürlich auf das zuverlässige Arbeiten des Ermittlers verlassen können.

Anforderungen:

- Neben dem Ergebnis werden zusätzliche Informationen mit aufgeführt (z.B. Funktionsaufruf + Parameter, Zeitpunkt).
- Die genaue Lokalisierung der Daten, die im Analyseschritt involviert waren, wird angegeben.
- Eine vollautomatische Mitprotokollierung wird unterstützt.
- Eine selektive Speicherung und gesammelte Ausgabe der Protokolle der einzelnen Analyseschritte wird innerhalb des Werkzeugs auf einfache Weise unterstützt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4
ANALYSE

Kriterium	Gewicht
Datenanalyse	
Rohdaten Analyse	4
Daten Extraktion und Wiederherstellung	4
Suchverfahren	3
Prüfsummen	3
Internetnutzung	1
Metadaten	2

Die Analyse eines Bitstream-Images kann auf unterschiedliche Weise und an unterschiedlichen Stellen des ursprünglichen Datenträgers erfolgen. Die Teilkriterien des aktuellen Analyse-Kriteriums haben daher einen gruppierenden Charakter, um die einzelnen Gebiete der Analyse besser voneinander Trennen zu können. Bei der Anordnung der Kriterien und dessen Bewertung wurde dabei versucht ein gewisse Abstufung zu finden. Die vorderen Kriteriengruppen behandeln grundlegende und häufig gebrauchte Funktionen, welche sehr nah auf dem Bitstream-Image arbeiten und nur bedingt eine Interpretation des Daten- bzw. Datei-Inhalts verwenden. Diese werden im allgemeinen stärker gewichtet als die später auftretenden Kriterien, bei welchen immer mehr eine Interpretation der Daten bzw. Dateien durch das Analysewerkzeug erfolgt und daher eher spezifisch für einen bestimmten Fall von Nutzen sind. Die Analysefunktionen leisten also eine mehr oder weniger umfangreiche Vorinterpretation der auszuwertenden Daten, welche durch den Benutzer nur schwer oder gar nicht von Hand zu erledigen wäre.

Die *Rohdaten Analyse* beschreiben die Funktionen, die unmittelbar mit den Bitstream-Image zusammenhängen. Zum Einen also, ob das Image überhaupt erkannt wird, zum Anderen, ob die sich darin befindlichen Dateisysteme auch vom Werkzeug unterstützt werden. Ohne diese Funktionalität wäre eine weitere Untersuchung des Images gar nicht möglich, daher ist dieses Kriterium als äußerst wichtig einzustufen.

Eine Abstraktionsstufe höher befindet sich das Kriterium *Daten Extraktion und Wiederherstellung* . Die Funktionen dieses Kriteriums stellen sicher, dass der Zugriff auf alle Daten einer einzelnen Partition des Images gewährleistet wird. Hierzu gehören auch Daten, die nicht mehr vom Dateisystem der Partition verwaltet werden (z.B. gelöschte Daten). Dieses Kriterium wird daher ebenfalls als äußerst wichtig eingestuft, da hiermit gewährleistet wird, dass keine Daten bei der Untersuchung außen vor gelassen werden.

Die Suche nach Schlüsselwörter ist ein inhärenter Bestandteil der Untersuchung eines Bitstream-Images, um Beweismittel zu finden. Bei der Bewertung des Katalogs wird davon ausgegangen, dass das Werkzeug eine einfache Suche auf den zu Verfügung gestellten Daten beherrscht. Sollte dies nicht der Fall sein[3], so ist das ganze Teilkriterium

[3] Dieser Fall könnte z.B. bei einem sehr spezialisierten Werkzeug auftreten, welches nur ganz bestimmte Funktionen anbietet. In der Regel wird dies bei Werkzeugen, die Bitstream-Images analysieren, aber nicht auftreten.

Suchverfahren mit 0 Punkten zu bewerten. Das Kriterium *Suchverfahren* beschreibt zusätzliche Suchalgorithmen, welche die einfache Suche aufwerten und Verfeinerungen bei einer Suchanfrage ermöglichen. Das Kriterium ist daher immer noch von sehr wichtiger Bedeutung für die Bewertung.

Die Verwendung von *Prüfsummen* wird ebenfalls als sehr wichtig angesehen, da ihre Verwendung den effektiven Umgang mit großen Datenmengen erlaubt und damit nicht unerheblich an der schnellen Durchführung einer Untersuchung beteiligt ist.

Die Analyse der *Nutzung des Internets* wird im Vergleich zu den anderen Kriterien als weniger wichtig angesehen, da es sich hier bereits um ein sehr spezielles Teilgebiet der Analyse handelt, welches nicht bei jeder Untersuchung zum Zuge kommt. Es wird an dieser Stelle nur deshalb aufgenommen, weil die Benutzung des Internets eine der wichtigsten Kommunikationsmedium zwischen IT-Systemen darstellt. Es ist also die entscheidende Quelle, wenn Informationen zu Systemen oder Personen gebraucht werden, welche mit dem Besitzer des Datenträgers in Kontakt standen, von welchem das zu untersuchende Image stammt.

Metadaten sind Daten, welche Informationen über andere Daten enthalten. Im konkreten Fall also Daten, die zusätzlich zu den offensichtlich vorhanden Daten zur Verfügung stehen bzw. ermittelt werden können. Diese sind von wichtiger Bedeutung, da hier oftmals Informationen erfasst werden können, die mit dem eigentlichen Datei-Inhalt nichts zu tun haben und vom ursprünglichen Besitzer nicht explizit angelegt wurden, sondern automatisch vom System.

Kriterium 4.1
ROHDATEN ANALYSE

Kriterium	Gewicht
Analyse	
Rohdaten Analyse	
Image Erkennung	1
Dateisystem Unterstützung	4

Die Analyse der Rohdaten beschreibt die Fähigkeit des Werkzeugs mit den einzelnen Bitstream-Images umzugehen und die darin enthaltenen Strukturen (Partitionen) zu erkennen. Bei der *Image Erkennung* wird bei der Bewertung davon ausgegangen, dass das Werkzeug zumindest sein eigenes Imageformat beherrscht, da dies genau das Aufgabengebiet der untersuchten Werkzeuge ist. Das Kriterium behandelt demnach nur zusätzliche Leistungen in Bezug auf Bitstream-Images und wird daher als weniger wichtig eingestuft. Im Vergleich dazu gestaltet sich die Unterstützung der *Dateisysteme* hingegen als äußerst wichtig, da ohne den (lesenden) Zugriff auf diese, eine weitere Untersuchung nicht möglich ist.

Kriterium 4.1.1
IMAGE ERKENNUNG

Kriterium	Gewicht
Analyse	
Rohdaten Analyse	
Image Erkennung	2

Die Erkennung eines Festplatten-Images ist eine der Grundlage für alle folgenden Untersuchungen, da ansonsten ein Zugriff auf die einzelnen Partitionen der Festplatte und somit die Daten des Beweisstückes, nicht möglich ist. Sehr viele Analysewerkzeuge bieten die Möglichkeit Images in einem eigenen Format anzulegen, welches unter Umständen zusätzliche Informationen, zum Beispiel eine Prüfsumme zu Wahrung der Integrität, beinhalten kann. Für die weitere Betrachtung wird davon ausgegangen, dass eine Anwendung das eigene Imageformat zu voll unterstützt.

Die Verwendung eines eigenen (evtl. proprietären) Image-Formats der Anwendung, und somit die Verwendung eines eigenen Algorithmus zur Image Erstellung, ist zumindest in zwei Punkten problematisch. Einerseits bei der Qualität, andererseits bei Portabilität des Images. Die Qualität dieser Verfahren (z.B. die zuverlässige und robuste Behandlung von Lesefehlern, oder ob auch wirklich alle Bereiche der duplizierten Festplatte bitweise kopiert wurden) und der daraus resultieren Formate wird eingehend in [CFT04] untersucht. Dies ist vor allem für die gerichtliche Verwertbarkeit von Interesse. Die Erstellung von Festplatten-Images ist aber nicht Gegenstand der vorliegenden Arbeit ist, daher wird auf diesen Punkt nicht weiter eingegangen.

Die Portabilität der Image-Formate bzw. die Unterstützung unterschiedlichster Formate durch das Analysewerkzeug, kann hingegen Auswirkungen auf eine Untersuchung haben. Dies liegt einerseits daran, dass ein zu untersuchendes Image von den unterschiedlichsten Quellen (z.B. andere Ermittlungsbehörde) stammen kann, welche eventuell nicht (mehr) die Möglichkeit haben ein Image im entsprechenden Format zu liefern (z.B. weil keine Lizenz für das Programm vorliegt oder weil der ursprüngliche Datenträger nicht mehr vorhanden ist und nur ein Image erstellt worden ist). Ein Zugriff und somit eine Untersuchung, wäre dann aber gar nicht, oder nur mit großem Aufwand möglich (z.B. indem eine Format Umwandlung durchgeführt wird). Andererseits besteht auch die Möglichkeit, dass eine Untersuchung mit unterschiedlichen Werkzeugen erfolgt, welche für eine bestimmte Aufgabe besser geeignet sind. Unterstützt ein Werkzeug aber nur das eigene Format, müsste für jedes Werkzeug ein eigenständiges Image angelegt werden, was zu erheblichen Platzbedarf führen kann. Als Lösung bietet sich hier die Unterstützung von reinen 1:1 Kopien des Datenträgers an (raw-Image), welche nur die bitweise kopierten Daten des Datenträgers und keine weiteren Informationen beinhalten. Diese können zum Beispiel mittels dem kostenlos erhältlichen `dd` erstellt werden, welche für fast jede Plattform zu Verfügung steht und bei vielen Systemen im Linux/Unix Bereich bereits standardmäßig mit installiert wird.

Für die Bewertung des Kriteriums ist es also entscheidend, wie viele unterschiedliche Image-Formate das Analysewerkzeug unterstützt. Hierbei ist es aber problematisch, dass fast jeder Hersteller ein eigenes Format für sein Werkzeug bereitstellt. Eine fundierte Untersuchung von unabhängiger Stelle über die Verbreitung der unterschiedlichen Formate, wie sie zum Beispiel für Betriebssysteme (Kriterium 4.1.2) vorliegt, ist nicht bekannt. Folglich kann auch keine Entscheidung getroffen werden, welches Format explizit unterstützt werden muss oder weggelassen werden kann. Als sinnvolle Bewertungsgrundlage ist also neben der Unterstützung für reine 1:1 Kopien, nur die Unterstützung mindestens eines Weiteren Formate anzurechnen, wobei eine Priorität auf den 1:1 Kopien liegt.

Erscheinungsformen:

D Keine weiteren Image-Formate werden unterstützt.

C Es wird mindestens ein weiteres proprietäres Image-Format unterstützt.
(z.B. von EnCase [Sof04a], ILook [Ilo04])

B Reine 1:1 Kopien (raw-Images, dd-Images) eines Datenträgers werden unterstützt.

A Es gilt sowohl B, als auch C.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	kaum erfüllt	1
D	nicht erfüllt	0

Kriterium 4.1.2
DATEISYSTEM UNTERSTÜTZUNG

Kriterium	Gewicht
Analyse	
Rohdaten Analyse	
Dateisystem Unterstützung	4

Die Durchführung einer Untersuchung an einem Festplattenabbild ist nur möglich, falls das Untersuchungswerkzeug lesenden Zugriff auf das verwendete Dateisystem unterstützt, da ansonsten eine weitere Analyse der Daten nicht stattfinden kann.

Hierbei ist vor allem die Verbreitung der Betriebsysteme und damit die Verbreitung der ihnen zugrundeliegenden Dateisysteme zu beachten. Die Betriebssysteme von Microsoft, zusammen mit dem Betriebssystem Linux, besitzen auf dem Markt eine Abdeckung von weit über 95% [Win04]. Die Wahrscheinlichkeit, dass eine forensische Untersuchung an einem Festplattenabbild dieser Betriebssysteme, und somit eines von diesen Betriebssystemen verwendeten Dateisystems, vorgenommen wird, ist daher signifikant hoch. Die Unterstützung anderer, nicht so verbreiteter Dateisysteme (z.B. Solaris FS), oder ihr Fehlen, sollte daher nicht zu einer Über- bzw. Unterbewertung des Kriteriums führen.

Des Weiteren sollte der lesende Zugriff des Analysewerkzeugs die gleichen Resultate bzw. Informationen über die Dateien liefern wie der Einsatz des ursprünglichen Betriebssystems. In der Praxis hängt dies aber von der Implementierung im Analysewerkzeug ab, welche unter Umständen auch unvollständig oder fehlerhaft sein könnte. Um dies zu testen und in die Bewertung einfließen zu lassen, müsste aber für jedes Dateisystem ein eigenes Teilkriterium angelegt werden, was auf Grund der Vielfalt der existierenden Dateisysteme [BS004] nur schwer möglich ist. Außerdem müsste für jedes Dateisystem eine Abstufung gefunden werden, welche den lesenden Zugriff kategorisiert. Beide Punkte würden bei der Bewertung des Kriteriums aber ein erhebliches Zeitkontingent und vertieftes Wissen über die unterschiedlichen Dateisysteme erfordern.

Für die Bewertung des vorliegenden Kriteriums sind also einige Einschränkungen gemacht worden, um die oben angesprochenen Punkte zu berücksichtigen und dennoch ein aussagekräftiges Ergebnis zu erhalten. Die Handhabung der großen Anzahl von Dateisystemen wird dadurch erreicht, dass alle „exotischen“ Dateisysteme zu einem Bewertungspunkt zusammengefasst werden. Bei der Fähigkeit des lesenden Zugriffs werden keine weiteren Abstufungen überprüft, da davon ausgegangen wird, dass eventuell bestehende Implementierungsfehler durch den Hersteller behoben werden. Wird dennoch nicht die volle Unterstützung eines Dateisystems angeboten bzw. ist dahingehend ein Fehlverhalten bekannt, sollten dem Werkzeug für dieses Dateisystem keine Punkte angerechnet werden. Insgesamt ist für die Bewertung dieses Kriteriums also nur die Quantität der vom Werkzeug unterstützten Dateisysteme entscheidend, wobei ein besonderes Augenmerk auf die am verbreitetsten Dateisysteme gelegt wurde.

Anforderungen:

- FAT Dateisystem-Familie wird unterstützt.
- NTFS Dateisystem-Familie wird unterstützt.
- EXT2/3 Dateisystem-Familie wird unterstützt.
- Weitere Dateisystem-Familien werden unterstützt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

D Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.2
DATEN EXTRAKTION UND WIEDERHERSTELLUNG

Kriterium	Gewicht
Analyse	
Daten Extraktion und Wiederherstellung	
Gelöschte Daten	4
Unzugeordnete Bereiche	4
Slack Bereiche	4
Auslagerungsdateien und Swap-Partitionen	2
Verschlüsselte und komprimierte Daten	2
Alternate Data Streams	1

Die Funktionen dieses Kriteriums stellen sicher, dass der Zugriff auf alle Daten einer einzelnen Partition des Images gewährleistet wird. Dateien, welche durch das Dateisystem verwaltet werden, *gelöschte Dateien, unzugeordnete Bereiche* (unallocated space) und *Slack Bereiche*, beschreiben vollständig die Daten einer Partition[4]. Diese Kriterien werden daher als äußerst wichtig angesehen, da hiermit gewährleistet wird, dass ein Zugriff auf jedes Bit innerhalb der Partition möglich ist.

Bei der Untersuchung von *Auslagerungsdateien* und *verschlüsselten und komprimierten Dateien* befindet man sich bereits auf der Dateiebene und nicht mehr auf der reinen Datenebene der Partition. Diese zwei Bereiche werden gesondert behandelt, da es sich hier um Containerdateien handelt. Sie sind also nicht als eine Datei mit einer einzigen Inhaltsform anzusehen (z.B. Textdatei), sondern können mehrere Dateien bzw. Datenfragmente von unterschiedlichen Dateitypen enthalten. Die Bereitstellung dieses Inhalts wird daher als wichtig eingestuft.

Alternate Data Streams (ADS) sind eine Besonderheit des NTFS Dateisystems und hätten damit auch innerhalb von 4.1.2 behandelt werden können. Sie werden hier zum Einen aufgeführt, da zwar mit den zugehörigen Mitteln des Betriebssystems auf sie zugegriffen werden kann, dies aber nur für Applikation und nicht für einen Benutzer vorgesehen war. Bei einer „normalen“ Nutzung des Dateisystems werden sie nicht bemerkt oder angezeigt, weswegen sie unter diesem Kriterium aufgeführt werden, da ein einfacher Zugriff erst zu Verfügung gestellt werden muss. Zum Anderen war die Existenz von ADS und ihre Verwendung lange Zeit nur Profis bekannt, in den letzten Monaten hat ihre Nutzung (insbesondere von schädlichem Programmen wie Viren) aber bedeutend zugenommen. Ihre Aufnahme in den Katalog dient daher auch dazu, diese Bereiche nicht zu vergessen. Im Vergleich zu den anderen Kriterienpunkten ist dieses Kriterium eher weniger wichtig, da es nur in speziellen Situation Verwendung findet und für seine Darstellung nur wenig Aufwand betrieben werden muss.

[4]Dies gilt auch für defekte Sektoren auf dem ursprünglichen Datenträger. Je nach Art der Erstellung des Bitstream-Images wird versucht, diese dennoch zu lesen oder durch entsprechende Füllbits zu ersetzen. Innerhalb des Images finden sich diese Sektoren in den unzugeordneten Bereichen.

Kriterium 4.2.1
GELÖSCHTE DATEN

Kriterium	Gewicht
Analyse	
Daten Extraktion und Wiederherstellung	
Gelöschte Daten	4

Die Wiederherstellung von gelöschten Daten beruht auf den Eigenheiten der Dateisysteme in Bezug auf die Verwaltung der Daten. Hier wird nur kurz auf das allgemeine Konzept dieses Verfahrens eingegangen, welches natürlich inhärent von dem verwendeten Dateisystem abhängig ist. Genauere Informationen lassen sich in den zugehörigen Spezifikation der Dateisysteme oder entsprechenden Abhandlungen finden (z.B. [NTF04] für das NTSF und FAT Dateisystem, [Sch00] für EXT2). In vielen Fällen wird der gesamte Speicherplatz und somit die vorhandenen Dateien mittels einer Datenstruktur (z.B. FAT- oder Inode-Tabelle) verwaltet. In dieser werden eine Menge von Verweisen bereitgestellt, welche für die Speicherung von Dateien verwendet wird und für jede Datei unter anderem die entsprechenden physikalische Position der Datei speichern. Beim Löschen einer Datei wird aus Gründen der Performance nicht der Datei-Inhalt gelöscht, sondern der entsprechende Verweis manipuliert, so dass er für die Speicherung von neuen Daten verwendet werden kann. Dies kann zum Beispiel durch das Setzten eines speziellen Bits erfolgen, oder durch eine Aufnahme in eine zweite Datenstruktur, welche die freien Verweise verwaltet. Nach dem Löschen sind also sowohl die Daten an ihrer physikalischen Position, als auch die Informationen im Verweis, noch im System vorhanden. Werden die Verweise nicht anderweitig verwendet, kann die erfolgte Manipulation des Verweises rückgängig und ein Teil der gelöschten Dateien wieder hergestellt werden.

Die Ergebnisse dieser Wiederherstellung sind jedoch stark von der Nutzung des Datenspeichers und dem verwendetem Dateisystem abhängig. Wird ein System häufig genutzt, werden in der Regel auch häufig neue Dateien angelegt. Dadurch steigt natürlich auch die Wahrscheinlichkeit, dass sowohl ein Verweis, als auch die physikalische Position auf dem Datenträger, für die Speicherung von neuen Daten wieder verwendet wird (Diese Wiederverwendung kann auch unabhängig voneinander erfolgen). Das Dateisystem hat insofern Einfluss auf diesen Prozess, in welcher Art es die Verweise in der Verwaltungsstruktur organisiert. Werden die zu Verfügung stehenden Verweise unabhängig von ihrem bisherigen Einsatz zugeteilt, zum Beispiel indem immer der nächste freie Verweis innerhalb der Verwaltungsstruktur verwendet wird, ist die Zahl der wieder herstellbaren Verweise relativ groß, da ein Verweis nicht sofort, sondern abhängig von der aktuellen Positionen, neu zugeteilt wird (wobei das Problem der Wiederverwendung des physikalischen Speicherplatzes natürlich weiterhin bestehen bleibt). Werden die Verweise hingegen relativ schnell wieder verwendet, indem zum Beispiel immer der erste freie Verweis innerhalb der Verwaltungsstruktur verwendet wird, ist die Ausbeute an wieder hergestellten Dateien sehr gering. Ist ein Dateisystem so ausgelegt, dass Verweise gar nicht vorgehalten werden, zum

Beispiel bei Datenbank basierten Dateisystemen, welche die Verweise dynamisch erzeugen und löschen, oder dass beim Löschen auch die physikalische Position überschrieben wird (z.B. aus Sicherheitsgründen), so ist eine Wiederherstellung von gelöschten Dateien in der Regel nicht möglich.

Für den Ermittler bietet diese Art der Analyse einige Vorteile, da er auf vermeintlich gelöschte Dateien noch Zugriff erhält. Ist einem Verdächtigen der Vorgang der Datenwiederherstellung nicht bekannt, oder konnte aus Zeitgründen das sichere löschen von Dateien (engl.: data-wiping) nicht durchgeführt werden, kann der Ermittler eventuell einen Großteil der Dateien rekonstruieren und so Beweise sichern. In einigen Fällen können hierbei Dateien wieder hergestellt werden, die schon vor längerer Zeit auf dem System gelöscht worden sind und dennoch fallrelevante Daten enthalten.

Das Analysewerkzeug sollte also in der Lage sein, gelöschte Dateien zu rekonstruieren und sie den anderen Analysemethoden zur Verfügung zu stellen. Für den Ermittler sollte dieser Vorgang völlig transparent ablaufen, so dass er sich nicht um die Eigenheiten der Dateisysteme kümmern muss. Da aber eine Vielzahl unterschiedlicher Dateisysteme existiert [BS004], wird für die Bewertung dieses Kriteriums insbesondere auf die Eignung für die verbreiteten Dateisysteme (FAT, NTFS, EXT2/3) Rücksicht genommen.

Anforderungen:

- Wiederherstellung bei FAT Dateisystemen wird angeboten.
- Wiederherstellung bei NTFS Dateisystemen wird angeboten.
- Wiederherstellung bei EXT2/3 Dateisystemen wird angeboten.
- Wiederherstellung bei weiteren Dateisystemen wird angeboten.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.2.2
Nicht zugeordnete Bereiche

Kriterium	Gewicht
Analyse	
Daten Extraktion	
Nicht zugeordnete Bereiche	4

Als nicht zugeordnete Bereiche (unallocated space) werden die Bereiche einer Partition bezeichnet, auf die innerhalb der Verwaltungsstruktur des Dateisystems (siehe Kriterium 4.2.1) keine Verweise mehr zeigen. Auf Grund von Fragmentierung bei der Datenverwaltung, müssen diese Bereiche nicht zusammenhängend sein (z.B. nur am Ende des physikalischen Speichers), sondern können sich über die ganze Partition verteilen.

Innerhalb der nicht zugeordneten Bereiche können diverse Daten (z.B. Dateien, Verzeichnisse, oder Fragmente davon) angetroffen werden, die zu einem früheren Zeitpunkt an dieser physikalischen Position des Datenträgers abgespeichert wurden. Ähnlich wie bei den gelöschten Dateien können sich in diesem Bereich also Daten finden, welche schon längst nicht mehr auf dem Datenträger vermutet wurden. Es ist also durchaus möglich, dass sich innerhalb dieser Bereiche fallrelevante Daten befinden, so dass es die Aufgabe des Ermittlers ist, auch diese Bereiche zu analysieren.

Innerhalb der unzugeordneten Bereiche können sich auch vollständig erhaltene Datei befinden. Deren Anfang kann in vielen Fällen mittels ihrer Signatur (Kriterium 4.3.5 Seite 80) genau ermittelt werden, welche charakteristisch für bestimmte Dateien ist. Ist für den Anfang einer Datei (header) ein spezielles Format vorgeschrieben, das auch die Größe der Datei beinhaltet oder ist auch das Ende einer Datei (footer) charakteristisch, können vom Anfang der Datei ab entsprechend viele Daten eingelesen werden. Wurde die Datei ursprünglich nicht fragmentiert abgelegt und zwischenzeitlich dieser physikalische Bereich auch nicht wieder verwendet, so besteht eine große Chance, auf diese Weise die Datei zu rekonstruieren. Alternativ kann auch vom Anfang der Datei an eine gewisse Anzahl von Daten eingelesen und der zugehörigen Applikation übergeben werden. Je nach Datenformat und Applikation (z.B. wenn ein linearer Datenstrom zur Speicherung verwendet wird, der auch unvollständig ohne Kenntnis des „Endes“ angezeigt werden kann) könnten diese Daten ebenfalls interpretiert werden.

Das Analysewerkzeug sollte also in der Lage sein, den Zugriff auf die nicht zugeordneten Bereiche zu ermöglichen. Da diese Bereiche, je nach Anzahl vorhandener Dateien auf dem Datenträger, einen erheblichen Umfang einnehmen können, ist es sinnvoll, wenn das Werkzeug auch die restlichen Analysemethoden, insbesondere die Suchalgorithmen, auf diesen Bereich zulässt. Eine zusätzliche automatische Funktionalität, welche die oben beschriebene Wiederherstellung anhand des Dateianfangs ermöglicht, wäre sinnvoll.

Erscheinungsformen:

D Die Bereitstellung von unzugeordneten Bereichen wird nicht unterstützt.

C Unzugeordnete Bereiche werden auf einfache Weise, zum Beispiel in einem Editor, zu Verfügung gestellt.

B Es gilt C. Zusätzlich können die restlichen Analysemethoden des Werkzeugs auf diese Bereiche angewandt werden.

A Es stehen Funktionen zur Verfügung, welche speziell für die Analyse der unzugeordneten Bereiche vorgesehen sind.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	nicht erfüllt	0

Kriterium 4.2.3
SLACK BEREICHE

Kriterium	Gewicht
Analyse	
Daten Extraktion und Wiederherstellung	
Slack Bereiche	4

Dateien haben abhängig von ihren beinhaltenden Daten eine bestimmte Dateigröße. Die Daten eines Massenspeichers werden aus Effizienzgründen (z.B. zur Verminderung des Verwaltungsaufwandes) nicht in einzelnen Bytes angefordert, sondern in Einheiten einer bestimmten Anzahl von Bytes. Diese, für das Dateisystem kleinsten Speichereinheiten, werden als Sektoren bezeichnet und sind abhängig von der verwendeten Hard- und Software. (bei Festplatten meist 512 Bytes, bei CD-Roms 2048 Bytes). Zur Verwaltung des Speicherplatz eines Massenspeichers, werden diese Sektoren von den Dateisystemen weiterhin zu logischen Datenblöcken zusammengefasst, welche als Cluster bezeichnet werden.

Entsprechen nun die gespeicherten Daten in einer Datei nicht einem Vielfachen der Clustergröße, so entsteht innerhalb dieses Clusters, zwischen dem Ende der gespeicherten Datei und dem Ende der zugewiesenen Speichereinheit, ein Bereich, welcher nicht mit den Daten der gespeicherten Datei überschrieben wird. Dieser Vorgang und die resultierenden Probleme sind in der Literatur über Betriebssysteme als interne Fragmentierung bekannt. Für die Computerforensik hingegen ist dieser Vorgang aber eher ein Vorteil, da in sich diesen Bereichen fallrelevante Daten befinden können. In der Fachliteratur zur Computerforensik und im weiteren Verlauf der vorliegenden Arbeit wird dieser Bereich als Slackbereich bezeichnet (engl: *slack area* oder im Bezug auf Dateien auch *file slack*).

Die am häufigsten anzutreffenden Slack-Bereiche sind dabei der RAM-Slack und der File-Slack (siehe Abbildung 4.3).

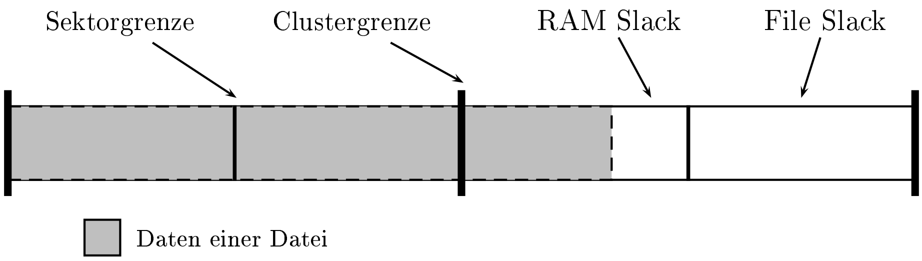

Abbildung 4.3: Wichtige Slack-Bereiche

Falls ein Betriebssystem die Daten blockweise (typischerweise die Größe eines Sektors) auf den Datenträger schreibt (zum Beispiel Microsoft Windows beim Zugriff auf das FAT Dateisystem in 512 Byte großen Blöcken), kann die Situation auftreten, dass nicht mehr genug Daten in einer Datei vorhanden sind, um den letzten zu schreibenden Block zu füllen. Dieser Block wird dann mit zufälligen Daten aus dem Hauptspeicher (RAM) „aufgefüllt“ und auf den Datenspeicher geschrieben. Dieser Bereich zwischen Ende der Datei und dem Ende des Sektors wird als RAM-slack bezeichnet. Der RAM-slack beinhaltet also zufällige Daten und Informationen, welche sich zum Zeitpunkt des Schreibens im Arbeitsspeicher befanden.

Werden zusätzliche Sektoren benötigt, um die Blockgröße des letzten logischen Datenblocks (Cluster) des Dateisystems zu erreichen, entsteht der File-Slack. Für diesen Bereich werden nicht extra Daten von einer anderen Stelle ausgelesen oder erzeugt, sondern es werden die Daten verwendet, die sich bereits an dieser Stelle des Datenspeichers befinden. Im File-slack können sich also Daten- und Informationsfragmente befinden (z.B. von gelöschten Dateien), welche zu einem früheren Zeitpunkt an dieser Stelle des Datenspeichers, einmal abgelegt wurden.

Der MFT-slack erhält seinen Namen von der Master File Table (MFT) des Microsoft NTFS-Dateisystems. Die Master File Table ist ist die Verwaltungsstruktur des NTFS-Dateisystems, welche für jede Datei und jedes Verzeichnis diverse Informationen (z.B. Dateiattribute) verwaltet [NTF04]. Für jede Datei (und jedes Verzeichnis) existiert dabei mindestens ein Datensatz (Verweis), welcher standardmäßig 1024 Bytes groß ist. Neben Informationen zu den Dateien, enthält dieser Verweis auch Fragmente der zugehörigen Datei. Ist eine Datei kleiner als 1024 Bytes, wird sie sogar vollständig in diesem Bereich abgelegt. Ist sie erheblich kleiner, enthält sie also zum Beispiel nur die Notiz einer Telefonnummer, entsteht zwischen dem Dateiende und der Grenze des MFT Eintrags der MFT-Slack. Unter Umständen können sich hierin Fragmente von Dateien finden, welche zu einem früheren Zeitpunkt durch den Verweis referenziert wurden.

Für den Ermittler sind die Slack-Bereiche also eine Quelle von Informationen, wenn auch meist bruchstückhafte, die Hinweise auf die laufende Untersuchung liefern können. Das Werkzeug sollte also in der Lage sein, diese für eine Analyse bereitzustellen. Durch den Vorgang der Fragmentierung können auch an anderen Stellen Slack-Bereiche entstehen (z.B. bei Grenzen von Partitionen, wenn der Datenträger eine bestimmte Rasterung vorgibt und bei der Erstellung der Partition nicht ein Vielfaches davon verwendet wird).

Anforderungen:

- File-Slack wird bereitgestellt.
- RAM-Slack wird bereitgestellt.
- MFT-Slack wird bereitgestellt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Zwei der genannten Punkte werden erfüllt.

C Nur einer der genannten Punkte wird erfüllt.

D Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	nicht erfüllt	0

Kriterium 4.2.4
AUSLAGERUNGSDATEIEN UND SWAP-PARTITIONEN

Kriterium	Gewicht
Analyse	
Datenextraktion	
Auslagerungsdateien und Swap-Partitionen	2

Ein Konzept der Speicherverwaltung von Betriebsystemen ist die Auslagerung bestimmter Teile des physikalisch vorhandenen Arbeitsspeichers in einem speziellen Bereich der Festplatte, um Prozessen einen größeren Adressraum zu Verfügung zu stellen. Die Windows Betriebssysteme verwalten diesen Bereich innerhalb einer Datei (Auslagerungsdatei, swap-file), bei Linux und Unix Derivaten hingegen ist dafür eine eigenen Partition (Auslagerungspartition, swap-partition) vorgesehen. Der Einfachheit halber wird im folgenden nur noch von Auslagerungsdatei gesprochen, da in Bezug auf das Kriterium kein Unterschied in den Auslagerungsbereichen besteht. Der Arbeitsspeicher und die Auslagerungsdatei bilden zusammen den virtuellen Speicher, welcher von Anwendungen vollkommen transparent verwendet wird. Abhängig davon, ob bei der Speicherverwaltung ein Paging (einzelne Speicherseiten werden ausgetauscht) oder Segmentierung (ganze Segmente/Abschnitte werden ausgetauscht) angewendet wird [Vir04], finden sich Segmente oder Speicherseiten (pages) innerhalb der Auslagerungsdatei.

Bedeutet die Auslagerung von Teilen des Arbeitsspeichers auf die Festplatte aufgrund der langsameren Zugriffe auf das Medium, eventuell einen Nachteil für die Systemleistung, macht gerade dieser Umstand die Analyse einer Auslagerungsdatei für den Ermittler Interessant. In der Auslagerungsdatei befinden sich auch im Nachhinein noch Inhalte des flüchtigen Arbeitsspeichers wie zum Beispiel Fragmente von bearbeiteten Dateien oder Teile der zuletzt laufenden Anwendungen. Je nach Nutzung des Systems bzw. Gebrauch des virtuellen Speichers, können diese von der letzten Arbeitssitzung stammen oder teilweise auch älter sein. Diese Fragmente der Auslagerungsdatei sind aber vor allem dann interessant, wenn sie Informationen enthalten, die sich ansonsten nicht in dieser Form auf dem restlichen Datenträger befinden. Hierunter fallen zum Beispiel Passwörter, die von einer Anwendung im Arbeitsspeicher vorgehalten werden, damit sie nicht jedesmal neu eingegeben werden müssen. Aber auch das Vorhandensein von ursprünglich verschlüsseltem Text, der von einer Anwendung im Klartext im Speicher abgelegt wurde, damit er vom Benutzer betrachtet werden kann, wäre denkbar.

Generell ist der Zugriff auf Auslagerungsdateien mit einem gewöhnlichen (Hex-)Editor möglich, da sie sich nicht von normalen Dateien unterscheiden. Für die Bewertung des Kriteriums ist es also entscheidend, ob die restlichen Analysefunktionen des Werkzeugs ohne Probleme auf diese Auslagerungsdateien angewandt werden kann. Ähnlich wie bei der Untersuchung von nicht zugeordneten Bereichen wären hier spezielle Analysemethoden sinnvoll.

Anforderungen:

- Auslagerungsdateien der Windows Versionen (9x, ME) werden unterstützt.
- Auslagerungsdateien der Windows Versionen (NT/2000/XP) werden unterstützt.
- Auslagerungspartition von Linux/Unix Systemen werden unterstützt.
- Spezielle Analysefunktion werden angeboten.

Erscheinungsformen:

A Es stehen spezielle Analysefunktion für die Auslagerungsdateien zu Verfügung.

B Die restlichen Analysemethoden des Werkzeugs können auf die Auslagerungsdateien zugreifen.

C Es ist nur ein normales Anzeigen der Auslagerungsdatei möglich.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	im mittlerem Umfang erfüllt	2
C	nicht erfüllt	0

Kriterium 4.2.5
Verschlüsselte und komprimierte Daten

Kriterium	Gewicht
Analyse	
Daten Extraktion und Wiederherstellung	
Verschlüsselte und komprimierte Daten	2

Daten, die in verschlüsselter oder komprimierter Form vorliegen, sind für eine Untersuchung insofern ein Problem, da sie ihren eigentlichen Inhalt vor den umfangreichen und automatischen Analysemethoden, wie der Suche (Kriterium 4.3) oder Prüfsummenbildung (Kriterium 4.4), verbergen. Vor der eigentlichen Analyse müssen diese Daten zunächst gefunden bzw. erkannt und anschließend entschlüsselt bzw. dekomprimiert werden, damit sie den restlichen Analysemethoden zur Verfügung gestellt werden können. Dabei sind zwei Fälle zu unterscheiden:

1. Eine gewisse Auswahl von Daten wird mittels Verschlüsselung bzw. Kompression zu einer Datei zusammengefasst. Diese kann dann unabhängig vom System weitergegeben werden, wobei der Zugriff mit Hilfe eines entsprechenden Programms und evtl. eines Schlüssels vollzogen wird.

2. Ein bestimmter (Container-) Bereich wird vom System oder einem Programm zu Verfügung gestellt. Der Zugriff auf diese Bereich ist dann für den Benutzer transparent, d.h. die dort abgelegten Daten werden automatisch verschlüsselt bzw. komprimiert, die von dort stammenden Daten werden automatisch entschlüsselt bzw. dekomprimiert.

Der erste Fall ist vor allem für die abgesicherte und Platz sparende Weitergabe oder die Sicherung (backup) von Dateien interessant. Der zweite Fall eher für die tägliche Arbeit, um Speicherplatz zu sparen, oder um zu gewährleisten, dass Daten stets verschlüsselt abgelegt werden und nicht erst nach einem zusätzlichen (manuellen) Prozess.

Das Auffinden und die Zuordnung von Dateien des ersten Falls kann in den meisten Fällen anhand ihrer Datei-Endung bzw. Signatur (siehe auch Kriterium 4.3.5) noch relativ einfach erfolgen. Beim zweiten Fall ist dies abhängig von der verwendeten Applikation und der Container-Datei, da ein Container nach außen hin wie eine große Binärdatei aussieht. Ist diese mit einer Signatur bzw. einer bestimmten Datei-Endung versehen, oder ist sie ein vom Betriebssystem angebotenes Merkmal, so ist auch hier ein Auffinden und eine Zuordnung zu einer Applikation möglich. Bestehen diese Merkmale aber nicht, oder ist gar eine ganze Partition als Container-Datei angelegt, so bleibt nur die Möglichkeit Informationen aus anderen Quellen des Falls zu verwenden (z.B. anhand der installierten Programme), um weitere Rückschlüsse zu ziehen.

Bei der zweiten Phase, also der Entschlüsselung bzw. Dekomprimierung der Daten, bereiten vor allem verschlüsselte Daten ein Problem. Ohne den richtigen Schlüssel, welcher aber eventuell im Laufe der Untersuchung an einer anderen Stelle gefunden werden kann, ist ein Zugriff in der Regel nicht möglich, da eine Brute Force Entschlüsselung sehr Ressourcen aufwändig und teilweise sogar praktisch unmöglich ist. Für die aktuelle Bewertung werden sie daher außen vor gelassen. Bei komprimierten Daten reicht es hingegen aus, den entsprechenden Algorithmus festzustellen und anzuwenden, um auf die Daten zugreifen zu können.

Für den Ermittler wäre es also ideal, wenn das Analysewerkzeug jegliche Art von verschlüsselten bzw. komprimierten Daten anzeigen und den anderen Analysefunktionen zu Verfügung stellen könnte. Die Bewertung muss sich hier aber wiederum auf die gängigsten Kompressionsverfahren beschränken, da ansonsten eine Bewertung zu Aufwändig wird.

Anforderungen:

- Mit dem ZIP Algorithmus komprimierte Daten werden zu Verfügung gestellt.
- Mit dem TAR Algorithmus zusammengefasste Daten werden zu Verfügung gestellt.
- Mittels NTFS komprimierte Daten [NTF04] werden zu Verfügung gestellt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Zwei der genannten Punkte werden erfüllt.

C Nur einer der genannten Punkte wird erfüllt.

D Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	nicht erfüllt	0

Kriterium 4.2.6
ALTERNATE DATA STREAMS

Kriterium	Gewicht
Analyse	
Extraktion	
Alternate Data Streams	1

Alternate Data Streams (ADS) sind ein Bestandteil des NTFS Dateisystems. Sie bieten dem Betriebssystem, Anwendungen oder (sehr) erfahrenen Benutzern die Möglichkeit zusätzliche Informationen zu einer Datei oder einem Verzeichnis abzulegen. Dabei sind beliebig viele Streams pro Datei bzw. Verzeichnis möglich und ein Stream kann sowohl reinen Text (z.B. Kommentare), als auch binäre Daten (z.B. Miniaturbilder einer Bilddatei (thumbnails)) und ausführbaren Programmcode enthalten. Die Notation und der Zugriff auf einen Alternate Data Stream erfolgt dabei mit Hilfe des : Operators: `Dateiname:Stream-Name`. Für weitere Informationen und Beispiele über den Umgang mit Alternate Data Streams siehe [Hey02] und [Car04c].

Eine wesentliche Eigenschaft der Alternate Data Streams besteht aber darin, dass ihr Vorhandensein weder vom Windows Datei Explorer noch von einem `DIR` Befehl angezeigt werden. Für den Zugriff ist also entweder der genaue Name der Datei und der Name des zugehörigen Alternate Data Streams oder zusätzliche Software notwendig (z.B. streams [Str04]), welche Alternate Data Streams auflisten kann. Diese Eigenschaft bietet also die Möglichkeit Daten vor einem unerfahrenem Anwender oder Ermittler zu verstecken und kann auch dazu verwendet werden, ausführbaren Code (z.B. Viren [W2K00]) an Überwachungsdiensten vorbeizuschleusen, welche die Möglichkeit von Alternate Data Streams nicht beachten.

Aus forensicher Sicht ist es also notwendig, dass ein Analysewerkzeug diese Alternate Data Streams erkennt und deren Inhalt für weitere Analysezwecke, zum Beispiel den diversen Suchalgorithmen (Kriterium 4.3 Seite 71) oder der Prüfsummenbildung (Kriterium 4.2 Seite 60), zur Verfügung stellt.

Erscheinungsformen:

C Alternate Data Streams werden nicht unterstützt.

B Das Vorhandensein von Alternate Data Streams wird angezeigt, eine Weiterverarbeitung innerhalb des Werkzeugs ist aber nicht vorgesehen.

A Alternate Data Streams werden erkannt und ihr Inhalt für weitere Analysezwecke zu Verfügung gestellt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	im mittlerem Umfang erfüllt	2
C	nicht erfüllt	0

Kriterium 4.3
SUCHVERFAHREN

Kriterium	Gewicht
Analyse	
Suchverfahren	
Index Erstellung	2
Reguläre Ausdrücke	3
Phonetische Suche	1
Wortabstandssuche	1
Dateityp Anomalien	1

Diese Gruppe beschreibt zusätzliche Suchalgorithmen, welche die einfache Suche aufwerten und verfeinern. Sie sind daher als Ergänzungen für die eigentliche Suche nach Schlüsselwörtern gedacht. Die *Erstellung eines Index* ist zwar anfänglich sehr zeitaufwändig, die anschließende Suche erfolgt dann aber mit einer kaum feststellbaren Zeitverzögerung. Gerade für Untersuchungen bei denen abzusehen ist, dass die Suche intensiv verwendet wird (z.B. wenn noch keine Spur vorliegt oder wenn ein sehr großer Datenbestand mit textuellen Inhalt vorliegt), amortisiert sich der anfängliche Zeitaufwand sehr schnell. Das Kriterium wird daher als wichtig eingestuft.

Die Verwendung von *regulären Ausdrücken* bei einer Suche ermöglicht es, nicht nur nach genauen Zeichenketten zu suchen, sondern nach Mustern, die auf mehrere Zeichenketten passen. Dadurch sind umfangreichere Suchanfragen möglich, die bessere Resultate liefern können. Im Vergleich zu den anderen Kriterien ist dieses als sehr wichtig anzusehen.

Die Suche nach Wörtern mit gleichen *phonetischen* Eigenschaften oder mit einem bestimmten Abstand zueinander, sind weitere Verfeinerungen einer einfachen Suche, welche auch mit anderen Techniken erreicht werden kann (z.B. mittels regulären Ausdrücken oder mehrfacher Ausführung einer einfachen Suche). Sie sind daher im Kontext der Suchverfahren weniger wichtig.

Die Suche nach *Dateityp Anomalien* wird zum Auffinden mutmaßlich versteckter Dateien verwendet. Da diese Art der Suche eher selten verwendet wird, ist sie im Vergleich zu den anderen Suchverfahren ebenfalls als weniger wichtig einzustufen.

Kriterium 4.3.1
INDEX ERSTELLUNG

Kriterium	Gewicht
Analyse	
Suchverfahren	
Index Erstellung	2

Bei der indexbasierten Suche erfolgt die Suche nach Schlüsselwörtern nicht jedesmal im gesamten Datenbestand, sondern in einem vorher angelegetem Index, der im Datenbestand enthaltenen Zeichenketten. Neben den Zeichenketten sind im Index auch die Positionen abgelegt, an welchen sie sich im Datenbestand befinden. Eine erfolgreiche Suche im Index liefert neben der Existenz der Zeichenkette auch sofort alle Positionen im untersuchten Datenbestand.

Der Nachteil dieses Verfahrens ergibt sich durch das Anlegen des Index. Hierfür ist es zunächst notwendig den ganzen Datenbestand zu durchsuchen und die gefundenen Zeichenketten in den Index aufzunehmen. Abhängig von der Größe des Datenbestandes und der Durchsatzrate des Systems bei der Indizierung, kann die erste Suche folglich nur zeitverzögert ausgeführt werden. Da beide Größen aber am Anfang einer forensischen Untersuchung bekannt sein sollten, kann diese Zeitverzögerung eingeplant werden und zum Beispiel über Nacht erfolgen, da sie vollständig automatisch abläuft.

Ein enormer Vorteil der indexbasierten Suche besteht aber in der Ermittlung von Suchergebnissen, welche in einem Bruchteilen der Zeit erfolgt, die für eine einfache Suche auf den ganzen Datenbestand nötig wäre [Joh03]. Dies ist vor allem auf die Größe und den Aufbau des Index zurückzuführen, der in den nächsten Absätzen kurz erläutert wird, da dieser bei der Bewertung von Teilaspekten des Kriteriums mitberücksicht werden muss.

Ein Index gliedert sich im wesentlichen in zwei Bereiche, auf welche der Umfang des indizierten Datenbestandes unterschiedlichen Einfluss hat und die somit unterschiedlich stark anwachsen. Im Bereich, in dem die unterschiedlichen Zeichenketten abgelegt werden, ist ein logarithmischer Größenzuwachs zu beobachten [Joh03]. Dies liegt daran, dass immer weniger unterschiedliche Zeichenketten gefunden werden, da die Anzahl unterschiedlicher Zeichenketten sowohl von sinnvollen Vorgaben (z.B. Länge und zulässiger Zeichensatz der Wörter (siehe unten)), als auch vom existierenden Wortschatz einer geschriebenen Sprache[5] abhängig ist. Sobald hier ein gewisser Satz an Zeichenketten vorliegt, wird dieser Teil des Index also kaum noch anwachsen. Die Größe des zweiten Bereichs, in welchem die genaue Position der Zeichenketten abgelegt wird, wächst linear mit der Größe des indizierten Datenbestandes [Joh03], da für jede gefundene Zeichenkette hier ein weiterer Eintrag erfolgt.

Die Suche in einem Index beschränkt sich also auf das Suchen nach Zeichenketten im oben beschriebenen ersten Bereich. Die Ausgabe der relevanten Positionen erfolgt dann in vernachlässigbarer Zeit. Die Geschwindigkeit bei indexbasierten Suche ist also inhärent vom Aufbau dieses ersten Bereichs abhängig. Hierzu gehört zum Einen die verwendete Datenstruktur in welcher die Zeichenketten abgelegt werden. Diese soll hier nicht weiter erörtert werden, und es sei auf die gängige Literatur zu Index- und Speicherungsstrukturen verwiesen (z.B. [See03]). Zum Anderen wird der Aufbau und insbesondere die Größe des Index aber von den Eigenschaften der Zeichenketten abhängig, dir in den Index aufgenommen werden. Den Zeichenketten sollten also Einschränkungen auferlegt werden, die im Folgenden kurz erläutert werden, da diese, neben einem Größengewinn auch Auswirkungen auf die Resultate der Suche und damit auf die Resultate der forensischen

[5] Hier ist zu beachten, dass nicht nur vollständige Wörter, wie sie z.B. im Duden stehen, indiziert werden, sondern auch Teilzeichenketten dieser Wörter. Trotzdem ist auch hier die Anzahl der vorkommenden Zeichenketten durch die schriftliche verwendet Sprache begrenzt, da gewisse Zeichenketten in einer Sprache nicht verwendet werden (z.B. yxyxy im Deutschen) und somit auch mit großer Wahrscheinlichkeit nicht im indizierten Datenbestand auftauchen.

Untersuchung mit sich bringen.

Als erste Einschränkung sind hier die der erlaubten Zeichen in den Zeichenketten zu nennen. Eine Beschränkung auf alphanumerische Zeichen[6] und Umwandlung aller Großbuchstaben in ihr kleines Pendant, dürfte zum Beispiel für den größten Teil der Anfragen ausreichen, da somit ein sehr großer Teil der Wörter der geschriebenen Sprache abgedeckt ist. Im englischsprachigen Raum würde zum Beispiel bei einer Standardcodierung von 8 Bit für ein Zeichen, die Anzahl der unterschiedlichen Zeichen von 256 auf 36 reduziert werden. Dies führt zu einer erheblichen Reduzierung der theoretisch möglichen Zeichenketten und resultiert in einem kleineren Index und schnelleren Suchanfragen. Bei Sprachen mit vielen zusätzlichen Buchstaben (z.B. durch Akzentsetzung) oder der Verwendung von Unicode (vor allem im asiatischen Bereich) fällt dieser Vorteil natürlich geringer aus. Hier muss entweder das Fehlen dieser Zeichen akzeptiert, die Anzahl der verwendeten Zeichen erhöht oder auf andere Methoden, wie zum Beispiel eine automatische Übersetzung `ä` $\rightarrow$ `a` oder `ä` $\rightarrow$ `ae`, zurückgegriffen werden. Diese Einschränkung sollte also vom Ermittler konfigurierbar sein, um fallspezifisch reagieren zu können, da ansonsten eventuell ein lückenhafter Index entsteht, der zu falschen Suchergebnissen führen kann.

Als zweite Einschränkung wäre die Längenbegrenzung der Zeichenketten zu nennen. Sinnvoll ist hier eine Begrenzung auf minimal 4 und maximal 15 Zeichen [Bak04]. Kürzere Zeichenketten tragen in der Regel zu wenig suchrelevante Informationen, da diese entweder wenig charakteristische Wörter wie Artikel und Bindewörter sind (siehe auch nächsten Punkt) oder aber aus zufälligen Zeichenketten bestehen, wie sie in Binärdateien mitunter auftreten können. Längere Zeichenketten hingegen sind meist schon durch ihren kürzeren Wortanfang genau genug charakterisiert.

Schließlich ist bei der Indizierung der Dateien für eine forensische Untersuchung noch auf eine weitere Begebenheit zu achten. Reicht es im normalen Betrieb eines Computer aus, nur Zeichenketten in Dateien zu indizieren, welche dem Dateisystem bekannt sind, ist es für den Ermittler in einer forensischen Untersuchung entscheidend, alle Zeichenketten eines Images zu indizieren (z.B. in gelöschten Dateien oder nicht zugeordnetem Speicher). Dies geschieht meistens dadurch, dass die Rohdaten seriell (also ein Cluster nach dem Anderen) indiziert werden. Da die Daten aber mitunter durch das Dateisystem fragmentiert abgelegt werden (siehe Kriterium 4.2.3), ist es notwendig, diese Fragmentierung zu berücksichtigen und auch solche Zeichenketten richtig zu indizieren, welche am Ende eines Clusters beginnen und nicht im folgenden Cluster weitergehen.

Zusammengefasst bietet die indexbasierte Suche gegenüber einer normalen Suche, einen enormen Geschwindigkeitsvorteil. Dies wird durch einen Zeit- und Speicherplatzverlust beim Erstellen des Index erkauft. Fragen zur Performance sowohl beim Anlegen des Index als auch bei der Suche werden aber an dieser Stelle nicht bewertet, da hier der Kosten/Nutzen Faktor zu groß wäre. Gleiches gilt für den benötigten Speicherplatz. Beide Faktoren sind vor allem von den indizierten Daten abhängig und weniger vom verwen-

[6] Allgemein ist eine alphanumerische Menge eine Kombination aus Ziffern und den Buchstaben eines Alphabets, mit welchen die Wörter der Sprache gebildet werden. In der Englischen Sprache wäre dies (A-Z & a-z) und die Ziffern 0-9. In der Deutschen Sprache würden auch die Umlaute und das ß hinzugezählt werden.

detem Indizierungs-Algorithmus.

Für die Bewertung des Werkzeugs ist es entscheidend, neben der Möglichkeit einen vollständigen Index anzulegen, auch den Aufbau der Zeichenketten an die aktuelle forensische Untersuchung anzupassen. Weiterhin wäre es sinnvoll, auf dem Index nicht nur ein einfaches Suchen, wie es in diesem Kriterium angesprochen wurde, sondern auch die anderen Suchverfahren des Oberkriteriums (z.B. die Suche mittels regulärer Ausdrücke) zuzulassen.

Anforderungen:

- Eine indexbasierte Suche wird angeboten.
- Die Parameter für die Erstellung des Index können selbständig konfiguriert werden.
- Eine Suche im Index ist auch mittels der anderen beschriebenen Suchverfahren möglich.
- Die Fragmentierung von Daten, und damit eine Trennung von zusammengehörenden Zeichenketten, wird berücksichtigt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.3.2
REGULÄRE AUSDRÜCKE

Kriterium	Gewicht
Analyse	
Suchverfahren	
Reguläre Ausdrücke	2

Reguläre Ausdrücke (engl.: regular expressions) bilden eine Familie von formalen Sprachen, mit deren Hilfe sich Mengen von Zeichenketten beschreiben lassen. Bei der Suche werden sie verwendet, um spezielle Zeichenketten zu finden, die einem bestimmten Muster entsprechen. Damit diese Muster definiert werden können, ist es notwendig, einigen Zeichen des Alphabets (Metazeichen) von ihrer ursprünglichen Bedeutung zu trennen und ihnen erweiterte Eigenschaften zuzuordnen. Ist es notwendig, dass diese Metazeichen ihre ursprüngliche Bedeutung tragen, so müssen sie mit einem weiteren Metazeichen (escape Zeichen) gekennzeichnet werden, welches die erweiterten Eigenschaften eines Zeichens wieder aufhebt (in vielen Fällen der `'\'`). Ein regulärer Ausdruck setzt sich demnach aus einer Kombination von Zeichen des zugrunde liegenden Alphabets und Metazeichen zusammen.

Neben dem schon angesprochenen umgekehrten Schrägstrich `'\'` werden sehr häufig die Zeichen `'['`, `']'`, `'('`, `')'`, `'?'`, `'+'`, `'*'`, als Metazeichen verwendet, um bestimmte Konzepte bei der Beschreibung von Mustern zu realisieren. Die wichtigsten Konzepte sind hierbei Auswahl eines Zeichens, Angabe einer Zeichenklasse und die Möglichkeit der Quantifizierung. Mit Hilfe der Zeichenauswahl (`'['`, `']'`) ist es möglich, ein Muster anzugeben, welches erlaubt, an einer bestimmten Stelle einer Zeichenkette aus einer vorher angegebenen Menge von Zeichen auszuwählen. Zum Beispiel würde auf das Muster `[EA]ngel` sowohl das Wort `Angel` als auch `Engel` passen. Die Möglichkeit der Zeichenklassen erweitert dieses Konzept der Auswahl, auf eine ganzen Klasse von semantisch zusammengehörigen Zeichen. So beschreibt zum Beispiel der Ausdruck `\d` die Klasse der Ziffern (engl.: **d**igit), welche auch mit Hilfe der Auswahl `[0123456789]` bzw. `[0-9]` beschrieben werden könnte. Schließlich bietet das Konzept der Quantifizierung die Möglichkeit, das mehrfache Auftreten von gleichen Mustern in einer Zeichenkette zu modulieren. Dies geschieht in der Regel durch Anhängen eines Quantors an ein schon vorhandenes Muster. Der Ausdruck `\d+` würde zum Beispiel die Zeichenketten der natürlichen Zahlen beschreiben, welche aus dem mehrfachen Vorkommen (`+`) von Ziffern (`\d`) aufgebaut sind.

Der letzte Absatz sollte nur einen groben Überblick über die Funktionsweise von regulären Ausdrücken bieten und ist in keiner Weise vollständig. Für mehr Informationen bieten sich [Reg04] und eine weitere Recherche im Internet an, welche zum Thema reguläre Ausdrücke umfassendes Material liefert. Welche Zeichen aber schließlich als Metazeichen Verwendung finden und welche Bedeutung sie tragen, ist stets von der Implementierung der Suche abhängig und sollte im zugehörigen Handbuch nachgeschlagen werden.

Für den Ermittler bietet die Suche mittels regulären Ausdrücken den Vorteil, dass diese nicht genau nach einer bestimmten Zeichenkette erfolgen muss, sondern die Möglichkeit besteht, Zeichenketten zu finden, welche in ein bestimmtes Muster passen. Hierdurch ist es möglich, die Menge der potentiellen Treffer um einiges zu erhöhen, aber dennoch durch geeignete Wahl der Muster ihren Umfang so weit einzuschränken, dass sie überschaubar bleibt. Die Suche kann also spezifischer und fein granularer ausfallen. Denkbar wäre hier zum Beispiel die Suche in Dokumenten, die alle ein Datum in einem bestimmten Format beinhalten (z.B. JJJJ-MM-TT). Mit Hilfe eines geeigneten Musters könnte die Suche zum Beispiel auf Dokumente eines bestimmten Zeitraums begrenzt werden, welche in den Zeitraum des untersuchten Vorfalles passen (z.B. 2001-09-1[01234] für die Suche nach Dokumenten im Zeitraum des Anschlags auf das World Trade Center). Ohne reguläre Ausdrücke wären hier entweder mehrere einzelne Suchanfragen notwendig, oder man müsste eine größere Anzahl von Treffern, bei einer Suche nach 2001-09-1, akzeptieren.

Die Bewertung dieses Kriteriums würde sehr umfangreich werden, wenn sie sich auf die Mächtigkeit der formalen Sprache beziehen würde, welche zur Bildung der regulären Ausdrücke vom Werkzeug bereitgestellt wird. Hierzu müsste man zum Beispiel bewerten, welche und wie viele Konzepte zur Beschreibung von Mustern möglich sind und „wie gut“ diese implementiert sind. Vom Umfang entspricht dies aber einem eigenen Kriterienkatalog, welcher den Rahmen dieser Arbeit und insbesondere den Aufwand beim Testen erheblich vergrößern würde. Für den aktuellen Katalog ist in diese Richtung also nur eine grobe Einschätzung möglich.

Erscheinungsformen:

C Es werden keine regulären Ausdrücke bei der Suche erlaubt.

B Einfache Ersetzungen sind erlaubt (wildcard-Suche) .
(z.B. ? für einmaliges Vorkommen beliebiger Zeichen, * für beliebiges Vorkommen beliebiger Zeichen.)

A Eine reguläre Sprache wird angeboten, welche es ermöglicht, reguläre Ausdrücke bei der Suche zu verwenden.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	im mittlerem Umfang erfüllt	2
C	nicht erfüllt	0

Kriterium 4.3.3
PHONETISCHE SUCHE

Kriterium	Gewicht
Analyse	
Suchverfahren	
Phonetische Suche	1

Die phonetische Suche (Ähnlichkeitssuche) ist eine Suche, die auf dem Annäherungsprinzip basiert. Im Gegensatz zur einfachen Suche, in welcher eine genaue Übereinstimmung mit dem Suchbegriff gefordert wird, werden hierbei auch Ergebnisse akzeptiert, welche sich nahe bei dem gesuchten Begriff befinden. Im Fall der phonetischen Suche wird diese Nähe durch die ähnliche lautende Aussprache des Suchbegriffs definiert. Zum Beispiel werden im Deutschen die Nachnamen Meier, Maier und Mair sehr ähnlich ausgesprochen und eine Unterscheidung ist in der Regel nur durch Nachfragen möglich. Bei einer phonetischen Suche nach Meier würden alle 3 Begriffe im Ergebnis auftauchen, bei einer einfachen Suche müssten hier 3 Suchanfragen gestartet werden. Die phonetische Suche ist also inhärent von der verwendeten Sprache abhängig, was zu einigen Problemen bei der Implementierung führt, welche später kurz angesprochen werden. Zunächst ist aber zu klären, warum die phonetische Suche überhaupt für die forensische Untersuchung von Bedeutung ist.

Dies liegt an der schon oben angesprochenen Mehrdeutigkeit bei der Verwendung der natürlichen Sprache, welche zu Inkonsistenzen bei der Schreibweise mancher Begriffe, also zu vermeintlich falscher Rechtschreibung, führen kann. Diese Mehrdeutigkeiten können nun an unterschiedlichen Stellen entstehen, welche im Laufe einer Ermittlung eventuell betroffen sind und vom Ermittler berücksichtigt werden müssen.

Zum Einen können dieses Mehrdeutigkeiten schon bei der ursprünglichen Eingabe oder Zusammenstellung der untersuchten Daten erfolgen. Entstehen hier Inkonsistenzen, existieren diese natürlich auch anschließend im untersuchten Bitstream-Image und sollten bei einer Untersuchung berücksichtigt werden, da eine direkte Suche nur Teilergebnisse liefern würde. Diese Art von Inkonsistenzen können zum Beispiel dann entstehen, wenn bereits der bei der Erstellung der Daten nur mehrdeutige Informationen (z.B. per Telefon oder aus unterschiedlichen Quellen) vorliegen, mehrere Personen an der Erstellung eines Dokuments arbeiten und unterschiedliche Schreibweisen von Begriffen verwenden, oder wenn bewusst falsche Rechtschreibung in einer Kommunikation verwendet wird (z.B. in einem Chat, um Schreibarbeit zu sparen oder weil eine veränderte Sprache verwendet wurde [Lee04]).

Zum Anderen können diese Mehrdeutigkeiten aber auch auf Seiten des Ermittlers auftreten. Beruht die Suche nach Schlüsselwörtern in einem Fall zum Beispiel auf der mündlichen Aussage eines Zeugen, welcher entsprechende Wörter nur beiläufig aufgeschnappt hat, oder kann der Auftraggeber einer Untersuchung die entsprechende Suchbegriffe nur grob umreißen, liegt es am Ermittler, diese Mehrdeutigkeiten aufzulösen. Die phonetische Suche kann hier den Ermittler unterstützen, so dass nicht mühsam alle denkbaren

Kombinationen von Hand überprüft werden müssen oder gar einen Teil der Ergebnisse übersehen werden.

Wie bereits angedeutet bereitet diese Mehrdeutigkeit bei der phonetischen Suche aber einige Probleme bei der Implementierung eines Suchalgroithmus. Der Algorithmus muss hier auf effiziente Weise gleichklingende Worte zu einer bestimmten Zeichenfolge kodieren, mit deren Hilfe dann der Datenbestand durchsucht werden kann. Da die Mehrdeutigkeiten aber inhärent von der verwendeten Sprache abhängen, gilt diese Abhängigkeit natürlich auch für die verwendete Kodierung. Dies hat zur Folge, dass nur sehr wenige solcher Algorithmen existieren [Bor04], die zumeist nur für eine oder wenige Sprachen ein Kodierungsschema bieten und des Weiteren für eine phonetische Suche im forensischen Bereich nicht feingranular genug sind. Für die englische Sprache, welche aus phonetischer Sicht gut zu modellieren ist, existiert zum Beispiel der relativ bekannte Soundex Algorithmus[7] [Nat95], der aber sehr grobgranular ist und deswegen für eine forensische Untersuchung, insbesondere im deutschsprachigem Raum, nicht geeignet ist. So würde er zwar für den oben angesprochenen Namen Meier für alle drei Ausprägungen den gleichen Code liefern (M600), aber auch für „Meer“ oder „Moor“ eine Übereinstimmung zeigen.

Die Problematik, dass nur wenige Algorithmen existieren, die noch dazu sehr stark sprachabhängig, und für eine Untersuchung eventuell zu grobkörnig sind, hat dementsprechend auch Auswirkungen auf die Bewertung des aktuellen Kriteriums. Da bei der aktuellen Vernetzung von digitalen Systemen nicht mehr davon ausgegangen werden kann, nur eine verwendete Sprache auf dem System vorzufinden und weiterhin kein universeller Algorithmus für alle Sprachen existiert, ist das Ergebnis einer phonetischen Suche sehr stark vom verwendetem Algorithmus, dem untersuchten Image und dem Gespür des Ermittlers abhängig.

Erscheinungsformen:

C Die phonetische Suche wird nicht angeboten.

B Eine einfache phonetische Suche wird angeboten.

A Für eine phonetische Suche stehen mehrere Algorithmen zur Auswahl.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	im mittlerem Umfang erfüllt	2
C	nicht erfüllt	0

[7] Die Soundex-Suche führt eine Suche aus, die auf dem Anfangsbuchstaben und den folgenden Konsonanten basiert. Sie funktioniert also nur für vollständige Wörter und liefert für Teilwörter keine Resultate. Es werden also Wörter gefunden, deren Vokale unbekannt sind.

Kriterium 4.3.4
WORTABSTANDSSUCHE

Kriterium	Gewicht
Analyse	
Suchalgorithmen	
Wortabstandssuche	1

Die Wortabstandssuche ist eine besondere Art der Kombination von zwei oder mehr gesuchten Zeichenketten. Hierbei werden zusätzliche Bedingung angegeben, welche die Relation der gefundenen Zeichenketten in einem Text genauer beschreiben. Als einfache Bedingung ist hier der Abstand zwischen den zwei Wörtern zu nennen. Dabei bietet sich als Entfernungsangabe für diesen Abstand das Produkt aus Anzahl und Einheit (Wort, Satz, Absatz, Seite) an.

Die Berechtigung oder Sinn für eine Wortabstandssuche liegt in der Überlegung, dass bestimmte Wörter nur fallrelevant sind, wenn sie in einem bestimmten Kontext (in diesem Fall der Abstand) zueinander stehen. Wird zum Beispiel in einem Fall ermittelt, in dem ein bestimmter Tatort und eine Person involviert sind, so könnten gerade die Texte interessant sein, in welchen beide Begriffe auftauchen. Dies führt zu einer weiteren Überlegung, dass Wörter, welche in einem Text näher beieinander stehen, wahrscheinlich auch inhaltlichen einen höheren Bezug zueinander aufweisen, als weiter auseinander stehende.Für das obigen Beispiel würde das bedeuten, dass ein Text umso relevanter ist, je näher die beiden Suchbegriffe beieinander liegen. Durch die Wortabstandssuche kann also unter Umständen schon eine Vorselektion von relevanten Daten erfolgen, was zu einem erheblich schnelleren Voranschreiten einer Untersuchung führen kann.

Um diesen Effekt der Vorselektion eventuell noch weiter zu erhöhen, können zusätzliche Bedingungen für die Relation der Suchbegriffe festgelegt werden. Hier wäre zum Einen das Zulassen von mehreren Wörtern zu nennen. Existieren für eine Untersuchung mehrere Suchbegriffe, so kann analog zu oben davon ausgegangen werden, dass ein Text umso relevanter ist, je mehr Suchbegriffe er enthält und je näher diese beieinander liegen. Zum Anderen kann aber auch die Reihenfolge der Wörter von Bedeutung sein, da hierdurch eine weitere semantische Bedeutung in die Suchanfrage fließen kann. Zum Beispiel trägt der Satz „Die Aktion XXX von YYY löste den Vorgang ZZZ aus“ eine ganz andere Bedeutung als „Der Vorgang ZZZ löste die Aktion XXX von YYY aus“.

Anforderungen:

- Eine einfache Wortabstandssuche wird unterstützt.
- Die Abstandssuche wird auch für mehrere Wörter erlaubt.
- Die Abfolge der Suchwörter kann vorgegeben werden.
- Weitere Bedingungen für die Relationen der Suchbegriffe können angegeben werden. Zum Beispiel die Grenzen für den Suchraum, in welchem sich die Wörter befinden müssen (z.B. Satzzeichen wie “, oder HTML Tags).

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.3.5
DATEITYP ANOMALIEN

Kriterium	Gewicht
Analyse	
Suchverfahren	
Dateityp Anomalien	2

Die Suche von Dateityp-Anomalien unterscheidet sich von den bisher genannten Suchverfahren. Wurden bisher Verfahren vorgestellt, die den Ermittler unterstützen sollen, Daten mit bestimmten Schlüsselwörter zu finden, welche in Verbindung mit der Untersuchung stehen, so wird bei der Suche nach Dateityp-Anomalien nach vermeintlichen Manipulationsversuchen gesucht, die eventuell Hinweise auf interessante Daten zeigen.

Um eine Dateityp-Anomalie zu entdecken, ist es zunächst notwendig zu wissen, wie überhaupt ein Dateityp erkannt wird. Unter den Windows Betriebssystemen gibt ein Punkt gefolgt von einer Kombination aus drei Buchstaben den Dateityp an (z.B. `.jpg` für eine Bilddatei, welche mittels des JPEG Algorithmus komprimiert wurde). Mit dieser Endung ist dann eine Anwendung assoziiert (zu finden unter Systemsteuerung - Ordneroptionen - Dateityp), welche den entsprechenden Dateityp verarbeiten kann. Andere Betriebssysteme (z.B. Linux) werten diese Endung aber nicht aus, sondern verwenden eine andere Art der Erkennung. Diese beruht auf der Eigenschaft, dass viele Dateitypen einen charakteristischen Dateianfang von 2 bytes, im folgenden Signatur genannt, besitzen. Diese Signatur (z.B. `FF D8` für JPEG Bilddateien) ist dann zusammen mit der zugehörigen Anwendung in einer bestimmten Datei (magic file) abgelegt, in welcher beim Öffnen einer Datei entsprechend nachgeschlagen werden kann (Diese Überprüfung kann auch mittels `file` <`Dateiname`> manuell erfolgen).

Der Umstand, dass Windows und auch sehr viele Anwender den Dateityp anhand der Endung erkennen, kann nun dazu missbraucht werden, Dateien zu verstecken indem die Dateiendung abgeändert wird. Ändert man zum Beispiel die Endung einer Bilddatei in die Endung einer Textdatei, so kann diese Datei evtl. von einem Bildverabeitungsprogramm, welches sich nur auf die Dateiendung verlässt, nicht mehr erkannt werden. Wird also ein Datenträger mit Hilfe dieses Programms durchsucht, so übersieht er die entsprechende Datei. Wird diese Datei zusätzlich noch in ein Verzeichnis abgelegt, das viele unterschiedliche Dateien enthält (z.B. das Windows System Verzeichnis), so kann es durchaus vorkommen, dass diese Datei übersehen wird.

An dieser Stelle setzt nun die Suche nach Dateityp-Anomalien an. Hierzu muss das Werkzeug, ähnlich dem Linux System, eine Liste von Dateiendungen und zugehörigen Signaturen führen. Für jede Datei im untersuchten Image muss dann eine Überprüfung in dieser Liste erfolgen. Tritt eine Anomalie auf, sollte eine Warnung erfolgen und falls möglich weitere Informationen gegeben werden. Diese zusätzlichen Informationen wären zum Beispiel, ob zu einer bekannten Dateiendung eine andere bekannte Signatur vorliegt, was auf einen Täuschungsversuch hindeuten kann. Des Weiteren sollte es möglich sein, diese Liste auf einfache Weise zu erweitern. Dies kann zum Beispiel notwendig sein, wenn eine Firma ein eigenes, proprietäres Dateiformat verwendet oder für ein bekannten Dateityp ein neues Dateiformat erscheint, welches eine neue Signatur trägt.

Anforderungen:

- Eine allgemeine Untersuchung auf Dateityp-Anomalien kann durchgeführt werden.
- Falls eine Anomalie vorliegt, wird diese vom Werkzeug genauer spezifiziert.
- Die Liste der Dateitypen und zugehörigen Signaturen kann erweitert werden.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Zwei der genannten Punkte werden erfüllt.

C Nur einer der genannten Punkte wird erfüllt.

D Keiner der Punkte wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	nicht erfüllt	0

Kriterium 4.4
PRÜFSUMMENBILDUNG

Kriterium	Gewicht
Datenanalyse	
Prüfsummenbildung	
Datenreduzierung	2
Existenzprüfung	2

Die Verwendung von (kryptographischen) Prüfsummen (engl.: message digest) kann in der Forensik an unterschiedlichen Stellen erfolgen. Bevor diese Verwendung und insbesondere der Einsatz erläutert wird, ist es zunächst sinnvoll zu klären, was Prüfsummen überhaupt darstellen und wie sie erzeugt werden.

Kryptographische Prüfsummen werden mit Hilfe von kryptographisch sicheren Hashfunktionen berechnet. Hashfunktionen sind nicht injektive Funktionen, welche Eingabedaten des Urbildes (oft auch Universum genannt) in einen Hashwert des, in der Regel kleineren, Bildbereiches (Adressbereiches) überführen. Diese Hashwerte (Prüfsummen) können dann dafür genutzt werden, die Integrität der ursprünglichen Eingabedaten zu überprüfen (Bildung eines digitalen Fingerabdrucks) oder um eine digitale Signatur zu erstellen.

Da bei der Berechnung von Hashwerten, auf Grund des kleineren Bildbereiches, Kollisionen[8] entstehen können, sind an die Hashfunktion einige Bedingungen (z.B. Kollisionsvermeidung) zu stellen, damit die Eingabedaten eindeutig durch ihren Hashwert charakterisiert werden können und somit die Überprüfung der Integrität der Daten gewährleistet ist. Erfüllt eine Hashfunktion die folgenden Punkte, so spricht man von einer kryptographischen (sicheren) Hashfunktion [Eck03], [Pom04].

1. Der Hashwert ist schnell und einfach zu berechnen und besitzt eine feste Länge.

2. Die Rekonstruktion der ursprünglichen Daten aus dem Hashwert ist nicht möglich.

3. Es ist praktisch unmöglich, ein Paar verschiedener Eingabewerte zu finden, deren Hashwert übereinstimmt.

4. Für einen vorgegebenen Hashwert eines Eingabewertes ist es praktisch unmöglich, einen weiteren Eingabewert zu finden, welcher den gleichen Hashwert liefert.

Die ersten beiden Punkte erinnern stark an die Eigenschaften einer Einwegfunktion[9]. Die beiden letzten Punkte leiten sich vom Geburtstagsparadoxon[10] ab. Des Weiteren

[8]Eine Kollision tritt dann ein, wenn die Hashfunktion für unterschiedliche Eingabedaten den gleichen Hashwert liefert.

[9]Eine injektive Funktion $f : X \rightarrow Y$ ist eine Einwegfunktion, wenn für alle $x \in X$ der Funktionswert $f(x)$ effizient berechenbar ist und kein effizientes Verfahren existiert, das Urbild $f^{-1}(x)$ zu berechnen.

[10]Das Geburtstagsparadoxon behandelt die Fragen, wie viele Personen sich in einem Raum befinden müssen, damit die Wahrscheinlichkeit größer 50% ist, das zwei beliebige Personen am gleichen Tag Geburtstag haben bzw. dass eine Person anwesend ist, deren Geburtstag mit einem vorgegebenen Geburtstag übereinstimmt.

sollte eine Hashfunktion noch den folgenden zwei Punkte genügen, um ihre Eignung als Integritätsnachweis weiter zu erhöhen:

5. Die Änderung eines Bits in den Eingabedaten führt zu einer Änderungswahrscheinlichkeit von 50% für jedes Bit der Prüfsumme.

6. Der Algorithmus der Hashfunktion ist öffentlich bekannt.

Punkt fünf führt dazu, dass falls zu einem Hashwert zwei unterschiedliche Eingabedaten gefunden werden, die Wahrscheinlichkeit sehr hoch ist, dass diese Eingabedaten sich an vielen Stellen sehr stark unterscheiden. Damit sollte es unmöglich sein, durch Hinzufügen von Leer- oder Füllzeichen in einem Textdokument oder durch Hinzufügen von Kommentaren in ausführbaren Code, die ursprüngliche Datei so zu verändern, dass zwar immer noch der gleiche Hashwert geliefert wird, aber inhaltlich eine völlig andere Bedeutung vorliegt bzw. eine andere Funktionalität gegeben ist. Punkt sechs stellt sicher, dass die Sicherheit der kryptographischen Hashfunktion (sieh obigen 4 Punkte) nicht von der Kenntnis oder Unkenntnis des verwendeten Algorithmus abhängig ist, sondern einzig von dessen Leistungsfähigkeit.

Bekannte und verbreitete Vertreter der kryptographischen Hashfunktionen, welche zur Bildung von Hashwerten verwendet werden, sind der Secure Hash Algorihtm (SHA-1) des amerikanischen National Institute of Standards and Technology (NIST) [oSN02] und Message Digest 5 (MD5) von Ron Rivest [Riv92].

Wie bereits anfangs erwähnt werden diese Prüfsummen in der Forensik an unterschiedlichster Stelle verwendet. Insbesondere finden sie bei der in Abschnitt 2.2 beschrieben online Datenerfassung Verwendung, um die Integrität der erfassten und nicht persistenten Daten zu gewährleisten. Des Weiteren besteht natürlich auch die Möglichkeit mittels Prüfsummen sicherzustellen, dass während einer Analyse die untersuchen Festplattenimages keiner Veränderung unterlagen. Interessant für die vorliegende Arbeit ist aber die Möglichkeit, zu jeder Datei, des zu analysierenden Images, eine Prüfsumme zu berechnen und deren Existenz in einer Datenbank zu überprüfen.

Das Werkzeug sollte also zum Einen dazu in der Lage sein, entweder für alle, oder nur einen Teil der untersuchten Dateien, zum Beispiel Dateien in einer bestimmten Größenordnung oder Typs (Bilder), auf unkomplizierte Weise eine Prüfsumme zu erstellen. Zum Anderen sollte die Möglichkeit bestehen, die Existenz der Prüfsumme, sowohl in öffentlich zugänglichen [NSR04], wie auch in selber erstellten Datenbanken durchzuführen. Um die Effektivität dieser Methode weiter zu erhöhen, sollte es möglich sein, auf den resultierenden Datenbestand ein wiederholtes Nachschlagen in verschiedenen Datenbanken durchzuführen.

Diese Technik der Prüfsummenbildung und Überprüfung kann nun auf zweierlei Arten verwendet werden, um mit größeren Datenbeständen umzugehen. Einerseits kann die zu untersuchende Datenmenge verringert werden (Datenreduzierung), indem eine Datenbank verwendet wird, welche Prüfsummen von bekannten Dateien (z.B. Bestriebssystemdateien) enthält. Andererseits können die Prüfsummen auch dafür verwendet werden, um gezielt nach bestimmten Dateien zu suchen (Existenzprüfung). Wiederum sind der Einsatz und damit die Verwertbarkeit der Ergebnisse sehr stark vom untersuchten Fall abhängig. Wird zum Beispiel explizit nach bestimmten Dateien gesucht, ist eine Datenreduzierung nicht notwendig. Sind hingegen keine Dateien bekannt, welche relevante Daten enthalten könnten, ist eher eine Datenreduzierung sinnvoll, um den Suchraum zu verkleinern. Daher werden beide Verfahren im Verhältnis zueinander als gleich wichtig eingestuft.

Kriterium 4.4.1
DATENREDUZIERUNG

Kriterium	Gewicht
Analyse	
Prüfsummenbildung	
Datenreduzierung	2

Wie bereits beschrieben erfolgt die Datenreduzierung mit Hilfe von Prüfsummen derart, dass für jede Datei eine Prüfsumme gebildet wird und deren Existenz in einer Datenbank nachgeschlagen wird. Ist eine Prüfsumme in der Datenbank präsent, so kann auf Grund der Verwendung von kryptographischen Hashfunktionen (siehe Oberkriterium) davon ausgegangen werden, dass es sich hierbei um eine bekannte Originaldatei handelt, welche von weiteren Untersuchungen ausgeschlossen werden kann.

Entscheidend für den Effekt der Datenreduzierung ist also die Verwendung geeigneter Datenbanken. Neben Datenbanken welche die Prüfsummen für die verbreitesten Betriebssysteme und Anwendungen beinhalten [NSR04] sind hier auch fallspezifische Datenbanken zu nennen. Werden zum Beispiel Images einer Firma untersucht, die alle einen bestimmten firmenspezifischen Satz an Dateien enthalten, ist es sinnvoll, diese Dateien von einer weiteren Untersuchung auszuschließen (z.B. CAD Modelle der verarbeiteten Bauteile, ein Standard Image, dass Installiert wird).

Anforderungen:

- MD5 wird unterstützt.
- SHA-1 wird unterstützt.
- Das Werkzeug ermöglicht es auf einfache Weise eigene Datenbanken aus einem auswählbaren Datenbestand zu erstellen.
- Die (gleichzeitige) Abfrage mehrerer Datenbanken ist möglich.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.4.2
EXISTENZPRÜFUNG

Kriterium	Gewicht
Analyse	
Prüfsummenbildung	
Existenzprüfung	2

Die Existenzprüfung bezeichnet die Suche nach einer Datei, deren Prüfsumme in einer bestimmten Datenbank vorliegt. Sie ähnelt der Datenreduzierung und beinhaltet ebenso die dort besprochenen Überlegungen zum Thema Hashalgorithmen und Datenbanken. Der einzige Unterschied besteht darin, dass bei einer Übereinstimmungen die entsprechenden Dateien nicht verworfen werden, sondern genau an diesen Dateien die weitere Untersuchung vollzogen wird. In den meisten Fällen werden diese „gefundenen“ Dateien aber schon das Resultat einer Untersuchung darstellen, da Dateien geliefert werden, die abhängig von der verwendeten Datenbank, einer bestimmten Eigenschaft genügen (z.B. Dateien deren Besitz strafbar ist).

Ein großer Vorteil dieser Methode beruht auf ihrer hohen Automatisierbarkeit (fragliche Dateien und entsprechende Datenbank auswählen, Überprüfung starten) und damit in der Möglichkeit, große Datenmengen automatisch einer forensischen Untersuchung zu unterziehen. So ist das Anlegen und Vorhalten einer Dateisammlung (z.B. Bilder, Musik, Filme oder Schriftstücke) im vier- bis fünfstelligen Bereich, auf Grund der einfachen Beschaffung (z.B. mittels eines Breitband Internetzugangs und der Verwendung von Peer to Peer Netzen oder FTP-Server) und aktueller Massenspeichergrößen (Festplatten im hundert Gigabyte Bereich sind Standardkomponenten), eine einfache Aufgabe. Diese Dateisammlung aber nach einem bestimmten Inhalt von Hand zu durchsuchen, wäre sehr zeitaufwändig. Geht man zum Beispiel davon aus, dass die Ansicht und Bewertung einer Bild-Datei 2 Sekunden veranschlagt, würde man allein für die Durchsicht eines 10000 Bilder umfassenden Archivs gute sechs Stunden brauchen, sofern man diese Informationsflut überhaupt durchhalten würde. Mittels der Bildung von Prüfsummen kann diese Aufgabe um einiges schneller[11] oder zeitsparender über Nacht erfolgen.

[11] Auf einem veralteten Pentium 90 hat md5 einen Durchsatz von ca. 5,5 MByte pro Sekunde [Tou95].

Ein weiterer Vorteil bei der Verwendung von Prüfsummen besteht darin, dass bei einer Übereinstimmung mit der Datenbank, der Inhalt der Datei eventuell nicht bekannt sein, oder vollständig analysiert [12] werden muss, sondern die Instanz, welche die Datenbank zu Verfügung stellt, dies bereits durch die Bereitstellung der Prüfsummen vollzogen hat.

Für den Ermittler ist dies ein Vorteil, da er so Dateiinhalte bewerten oder erkennen kann, ohne dass er auf dem Gebiet, das der Inhalt beschreibt oder darstellt, ein Experte sein muss. Dies findet zum Beispiel bei der Erkennung von schädlichen Programmen (z.B. Viren, Rootkits, Trojanischen Pferden, usw.) statt, bei welchem der Ermittler sowohl den schädlichen Charakter bzw. Code des Programmes identifizieren, als auch die Schwächen des Wirtssystem kennen müsste. Aber auch bei Inhalten von Dateien, deren Beurteilung von subjektiven Eindrücken beeinflussbar ist (z.B. volksverhetzende Schriften und Lieder), kann die Verwendung entsprechenden Datenbanken eine Hilfe sein. Für den Bereitsteller einer Prüfsummendatenbank bietet dieses Verfahren den Vorteil, dass Informationen zur Identifizierung von Dateien bereitgestellt werden können, ohne die eigentlichen Inhalte selber vorzuhalten oder bekannt zu geben. Dies kommt zum Beispiel bei der Erkennung von Medien mit pädophilen Inhalten zum Zuge, deren Besitz schon strafbar ist.

Die Verwendung der im Oberkriterium beschriebenen kryptographischen Hashverfahren birgt aber auch einen Nachteil, der kurz erwähnt werden sollte. Die Erfassung einer Datei mittels einer Prüfsummen funktioniert nur an schon bekannten Dateien, von welchen auch eine Prüfsumme angelegt werden konnte! Da aber schon eine kleine Veränderung in der Ausgangsdatei zu einer unterschiedlichen Prüfsumme führt, ist es ausreichend, an seinem Datenbestand eine kleine Änderung vorzunehmen (z.B. mittels eines selbstgeschriebenen Programms oder der Stapelverarbeitungsfunktion einer Anwendung), um eine Erkennung mittels Prüfsumme zu umgehen. Das Aufhellen von Bildern oder die Lautstärkenanhebung um 1% bei Musik, würde zum Beispiel für die meisten Anwender keinerlei Unterschied in der Nutzung des Inhalts bedeuten, für einen Prüfsummentest hätte dieses Vorgehen aber gravierende Auswirkungen.

Anforderungen:

- MD5 wird unterstützt.
- SHA-1 wird unterstützt.
- Das Werkzeug ermöglicht es auf einfache Weise eigene Datenbanken aus einem auswählbaren Datenbestand zu erstellen.
- Die (gleichzeitige) Abfrage mehrerer Datenbanken ist möglich.

Geht man von hochwertigen Bildern von 1 MByte Größe aus, wären dies ca. 5 Bilder pro Sekunde, sofern man für eine einfache Datenbankanfrage einen Bereich von wenigen Millisekunden ansetzt. Die Überprüfung mittels Prüfsummen wäre als zehnmal schneller als die manuelle Untersuchung. Bei aktuellen Prozessoren dürfte dieser Vorteil noch um einiges größer ausfallen.

[12] Eine Überprüfung, ob die Datei auch wirklich die Gesuchte Datei ist und nicht der (unwahrscheinliche) Fall eingetreten ist, dass eine identische Prüfsumme berechnet wurde, muss natürlich dennoch erfolgen.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.5
INTERNET BENUTZUNG

Kriterium	Gewicht
Analyse	
Internet Benutzung	
Internetbrowser	2
E-Mail Anwendungen	3
Messanger	1
Peer to Peer Netze	X

An dieser Stelle wurden nur die wichtigsten Anwendungskategorien ausgewählt, die bei Kommunikation über das Internet verwendet werden. Sie bieten eine entscheidende Quelle für Informationen zu Systemen oder Personen, welche mit dem Besitzer des Datenträgers in Kontakt standen, von welchem das zu untersuchende Image stammt. Die entscheidene Kategorie ist hierbei die Auswertung von *E-Mail Anwendungen*. Neben den Informationen über die Kommunikationspartner, kann in vielen Fällen auch an Informationen über den Kommunikationsinhalt gelangt werden.

Im Vergleich dazu wird die Auswertung des *Internetbrowsers* als wichtig eingestuft. Der Browser ist eine Quelle für Informationen, welche den Verdächtigen interessieren. Aus diesen können eventuell Rückschlüsse auf ausgeführte oder geplante Aktionen erfolgen. Ein *Messenger* kann als Quelle von (persönlichen) Kontakten herangezogen werden, welche als zusätzliche Informationsquelle (Zeugen) herangezogen werden können.

Peer to Peer Netze sind als Quelle für Informationen nur in bestimmten Situationen hilfreich. Des Weiteren wurde kein geeigneter Bewertungsschlüssel gefunden, so dass dieses Kriterium nicht gewertet wird.

Kriterium 4.5.1
INTERNETBROWSER

Kriterium	Gewicht
Analyse	
Internet Benutzung	
Interntbrowser	2

Der Internetbrowser ist bei der Benutzung des Internets nicht mehr wegzudenken. Neben dem reinen betrachten von WWW Seiten, wird er zunehmend auch für den Datenzugriff auf andere Ressourcen wie EMail (GMX, YAHOO, HOTMAIL, ...), Datenbanken (phpMyAdmin) oder die Konfiguration von Systemen verwendet, auf welchen zum Beispiel ein kleiner Webserver läuft. Bei der Kommunikation mit diesen Ressourcen fallen eine Menge von Daten an, welche in der Regel vom Browser auf dem verwendeten System zwischengespeichert werden. Diese Daten können entweder selber schon fallrelevant sein (z.B. unerlaubte Nutzung von firmeninternen Ressourcen) oder wichtige Hinweise für die laufende Untersuchung liefern (z.B. wenn der Verdächtige sowohl für unsichere Webanwendungen als auch zur Sicherung seiner geheimen Daten das gleiche Passwort verwendet).

Zu den Ablagebereichen der Daten zählen insbesondere der Verlauf (History, besuchte Seiten), der Cache (temporäre Internetdateien) und die Cookies (kleine Dateien, welche Informationen über eine Session auf einer bestimmten Internetseite speichern). Aber auch gespeicherte Bookmarks oder die automatische Vervollständigung von Formular- und Anmeldedaten können Quellen zusätzlicher Informationen sein. In der Regel liegen diese Daten in den entsprechenden Verzeichnissen der Benutzer (z.B.: `\BENUTZERNAME\Lokale Einstellungen\Temporary Internet Files` unter Windows 2000) oder dem Programmverzeichnis der Anwendung.

Problematisch, im Sinne einer Ermittlung, ist das Angebot der Browser, diese Daten mit wenigen Mausklicks zu löschen (meist innerhalb des Menüs Einstellungen). Ausnahme hiervon ist der Internet Explorer, welcher zwar vordergründig alle Dateien löscht, im Hintergrund aber eine Datei Index.Dat führt, mit welcher der Zugriff auf lokal gespeicherte Webinhalte geregelt wird. Da diese Datei ständig vom Betriebssystem offen gehalten wird, ist es nur mit zusätzlichen Programmen möglich, diese zu löschen. In ihr werden Verweise auf alle besuchten Webseiten indiziert, welche innerhalb der Temporären Internetdateien abgelegt wurden. Mittels dieser Datei kann also auch im Nachhinein festgestellt werden, welche Seiten besucht wurden [Ind04], [Cur02]

Die zwischengespeicherten Daten liegen in der Regel im Klartext vor und es wäre somit möglich, diese auch manuell mit einem Editor auszuwerten. Aufgrund der Standardeinstellungen für den maximalen Speicherplatzbedarf dieser Daten, welcher je nach Browser und vorhandenen Ressourcen (physikalischer Speicher, Größe der Partition) im zwei- und niedrigem dreistelligen Bereich liegt, ist aber eine manuelle Auswertung zumindest am Anfang nicht sinnvoll. An dieser Stelle sollte das Analysewerkzeug ansetzen und die vorhandenen Daten durchsuchen und entsprechend für den Ermittler aufbereiten. Eine der aufbereiteten Informationen könnte zum Beispiel die Liste der besuchten Webseiten sein, welche neben dem Zeitpunkt des letzten Besuches auch die zugehörigen Seitenfragmente anzeigt, die sich noch im Cache befinden. Aber auch eine Liste der Server, von welchem sich noch Cookies auf dem Datenträger befinden, in Kombination mit den benutzten Sessions IDs, wäre denkbar. Hiermit könnte bei den entsprechenden Providern eventuell noch zusätzliche Informationen über den Verdächtigen angefordert werden, die dort noch vorgehalten werden.

Eine umfassende Bewertung dieses Kriteriums ist mit einigen Schwierigkeiten verbunden. Zum Einen liegt das an der Vielzahl unterschiedlicher Browserfamilien (Internet Explorer, Mozilla, Netscape, Opera, ...), welche zusätzlich in unterschiedlichen Versionen vorliegen. Da diese sich aber teilweise erheblich in der Datenhaltung unterscheiden, müsste jede diese Konstellationen einzeln überprüft werden, wobei hier die Vielzahl der unterschiedlichen Quellen (History, Cache, Cookies, ...) noch zusätzlich zu berücksichtigen sind. Zum Anderen müsste für den Test dieser Aufbereitung eine erhebliche Zeitspanne geopfert werden, da für eine realistische Umgebung für jede dieser Konstellationen zumindest einmal eine Internetnutzung über mehrere Tage hinweg simuliert werden müsste, um einen repräsentativen Datenbestand zu erhalten. Schließlich ist die Aufbereitung von Daten aber auch ein sehr qualitativer Vorgang. Ein Liste der besuchten Webseiten würde man zum Beispiel auch durch eine Mustersuche (z.B. nach `http://(\w+\.)+` siehe Kriterium 4.3.2 Seite 75) im entsprechenden Verzeichnis erhalten, entscheidend wären aber die zusätzlichen Informationen. Für diese Aufbereitung einen geeigneten Schlüssel zu finden und zusätzlich die oben angesprochenen Konstellationen zu berücksichtigen, würde aber dem Umfang eines eigenen Kriterienkatalogs entsprechen, was den Rahmen der vorliegenden Arbeit aber bei weitem sprengen würde. Im Sinne einer schnellen und einfachen Bewertung dieses Teilkriteriums ist es also nur entscheidend, ob für die Bereiche irgendeine Art der Datenaufbereitung zu Verfügung steht.

Anforderungen:

- Eine Analyse der Index.dat wird angeboten.
- Eine automatische Aufbereitung der Cookies wird angeboten.
- Eine automatische Aufbereitung der temporären Internet-Dateien wird angeboten.
- Eine automatische Aufbereitung der Browser History wird angeboten.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.5.2
E-Mail Anwendung

Kriterium	Gewicht
Analyse	
Internet Benutzung	
E-Mail Anwendungen	2

Die Verwendung von EMail ist die wichtigste und weit verbreitetste Form der elektronischen Kommunikation. Aus forensischer Sicht sind EMails dabei ein hervorragende Quelle von Informationen, weil sie neben dem eigentlichen Inhalt der Kommunikation weitere Daten, wie Absender, Empfänger und Zeitpunkt liefern. Sind also in einem Fall mehrere Personen involviert, welche Kontakt zu dem Besitzer des untersuchten digitalen Systems hielten, so wird die Analyse der EMail Kommunikation eine der ersten Stellen sein, an denen der Ermittler seine Nachforschungen beginnt.

Insbesondere die Verwendung einer lokalen EMail Anwendung, also quasi die Benutzung einer lokalen Mailbox, birgt hier ein Potential für Informationen, welches bei anderen Arten der Kommunikation nicht möglich ist. Zum Einen ist hier die oft sehr lange Vorhaltezeit und damit die Anzahl der gespeicherten EMails zu berücksichtigen. Diese ist bei der Verwendung von Webmail Systemen (siehe Kriterium 4.5.1) in der Regel nicht gegeben, da hier oft die Größe der Mailbox nur wenige Megabyte beträgt und teilweise die maximale Aufbewahrungszeit der EMails auf wenige Monate beschränkt ist. Durch die Verwendung einer lokalen Mailbox ist es also möglich, die Kommunikation über einen großen Zeitraum zu beobachten und zu analysieren. Neben der Möglichkeit somit auch ältere Daten, zum Beispiel über die Planung der aktuell untersuchten oder vorhergegangen Straftat, zu erhalten, kann die große Datenbasis aber zum Beispiel auch dazu verwendet werden, detaillierte Täterprofile zu erstellen, was mit Hilfe anderen Methoden (z.B. Mitschnitt eines Telefongesprächs) unter Umständen nicht in diesem Umfang möglich wäre. Zum Anderen kann aber auch der Umgang mit EMails innerhalb der Anwendung weitere Rückschlüsse liefern. Dokumente und wichtige Daten, welche sich im Anhang einer EMail befinden, werden in der Regel zur Weiterverarbeitung in einer dafür vorgesehenen Verzeichnisstruktur auf dem lokalen Datenträger abgespeichert und dann zusätzlich innerhalb der Mailbox einsortiert (z.B. unter dem Namen des entsprechenden Absenders). Dies hat für den Ermittler zwei Vorteile. Erstens kann so die Herkunft von bestimmten Daten sehr leicht festgestellt werden, wobei aber die einfache Fälschung einer Absenderadresse nicht zu vergessen ist. Zweitens können auf diese Weise eventuell noch Daten gefunden werden, welche auf dem Datenträger an ihrer vorgesehenen Position bereits gelöscht wurden, als EMail Anhang aber noch präsent sind. Zum Beispiel wenn ihr Vorhandensein aufgrund des Umfangs der Mailbox bereits vergessen wurde, oder wenn der Verdächtige bereits versucht hat, Beweise zu vernichten, dabei aber seine gesamte Mailbox vergessen hat oder zeitlich nicht mehr dazu gekommen ist.

Außer der EMail, sind aber auch weitere Funktionalitäten der EMail Anwendung zu nennen, welche zusätzliche Informationen liefern können. Sehr häufig ist es zum Beispiel möglich, im Adressbuch neben der EMail Adresse auch zusäztliche Kontaktinformationen wie Telefonnummer, Adresse oder persönliche Notizen abzulegen. Ein integrierter und genutzter Terminplaner könnte zum Beispiel Aufschlüsse über vergangene oder zukünftige Termine liefern, welche eventuell interessant für die laufende Ermittlung sind. Eine Untersuchung dieser Punkte ist aber nur mit einer vollständigen Analyse der EMail Anwendung möglich. Berücksichtigt man weiterhin die Vielzahl unterschiedlicher Anwendungen (z.B. Outlook Derivate unter Windows, Kmail oder pine unter Linux, Thunderbird als Systemübergreifende Lösung) würde sich der Bewertungsumfang noch weiter potenzieren. Für das aktuell Kriterium muss also wiederum ein Schema gefunden werden, welches eine einfache und schnelle Bewertung erlaubt. Die Bewertung beschränkt sich daher auf eine Auswahl der am häufigsten eingesetzten Mailbox Formate (Outlook, Outlook Express, mbox Format, ...) und auf die Möglichkeit deren Struktur darzustellen.

Anforderungen:

- Outlook Mailbox Format (.PST) wird unterstützt.
- Outlook Express Mailbox Format (.DBX) wird unterstützt.
- Mbox bzw. Mdir Format wird unterstützt.
- Mailbox der Mozilla Familie wird unterstützt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.5.3
MESSENGER

Kriterium	Gewicht
Analyse	
Internet Benutzung	
Messenger	1

Eine weitere Form der Kommunikation, welche über das Internet abgewickelt wird, ist die Verwendung von Instant Messengern. Ähnlich einem Adressbuch werden hierbei die Kontakte in einer so genannten Buddy-Liste geführt. Der große Vorteil gegenüber der asynchronen Kommunikation mit EMail besteht darin, dass in der Regel angezeigt wird, ob ein Kontakt aus der Buddy-Liste gerade „online ist“. Daraufhin kann sofort eine Unterhaltung entweder über das Senden von kurzen Nachrichten (Push-Verfahren) oder mit dem Öffnen eines Chats begonnen werden.

Wie bei anderen Arten der Kommunikation auch, ist für den Ermittler interessant, wer miteinander kommuniziert hat und welche Informationen dabei ausgetauscht wurden. Das Analysetool sollte daher in der Lage sein die Buddy-Liste und eventuell vorhandene Protokolle einer Kommunikation (Logdateien der geführten Chats und Liste der gesendeten Nachrichten) zu extrahieren und Datentechnisch aufzubereiten (z.B. Zusammenfassung jeglicher Kommunikation mit einem Kontakt).

Analog zu den bereits aufgeführten Kriterien existieren eine Vielzahl unterschiedlicher Instant Messenger. Diese unterscheiden sich zum Einen erheblich in ihrer Funktionalität und verwenden zusätzlich noch unterschiedliche, zum Teil proprietäre Protokolle für ihre Kommunikation untereinander. Es treten also wiederum die gleichen Überlegungen und

Schlussfolgerungen in Bezug auf die Bewertung eines Kriteriums auf, wie sie bereits bei den oben genannten Kriterien erfolgte. Entscheidend für die Bewertung der Analysefähigkeit von Instant Messengern ist also wiederum die Unterstützung der am häufigsten eingesetzten Anwendungen.

Anforderungen:

- AOL Instant Messenger (AIM) wird unterstützt.
- Microsoft Messenger (MSN) wird unterstützt.
- ICQ wird unterstützt.
- Jabber Implementierungen werden unterstützt.

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.5.4
PEER TO PEER NETZE

Kriterium	Gewicht
Analyse	
Internet Benutzung	
Peer to Peer Netze	X

Ein Peer to Peer (P2P) Netz ist ein Neztwerk, dessen Kommunikation nicht auf dedizierten Servern basiert (z.B. EMail), sondern in der Regel eine direkte Verbindung zwischen den einzelnen Teilnehmern (peers) verwendet. In einem reinem P2P Netz fungieren die einzelnen Teilnehmer also sowohl als „clients“, wenn sie auf die Daten von anderen Teilnehmern zugreifen, als auch als „server“, wenn sie anderen Teilnehmern ihre Daten zu Verfügung stellen.

P2P Netze haben sich in den letzten Jahren vor allem zum Austausch von größeren Datenmengen, wie Bildern, Musik und Filmen etabliert und weniger für die reine schriftliche Kommunikation, für die eher auf andere Mittel wie EMail oder IRC zurückgegriffen wird. Beim Datenaustausch sind dabei zwei verschiedene Methoden zu unterscheiden, welche mittels unterschiedlichen Protokollen implementiert werden. Bei der ersten Methode wird dabei eine Datei vollständig und in der Regel linear von einer einzigen Quelle empfangen. Diese Methode findet vor allem bei kleineren Datenmengen wie für Bilder und Musik Verwendung, welche bei heutigen Internetanbindungen in wenigen Sekunden oder Minuten übertragen sind. Bei der zweiten Methode wird eine große Datei (z.B. Filme oder Anwendungen) in mehrere logische Teile (chunks) zerlegt, welche von verschiedenen Quellen parallel bezogen werden können und erst auf dem Zielsystem zusammengesetzt werden.

Für den Ermittler sind in Bezug auf P2P Netze vor allem zwei Informationen interessant. Zum Einen ist das die Information, von welcher Quelle eine bestimmte Datei erhalten wurde. Zum Anderen, welchen Inhalt eine Datei trägt bzw. von welcher Art eine Datei ist, die noch nicht vollständig übertragen wurde. Sind die Daten erst einmal vollständig auf das System übertragen unterscheiden sie sich, bis auf den Aufenthaltsort eines eventuell dafür bestimmten „download“ Verzeichnisses, nicht mehr von anderen Dateien und können entsprechend dem vorliegenden Kriterien analysiert werden. Für beide Informationen ist dabei die erste Methode in der Regel ergiebiger, was auf die Implementierung der einzelnen Protokolle zurückzuführen ist.

Da bei der ersten Methode die Daten nur von einer Quelle stammen, werden deren Adressinformationen (z.B. Benutzername im jeweiligen P2P Netz und IP-Adresse) als Teil der Übertragunsinformationen gespeichert, um nach einem Verbindungsabbruch die Übertragung wieder fortzusetzen. Abhängig von den Einstellungen der Anwendung können diese Adressinformationen auch nach einer erfolgreichen Übertragung noch zu Verfügung stehen, wenn nicht explizit eine manuelle oder automatische Löschung vorgenommen wurde. Anhand dieser Informationen kann in sehr vielen Fällen die Quelle der Daten ermittelt werden, wodurch sich weitere Möglichkeiten der Nachforschung ergeben (z.B. der natürliche Aufenthaltsort einer Person oder Resource anhand von IP-Adresse und Verbindungsprotokoll des zugehörigen Providers). Weiterhin wird in den Übertragunsinformationen auch der Dateiname gespeichert, der Rückschlüsse auf den Datei-Inhalt liefern kann. Viel interessanter ist hier aber die lineare Übertragung der Daten. Ist die angeforderte Datei in einem linearen Format (z.B. Text oder Musik), so kann in vielen Fällen deren Inhalt bereits betrachtet und analysiert werden (z.B. Sichtung der ersten Seite eines Dokuments, oder Anhörung der ersten Minute eines Liedes), auch wenn die Datei noch nicht vollständig übertragen wurde.

Etwas anders verhält es sich bei der zweiten Methode, welche das parallele Beziehen von Teilen der Datei erlaubt. Hier wird nur ein Identifikator (z.B. Name und Prüfsumme) für die Datei und die Informationen der bereits erhaltenen Teile gespeichert. Bei einer erneuten Einbuchung in das P2P Netz werden dann anhand des Identifikators die aktuell verfügbaren Quellen ermittelt und fehlende Teile angefordert. Es liegen also keine Informationen über die Quellen oder zurückliegende Verbindungen vor, welche analysiert werden könnten. Ähnlich sieht es mit der Analyse des Datei-Inhalts aus, da dieser in der Regel nur lückenhaft vorliegt, wodurch die Interpretation der meisten Daten nicht möglich ist. Falls zu den bereits übertragen Teilen der Anfang der Datei gehört, kann natürlich auch hier die oben erwähnte Methode der Analyse vollzogen werden.

Ein weiteres Problem besteht darin, dass nicht feststellbar ist, welche P2P Anwendung am häufigsten genutzt werden. Zwar ist es möglich, an Internet Gateways das Volumenaufkommen der einzelnen Protokolle anhand der Ports festzustellen, daraus lassen sich aber (ohne genaue Analyse) keine sicheren Rückschlüsse auf die verwendeten Anwendungen folgern. Eine Reduzierung auf die unterstützten Protokolle ist nicht möglich, da diese nur die Datenkommunikation spezifizieren, nicht aber in welcher Form die zugehörigen Daten (z.B. bereits empfangene Teile) abzulegen sind. Eine repräsentative Auflistung von P2P Programmen ist somit nicht möglich. Ohne eine derartige Liste ist eine aussagekräftigen Bewertung aber nicht machbar.

Kriterium 4.6
METADATEN

Kriterium	Gewicht
Analyse	
Metadaten	
MAC-Zeiten	2
Applikationsabhängige Metadaten	X

Die Anzeige der MAC Attribute für eine Datei ist bereits durch das Kriterium 4.1.2 abgedeckt. Für die Gewichtung sind daher nur die zusätzlichen Möglichkeiten einer Auswertung zu Berücksichtigen. Daher wird die umfassende Analyse der *MAC-Zeiten* an dieser Stelle nur noch als wichtig eingestuft.

Bei der Untersuchung von *applikationsabhängigen Metadaten* zeigte sich, dass für deren Analyse kein allgemeines Vorgehen möglich ist und auch kein Konzept vorliegt (wie z.B. bei der Suche mittels regulären Ausdrücken), welches für eine Analyse angewandt werden könnte. Das Anlegen von Metadaten ist inhärent von der verwendeten Applikation abhängig und unterscheidet sich teilweise sogar von Version zu Version [Met03][Met04]. Ein Werkzeug müsste also für jedes zu Verfügung stehende Programm entsprechende Informationen vorhalten und einen Mechanismus bieten, diese zu extrahieren. Es ist daher keine sinnvolle Beurteilung gefunden und somit auch keine Gewichtung für dieses Kriterium vorgenommen worden.

Kriterium 4.6.1
MAC-ZEITEN

Kriterium	Gewicht
Analyse	
Metadaten	
MAC-Zeiten	2

Der Begriff MAC-Time ist ein Acronym für die Modification-, Access- und Change Zeitenpunkte einer Datei im Dateisystem[13]. Die Modification Zeit gibt den Zeitpunkt wieder, wann auf eine Datei das letzte Mal ein schreibender Zugriff erfolgte. Der Access Zeitpunkt repräsentiert den Zeitpunkt, an welchem die Datei das letzte Mal gelesen oder ausgeführt wurde. Der Change Zeitpunkt schließlich gibt an, zu welcher Zeit die Meta-Daten (z.B. Zugriffs- oder Eigentumsrechte) einer Datei das letzte Mal einer Veränderung unterlagen.

Mit der Analyse der MAC-Zeiten kann also ermittelt werden, welche Dateien in einer gewissen Zeitspanne, einem bestimmten Zugriff unterlagen. Dies kann zum Beispiel dazu verwendet werden, alle Dateien zu ermitteln, die während eines Tathergangs involviert waren, oder es kann festgestellt werden, auf welche Weise bzw. mit welcher Methode ein Tathergang erfolgte (timeline-analysis).

Da die MAC-Zeiten aber zum Einen sehr leicht veränderbar sind (einfaches lesen, schreiben oder kopieren) und immer nur den letzten Zeitpunkt einer Veränderung beinhalten, zum Anderen aber die Datei- und Betriebssysteme, bei gleichen Vorgängen, unterschiedliche Komponenten der MAC-Zeiten setzen, sind bei der Analyse der MAC-Zeiten noch folgenden zwei Punkte zu berücksichtigen.

Auf Grund des ersten Punktes ist es also entscheidend, welche Dateien untersucht werden und wie viele Aktionen zwischen dem untersuchten Zeitabschnitt und der Sicherstellung des Systemes ausgeführt wurden. Falls eine Sicherstellung relativ zeitnah zu einem untersuchten Tathergang erfolgt ist, und Dateien untersucht werden, welche nur während diesem Vorgang unmittelbar Verwendung finden und ansonsten weniger häufig genutzt werden, kann davon ausgegangen werden, dass die aktuellen MAC-Zeiten zu dem besagten Tathergang passen. Ist zum Beispiel ein nur wenige Stunden zurückliegender, unerlaubter Zugriff auf ein System oder einen Bereich entdeckt worden, der eine Sammlung von Dokumenten enthält, auf welche nur selten ein Zugriff erfolgt (z.B. Ablage älterer Firmendokumente), so ist eine Ermittlung der eingesehenen oder manipulierten Dokumente mit Hilfe der MAC-Time Analyse durchaus erfolgversprechend. Wurde hingegen vor der Sicherstellung am besagten System, und insbesondere im (Daten)Bereich des untersuchten Vorfalles, produktiv weitergearbeitet, sind die MAC-Zeiten mit Vorsicht zu betrachten. So ist zum Beispiel die Analyse der MAC-Zeiten von Dateien, welche mit dem Start eines Betriebssystem zusammenhängen, nach mehrmaligen Neustarten des Systems, nicht mehr sinnvoll.

Der zweite Punkt ist vor allem für die Interpretation der ermittelten MAC Zeiten zu beachten. So ändert sich zum Beispiel beim Umbenennen einer Datei unter Debian

[13]Da Verzeichnisse aus der Sicht des Dateisystems ebenfalls (spezielle) Dateien sind, werden auch für Verzeichnisse MAC-Zeiten verwaltet

Linux (ext2) keine der MAC-Zeiten, unter Windows 2000 (NTFS) wird hingegen beim Umbenennen der Access Zeitpunkt aktualisiert [Ges04]. Es ist also für den Ermittler notwendig, die Eigenheiten des Betriebssystems in Bezug auf das Setzen der MAC Zeiten in Erfahrung zu bringen und diese bei einer Interpretation zu berücksichtigen.

Da die einfache Anzeige der MAC-Zeiten für eine Datei bereits in Kriterium 4.1.2 behandelt wurde, ist bei der Beurteilung diese Kriteriums nur noch eine die Auswertung und Präsentation der MAC-Zeiten von mehreren Dateien zu beachten.

Anforderungen:

- Die MAC-Zeiten werden übersichtlich präsentiert (z.B. tabellarisch, graphisch)
- Es ist möglich, nur einen bestimmten Zeitrahmen zu betrachten.
- Es ist möglich, die Anzeige auf eine oder zwei der drei Attribute zu beschränken.
- Es ist möglich, direkt aus der Präsentation/Auswertung auf die entsprechenden Datei zuzugreifen (z.B. Verlinkung).

Erscheinungsformen:

A Alle Punkte werden erfüllt.

B Drei der genannten Punkte werden erfüllt.

C Zwei der genannten Punkte werden erfüllt.

D Nur einer der genannten Punkte wird erfüllt.

E Kein Punkt wird erfüllt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4
B	größtenteils erfüllt	3
C	im mittlerem Umfang erfüllt	2
D	kaum erfüllt	1
E	nicht erfüllt	0

Kriterium 4.6.2
Applikationsabhängige Metadaten

Kriterium	Gewicht
Analyse	
Metadaten	
Applikationsabhängige Metadaten	X

Applikationen können Metatdaten über die ihnen zugeordneten Dateien an unterschiedlichster Stelle ablegen. Einerseits kann dies direkt in den Dateien erfolgen (z.B. Autor des Dokuments). Andererseits in dem Verzeichnis, in welcher sich die Datei befindet (z.B. thumbnails), also immer noch nah an den eigentlichen Dateien. Schließlich bleibt noch die Möglichkeit, Metadaten an anderer Stelle abzulegen, also fern von den eigentlichen Dateien. Zum Beispiel innerhalb des Verzeichnisses, in welches die Applikation installiert wurde, oder in einem speziellen Verzeichnis, welches für diese Metadaten vorgesehen ist (z.B. der Verlaufs Ordner unter Windows, in welchem der Zugriff auf die zuletzt geöffneten Dokumente gespeichert wird).

Das Anlegen von Metadaten kann bei der Erstellung bzw. Bearbeitung einer Datei entweder automatisch oder manuell erfolgen. Automatisch erstellte Metadaten können sich dabei auf Informationen aus dem System beziehen, zum Beispiel wenn der angemeldete Benutzer automatisch als Autor eingetragen wird, oder direkt von der Applikation stammen, wie zum Beispiel das Eintragen der Registrierungsnummer, welche eine Zuordnung zwischen Dokument und erstellender Applikation möglich macht. Weiterhin könnte aber auch das Anlegen eines kleinen Puffers denkbar sein, welches auch im nachhinein ermöglicht, bestimmte Änderungen rückgängig zu machen. Zu den manuell erzeugten Metadaten gehören zum Beispiel hinzugefügte Notizen oder Kommentare, welche beim einfachen Betrachten oder Ausdrucken eines Dokuments nicht erscheinen, sondern nur lesbar sind, wenn man sie explizit anzeigen lässt.

Metadaten können also für den Ermittler eine Quelle vielfältiger Informationen sein, da sie in der Regel unabhängig vom Datei-Inhalt angelegt und auf Grund fehlenden Fachwissens nur selten manipuliert werden. Genau dieses fehlenden Wissen um die Metadaten, welches man sich bei der schieren Anzahl von unterschiedlichen Anwendungen auch kaum aneignen kann, wäre aber ein Ansatzpunkt für die Bewertung des Analysewerkzeugs. Das Werkzeug sollte also in der Lage sein, zu jeder gegebenen Datei, alle Metadaten bereitzustellen, die in irgendeiner Form vorliegen. Für eine sinnvolle Bewertung müsste also zunächst festgestellt werden, welche Anwendungen überhaupt in Betracht für so eine Analyse kommen. Allein die quantitative Anzahl an unterschiedlichen Applikationen würde hieraus aber eine umfangreiche Untersuchung machen. Anschließend müsste für jede Anwendung ein eigenes Kriterium aufgestellt werden, welches die Ergiebigkeit der Metadatenanalyse bewertet, da eine einfache Aussage wie „Metadaten der Applikation XY können ermittelt werden“ nur sehr wenig Aussagekraft beinhalten würde.

4.5 Nicht aufgenommene Kriterien

Während der Sammlung von Kriterien wurden auch einige gefunden, welche später keinen Einzug in den Kriterienkatalog hielten. Teilweise wurden sie im Kriterienkatalog erwähnt (Kriterium 4.5.4 und Kriterium 4.6.2), da sie einen gewissen Themenbezug aufwiesen. Andere wurden gänzlich herausgenommen und sollen hier kurz beschrieben werden.

4.5.1 Betriebswirtschaftliche Kriterien

Wie bei jeder Anschaffung von Software, sind auch bei der Computerforensik die wirtschaftlichen Auswirkungen zu beachten. Diese sind zwar, im Vergleich zum Schaden, welcher bei einer Aktion entsteht, die zu einer forensischen Untersuchung führt, meist eher gering. Dennoch werden auch für die Bereitstellung einer forensische Untersuchungsumgebung nur begrenzte Ressourcen zu Verfügung stehen, welche in der Bewertung der Software berücksichtigt werden müssen.

Für eine Bewertung der Anschaffungskosten des Werkzeugs sollte nicht sein absoluter Preis entscheidend sein, welcher durchaus mehrere tausend Euro für eine Einzelplatzlizenz betragen kann (z.B. EnCase), sondern sein Anteil am zur Verfügung stehenden Etat. Hierdurch wird sichergestellt, dass dieser Kriterienpunkt für die unterschiedlichsten Anwender des Kriterienkatalogs vergleichbar bleibt, da einem Konzern oder einer Behörde sicherlich ein ganz anderer Etat zu Verfügung steht, als einer Privatperson oder einem kleinem Unternehmen. Desweiteren wären hier die laufende Kosten eines Werkzeugs zu nennen, zum Beispiel für Schulungen oder Software-Updates (Total Cost of Ownership (TCO)).

4.5.2 Juristische Kriterien

Die juristischen Aspekte wurden während der Erstellung des Katalogs fast gar nicht beachtet. Da der Anstoß einer forensischen Untersuchung in der Regel durch eine Straftat erfolgt, sind diese natürlich zu beachten, wenn eine Verwertung der Beweise vor Gericht angestrebt wird. Hier wäre zum Beispiel die Akzeptanz der Analyseprotokolle vor Gericht zu nennen, oder ob der der Einsatz des Werkzeugs allgemein anerkannt wird.

5 Andwendung des Kriterienkatalogs

Dieses Kapitel beschreibt die Anwendung des Kriterienkalogs an den drei Werkzeugen *EnCase Forensic Edition, The Sleuth Kit* und *ILook Investigator*. Es erfolgt zunächst eine Beschreibung der Werkzeuge, um ein wenig mehr über die Hintergründe und Intentionen dieser Programme zu erfahren. Anschließend folgt eine Erläuterung, wie bei der Beurteilung der Kriterien vorgegangen wurde und welches Vorgehen sich für weitere Beurteilungen anbietet. Abgeschlossen wird das Kapitel mit der Anwendung des Kriteriumkatalogs und einer Diskussion der Ergebnisse.

5.1 Beschreibung der Werkzeuge

Die Beschreibung der Werkzeuge liefert Informationen über die Herkunft, den Aufbau und die Intention der Programme. Dies soll die Einordnung in das weite Gebiet der Computerforensik ermöglichen, da diese Informationen Gründe aufzeigen, welche sich unmittelbar auf den Funktionsumfang, und somit auf die Bewertung des Werkzeugs auswirken.

5.1.1 EnCase Forensic Edition

Die Firma Guidance Software bietet mit dem Produkt *EnCase Forensic Edition* (EnCase) [Sof04a] ein umfassendes Werkzeug für die computerforensische Untersuchung an. Es läuft unter den aktuellen Windows Betriebssystem und bietet einen enormen Funktionsumfang, welcher mittels einer GUI zu Verfügung gestellt wird. Neben der Analyse von Bitstream-Images bietet es die Möglichkeit die entsprechenden Funktionen auch am laufenden System anzuwenden. Des Weiteren besteht die Option, Bitstream-Images anzulegen und Festplatten aus Raid Systemen zu analysieren. Zum Zeitpunkt der Testphase war die aktuelle Version 4 für ca. 2500.- € käuflich zu erwerben.

EnCase ist laut Guidance Software das am häufigsten verwendete Produkt im Bereich der Computerforensik. Dies ist auch sehr deutlich an dem Vergleich der zu Verfügung stehenden Quellen im Internet zu sehen [goo04]. Für die Anwendung des Kriterienkatalogs ist dies insofern von Vorteil, dass sehr viele Informationen aus unterschiedlichen und unabhängigen Quellen bereitstehen, welche für die Bewertung eventuell herangezogen werden können.

Die Intention von EnCase besteht darin, dem Anwender ein Werkzeug in die Hand zu geben, mit welchem die komplette Untersuchung eines Falles ermöglicht wird. Dies hat zur Folge, dass die angebotenen Funktionen nahezu den gesamten Themenbereich des Kriterienkatalogs abdecken.

5.1.2 The Sleuth Kit / Autopsy Forensic Browser

The Sleuth Kit (TSK) [Car04a]wurde von Brian Carrier entwickelt und besteht aus einer Sammlung von Kommandozeilentools (im folgenden nur noch Tools genannt), welche open source zu Verfügung gestellt werden. Ein Teil der Tools wurde hierbei aus dem *The Coroners Toolkit* [FV04] übernommen. Es läuft zuverlässig unter Linux, MacOS X, Open- & FreeBSD, Solaris und mit Hilfe der CYGWIN Umgebung [Cyg04] auch unter Windows.

Die Tools des TSK sind vor allem auf die grundlegenden Analyse von Daten ausgelegt und hier insbesondere auf die vollständige Bereitstellung der Daten eines Bitstream-Images. Hierfür werden knappe 20 Tools zu Verfügung gestellt, die jeweils eine sehr spezielle Aufgabe übernehmen. Teilweise werden deshalb auch Funktionen des zugrunde liegenden Systems verwendet (z.B. `grep`, `find`). Die weitere Interpretation der Daten bzw. Dateien erfolgt daher eher rudimentär. Andere Aufgaben einer forensischen Untersuchung (z.B. anlegen von Bitstream-Images, Protokollierung) werden völlig außen vor gelassen. Ein großer Vorteil des TSK besteht darin, dass es auf vielen Betriebssystemen läuft (siehe Bewertung) und als open source Software vertrieben wird [Car02]. Somit ist die Möglichkeit gegeben, eigenständig Erweiterungen oder Änderungen durchzuführen.

Da sich das Einsatzgebiet des TSK sehr auf die grundlegende Analyse der Daten bezieht und der Einsatz der Tools durch ihre starke Spezialisierung teilweise sehr kompliziert ist[1], wurde von Brian Carrier der *Autopsy Forensic Browser* (Autopsy) entwickelt. Dieser stellt einen Webserver zu Verfügung, der mittels eines Browser eine graphische Oberfläche für den Zugriff auf das TSK bietet. Des Weiteren wurden zusätzliche Funktionalitäten eingebaut, welche den Ermittler bei einer forensischen Untersuchung unterstützen (z.B. Projektverwaltung, Protokollierung, einfacher Datenzugriff).

5.1.3 ILook Investigator

ILook Investigator (ILook) [Ilo04] wurde ursprünglich von Elliot Spencer entwickelt, der es mittlerweile an den Internal Revenue Service der USA abgegeben hat. ILook läuft ebenfalls auf den neueren Windows Betriebssystemen und erhebt den gleichen Anspruch wie EnCase: ein Werkzeug für eine umfassende forensische Untersuchung. Dementsprechend ähnelt es EnCase im Funktionsumfang und der Bedienung.

Problematisch ist hingegen die Verfügbarkeit des Programms. Zwar ist es kostenlos erhältlich, das aber nur für Personen im Bereich der Computerforensik, welche zusätzlich noch bei einer der folgenden Institutionen beschäftigt sind:

- Strafverfolgungsbehörde
- Staatlicher Geheimdienst

[1] In der Regel stellen die einzelnen Tools nur die Daten zu Verfügung, für ihre Durchsuchung sind dann zusätzliche Funktionsaufrufe, zum Beispiel von `grep`, notwendig. Des Weiteren erfolgt die Steuerung der Tools mittels Kommandozeilenparameter, von denen meist mehr als 10 zu Verfügung stehen. Für eine Analyse, wie sie einem Kriterium im Katalog entspricht, ist daher in der Regel ein umfangreicher Befehl notwendig, welcher den Aufruf mehrere Tools beinhaltet.

- Militär (im Bereich Kriminalität oder Spionageabwehr)
- Staatliche oder regulierende Behörde im Bereich der Strafverfolgung

Insbesondere wird die Ausgabe an Forschungseinrichtungen explizit untersagt. Dies sind natürlich sehr starke Einschränkungen die eine weite Verbreitung des Programms verhindern. Ähnlich sieht es auch mit Informationen über dieses Programm aus. Es existiert keine offizielle öffentliche Diskussionsmöglichkeit, auf ein internes Message-Board ist der Zugriff nur mit Anmeldung möglich, die den gleichen Auflagen wie denen des Programmes entsprechen.

Ein Bewertung dieses Werkzeugs hätte also nur innerhalb des Landeskriminalamt Bayerns stattfinden können. Dort wird das Werkzeug aktuell aber nicht eingesetzt, es konnte also auch nicht auf etwaige Erfahrung im Umgang mit diesen Werkzeug gesetzt werden. Des Weiteren ist das Werkzeug durch die strenge Vergabepolitik nur für einen sehr begrenzten Teilnehmerkreis verfügbar. Dementsprechend mager sieht es auch mit Informationen aus, die über das Werkzeug zu Verfügung stehen. Aus diesem Grund wurde eine Bewertung von ILook nicht durchgeführt.

5.2 Beurteilung der Kriterien

Während der gesamten Zeit der Erstellung des Kriterienkatalogs wurde mit den Werkzeugen EnCase (Version 4.2x) und TSK/Autopsy (Version 1.7x bzw. 2.0x) gearbeitet[2]. Dabei wurden immer wieder die ausgearbeiteten Kriterien mittels der Werkzeuge getestet und angepasst. Die abschließende Anwendung des Kriterienkatalogs auf die Werkzeuge erfolgte also nicht mit der gleichen Grundlage, wie es eine der Intentionen für die Anwendung des Katalogs vorgibt. Nämlich die effektive Bewertung von Werkzeugen ohne eine lange Einarbeitung in diese. Dennoch wurden bei der Beurteilung einige Schlussfolgerungen gezogen, welche auch für diese ursprüngliche Situation anwendbar sind.

Für die Bewertung eines Kriteriums sind Informationen aus unterschiedlichen Quellen zu verwenden, um differenzierte Aussagen zu bekommen, so dass eine allgemeine Beurteilung der Fähigkeiten des Werkzeugs möglich ist. Insbesondere sollte man sich nicht allein auf das Material verlassen, welches vom Hersteller zu Verfügung gestellt wird (z.B. das Handbuch oder eine ausführliche Produktbeschreibung). Diese bieten zwar einen guten Überblick der Funktionen und sind eine hervorragende Quelle für Informationen zu den einzelnen Kriterien, oftmals werden hier aber nur die positiven Seiten eines Werkzeugs genannt. Kleinere Fehler, Ungereimtheiten im Programmablauf oder die unvollständige Unterstützung einer Funktion werden hier gerne verschwiegen. Dennoch sollten sie als erste Anlaufstelle für die Beurteilung verwendet werden, da sie einen ersten und umfassenden Eindruck des Werkzeugs bieten.

Neben dieser Dokumentation des Werkzeugs ist insbesondere der vorliegende Kriterienkatalog an sich als Quelle für Informationen geeignet. Die Beschreibung der Kriterien

[2]Die Änderungen in der zweiten Nachkommastelle sind dabei zu vernachlässigen, da hier in der Regel nur Fehler behoben wurden. Auf die grundsätzliche Arbeitsweise der Werkzeuge hatten sie aber keinen Einfluss.

bietet einen Querschnitt der Leistungen, welche das Werkzeug erbringen soll. Diese können dann zu einem Vergleich herangezogen werden.

Einen enormen Informationsgewinn über das Werkzeug erhält man natürlich durch seine Anwendung. Hierbei kann man alle Funktionen testen und auf ihre Ergiebigkeit hin überprüfen. Hierbei sind zwei Vorgehensweisen denkbar. Einerseits kann einfach ein Bitstream-Image der eigenen Partition erstellt werden, auf welchem die einzelnen Funktionen getestet werden. Hier zeigt sich vor allem eine eventuell vorhandene Möglichkeit des Werkzeugs als hilfreich, die Analysefunktionen auch auf die Datenträger des laufenden Systems anzuwenden. Dadurch ist es nicht notwendig extra ein Bitstream-Image bereit zu halten. Die zweite Möglichkeit besteht darin, im Internet zur Verfügung gestellte Bitstream-Images zu verwenden [CFT04], [Car04a], [Hon04]. Diese beinhalten bestimmte Daten oder Konstellationen, welche bei einer Untersuchung auftreten können. Somit kann der Einsatz und die Leistungsfähigkeit der Funktionen an realen Situationen festgestellt werden, da die entsprechenden Konstellationen ausreichend dokumentiert sind.

Die effektivste Art einer Beurteilung ist aber in Zusammenarbeit mit einer Person möglich, welche das Werkzeug schon länger einsetzt (wie es auch bei der vorliegenden Arbeit erfolgte). Besteht diese Möglichkeit in irgendeiner Form, sollte sie auf jeden Fall eingesetzt werden, da die bereits gewonnene Erfahrung im Umgang mit dem Werkzeug, in keiner Weise durch andere Methoden ersetzt werden kann. In diesem Fall reduziert sich eine Beurteilung in der Regel auf ein Frage, und Antwortspiel. Das aktuelle Kriterium und die Anforderungen werden einfach genannt. Dies sind für den erfahrenden Anwender in der Regel genug Informationen, um eine sofortige Beurteilung durchzuführen.

Schließlich ist das Internet noch als Quelle für Informationen verwendbar. Hier zeichnen sich besonders die öffentlichen Diskussionsrunden der untersuchten Werkzeuge (z.B. des Supports) als gute Quellen aus. Dort werden in der Regel die Probleme beim Umgang mit dem Werkzeuge diskutiert, die oftmals auch die Themenbereiche der Kriterien behandeln und so eine weitere Grundlage für die Bewertung liefern. Hier ist es sinnvoll, gezielt nach Informationen zu einem bestimmten Kriterium bzw. einer bestimmten Anforderung aus dem Kriterium zu suchen. Eine allgemeine Suche liefert hier meist keine guten Resultate in Bezug auf das Kriterium, sondern eher Hintergrundinformationen zu den einzelnen Gebieten.

Mit einer Bemerkung zu diesen Hintergrundinformationen und dem damit verbunden Hintergrundwissen soll dieser Abschnitt beendet werden. Es hat sich an der eigenen Erfahrung gezeigt, dass die Bewertung der Kriterien umso leichter und differenzierter ausfällt, je mehr Wissen in Bezug auf die Computerforensik allgemein, und die Analyse von Bitstream-Images im besonderen, vorhanden ist. Das Lesen des Kriterienkatalogs alleine dürfte daher nicht ausreichen, um eine aussagekräftige Bewertung eines Werkzeugs durchzuführen. Hier sei auf die vorhandene Literatur verwiesen, die einen umfangreichen Überblick der Computerforensik liefert (z.B. [Ges04]).

5.3 Anwendung des Kriterienkatalogs

Die Anwendung des Kriterienkatalogs auf die Werkzeuge erfolgt in Anlehnung an die Beurteilung der einzelnen Kriterien. Dabei wurden alle beschriebenen Quellen von Information verwendet. Insbesondere wurde aber auf die Erfahrung der Mitarbeiter des Landeskriminalamt Bayerns gesetzt.

Bei EnCase war dies Herr Köllner, der auch während der gesamten Erstellungsphase der Diplomarbeit als Berater tätig war. Die Befragung erfolgte hier sehr ausführlich, indem in den meisten Fällen die entsprechenden Funktionalitäten am laufenden System nachgestellt und überprüft wurden. Für die Bewertung des Sleuth Kit/Autopsy erfolgte eine Befragung von Herr Mauersberger, der aber nur die Tools des TSK verwendet. Für die Beurteilung von Autopsy musste also auf die anderen Quellen zurückgegriffen werden.

Bei der Befragung der Mitarbeiter zeigten sich auch sehr deutlich die Vorteile dieser Methode. Zieht man die umfassenden Vorarbeiten mit den Werkzeugen ab und betrachtet nur die reine Zeit für die abschließende Anwendung, so ist hier eine deutliche Zeitersparnis festzustellen. Die Anwendung des Katalogs konnte mit Hilfe der Befragung in nur wenigen Stunden erfolgen und musste nur an einzelnen Stellen ergänzt werden. Die Bewertung von Autopsy hingegen erforderte ein Vielfaches dieser Zeit.

Bei der Anwendung des Kriterienkatalogs ist es ratsam, mit den Analyse-Kriterien zu beginnen. Diese sind sehr genau spezifiziert und beinhalten eine sehr konkrete Aufgabenstellung. Nebenbei wird man mit dem Umgang des Werkzeugs vertraut, so dass die anschließende Bewertung der allgemeinen Kriterien um einiges leichter ausfällt. Des Weiteren sollte die Reihenfolge bei der Bewertung der Kriterien eingehalten werden. Einerseits bauen die Beschreibungen der Kriterien aufeinander auf, andererseits wird diese Reihenfolge in den meisten Funktionsbeschreibungen verwendet, so dass man für einen ersten Überblick einfach dieser folgen kann.

Es folgt die Anwendung des Kriterienkatalogs auf die einzelnen Werkzeuge, wobei die Versionen Encase 4.2x, TSK 1.7x bzw. Autopsy 2.0x untersucht wurden. Die Bewertung erfolgte dabei nach bestem Wissen und Gewissen. Eventuell Fehler bei der Auswertung und dem Berechnungsverfahren sind zu entschuldigen.

5.3.1 EnCase Forensic Edition

WurzelkriteriumKriterium

Kriterium	Gewicht	Bewertung
Werkzeug der Computerforensik		**3,2067**
Anwender Support	2	3,6
Bedienung des Werkzeugs	3	2,2208
Protokollierung	2	4
Analyse	4	3,3475

Kriterium 1 -ANWENDER SUPPORT (Seite 37)

Kriterium	Gewicht	Bewertung
Anwender Support		**3,6**
Dienstzugang	2	3
Reaktionsverhalten	3	4

Kriterium 1.1 -DIENSTZUGANG (Seite 37)
Der Kontakt zu Guidance Software und somit die Nutzung des Supports im Bezug auf EnCase kann über EMail oder eine hotline (normale Verbindungsgebühren) erfolgen. Des Weiteren wird ein öffentliches Message Board betrieben, für welches Mitarbeiter zur Betreuung der Anfragen eingestellt sind. Laut Internetpräsenz wird kein Servicevertrag in Bezug auf den Support von EnCase angeboten.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 1.2 -REAKTIONSVERHALTEN (Seite 38)
In den meisten Fällen wird auf eine Supportanfrage im Forum innerhalb von 24 Stunden eingegangen und eine Lösung angestrebt. Bei kritischen Fällen wird teilweise auch die telefonische Kontaktaufnahme seitens Guidance Software initiiert.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 2 -Bedienung des Werkzeugs (Seite 40)

Kriterium	Gewicht	Bewertung
Bedienung des Werkzeugs		**2,2208**
Robustheit	3	0
Dokumentation	4	2,8571
Automatisierung	3	3
Projektverwaltung	1	4

Kriterium 2.1 -Robustheit (Seite 41)
Das Programm verhält sich in einigen Fällen nicht robust. So kann sich das Programm zum Beispiel unvermittelt beenden, wenn es versucht mit dem internen Bildbetrachter Bilder darzustellen, deren Code fehlerhaft ist. Bilder mit fehlerhaftem Code können zum Beispiel bei der Datenwiederherstellung aus nicht zugeordneten Bereichen entstehen, welche fragmentiert sind (siehe 4.2.1 Seite 61). Ist hier eine Datei rekonstruiert worden, deren Dateisignatur auf ein Bild schließen lässt, so versucht EnCase die Daten nach der Signatur als Bild zu interpretieren. Trifft der Bildinterpreter dann auf ein Dateisegment, welches zum Beispiel durch Fragmentierung nicht zum ursprünglichen Bild gehört hat, kann der Fall eintreten, dass sich EnCase ohne weitere Vorwarnung beendet.

Ähnlich verhält es sich, wenn zu viele Untersuchungsaktionen gleichzeitig gestartet werden oder ein Untersuchung zu umfangreich wird. Mit „zu umfangreich“ ist hier gemeint, dass über einen gewissen Zeitraum diverse Analysemethoden auf das Image angewendet werden. Mit der Zeit reagiert hier EnCase immer zäher auf Benutzereingaben, bis es schließlich mit einer Prozesslast von 100% „einfriert“ und nicht mehr reagiert. Guidance Software gibt hier, abhängig vom Vorgang, der gerade ausgeführt wurde, an, dass EnCase noch arbeitet und die Beendigung dieser Arbeit abwarten soll. Eigene Erfahrungsberichte zeigen aber, dass hier auch längeres Abwarten (einige Stunden bei einem kleinen Image) nicht zum Erfolg führt. EnCase ist dann nur noch mittels dem Task-Manager zu beenden.

Allgemein entsteht hier kein zwischenzeitlich stabiler Zustand, welcher auf eine ungültige Aktion aufmerksam macht bzw. diese abfängt und die Gelegenheit bietet, evtl. schon erhaltene Ergebnisse zu sichern. Zwar wird der aktuelle Stand der Untersuchung periodisch in eine „Case“ Datei abgelegt, die es ermöglichen soll, nach einem unbeabsichtigten Ende des Programms an diese Stelle zurückzukehren, aber in vielen Fällen funktionierte dies nicht besonders gut, da die letzte Sicherung oft zu einem Zeitpunkt erfolgte, als kein vernünftiges Arbeiten mehr notwendig war.

Maßstab

Ausprägung	Kriterium wird	Punkte
D	nicht erfüllt	0

Kriterium 2.2 -DOKUMENTATION (Seite 43)

Kriterium	Gewicht	Bewertung
Bedienung des Werkzeugs		
Dokumentation		**2,8571**
Funktionsbeschreibung	4	4
Tutorials	1	4
Online Hilfe	2	0

Kriterium 2.2.1 -FUNKTIONSBESCHREIBUNG (Seite 44)
Dem Produkt liegt ein gedrucktes Handbuch bei, welches über das Internet auch in elektronischer Form vorliegt. Alle Funktionen werden beschrieben und teilweise als Schritt-für-Schritt-Vorgang unter Zuhilfenahme von screenshots verdeutlicht. Die Ergebnisse der einzelnen Funktionen werden ebenfalls beschrieben.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 2.2.2 -TUTORIALS (Seite 46)
Bereits das Handbuch ist als eine Art Tutorial aufgebaut, wenn es sequentiell gelesen wird. Wie bereits im vorherigen Kriterium angedeutet, werden die einzelnen Funktionen anhand von Schritt-für-Schritt-Vorgängen erklärt, welche als Minitutorials angesehen werden können. Die einzelnen Kapitel des Handbuches sind in ihrer Abfolge so gewählt, dass sie in etwa den Vorgang einer forensischen Untersuchung widerspiegeln und immer tiefer in die Materie einsteigen. Des Weiteren stehen auf der Webseite „online support videos" zu Verfügung, welche die wichtigsten Funktionsweisen des Programms anhand eines kleinen Videos vorführen. Auch die regelmäßig veröffentlichten „webinars" (längere Filme, die verschiedene Themen in Bezug auf Computerforensik behandeln) können teilweise als Tutorials aufgefasst werden, wenn sie sich mit speziellen Funktionsweisen des EnCase Produkts auseinandersetzen.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 2.2.3 -ONLINE HILFE (Seite 47)
Eine Online Hilfe ist in der aktuellen Version nicht implementiert.

Maßstab

Ausprägung	Kriterium wird	Punkte
E	nicht erfüllt	0

Kriterium 2.3 -AUTOMATISIERUNG (Seite 49)
EnCase stellt mittels EnScript eine Programmiersprache (angelehnt an C++) und API (Application Program Interface) zu Verfügung, mit welcher der komplette Funktionsumfang von EnCase angesteuert werden kann. Auf der Webseite steht für die Automatisierung häufig verwendeter Vorgänge bereits eine Bibliothek von EnScript Programmen zu Verfügung. Die Ergebnisse einer Analyse bleiben während den Analyseschritten bestehen; es ist also ohne weiteres möglich, auf diesen Daten weiterzuarbeiten. Eine Makrofunktion wird nicht angeboten.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 2.4 -PROJEKTVERWALTUNG (Seite 50)
In EnCase wird die Untersuchung eines Vorfalls mit „case“ bezeichnet. Jeder case enthält alle vorliegenden untersuchungrelevanten Informationen und kann aus mehreren Datenträger Images bestehen. Innerhalb einer übersichtlichen Baumstruktur können mehrere cases gleichzeitig geöffnet und verwaltet werden, dabei ist eine case übergreifende Analyse möglich. Das Ablegen von Notizen (Bookmarks) ist jederzeit möglich. Die Verwaltung der Daten wird vollständig von EnCase übernommen.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 3 -PROTOKOLLIERUNG DER UNTERSUCHUNG (Seite 52)
Es erfolgt keine automatische Protokollierung der einzelnen Schritte der Untersuchung oder der Ergebnisse. Die Ergebnisse einzelner Analyseschritte können per Knopfdruck als Bookmark gespeichert werden. Die Bookmarkfunktion ist eine Art Notizblock, in welchem neben den Ergebnissen auch eigene Notizen oder Datenfragmente, wie Textblöcke oder Bilder, abgelegt werden können. Bei der Ablage als Bookmark werden automatisch der Zeitpunkt der Ablage, und falls vorhanden, weitere Informationen wie Dateiattribute oder physikalischer Position im Image mit aufgenommen.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4 -ANALYSE (Seite 54)

Kriterium	Gewicht	Bewertung
Datenanalyse		**3,3475**
Rohdaten Analyse	4	3,8
Daten Extraktion und Wiederherstellung	4	4
Suchverfahren	3	2,125
Prüfsummen	3	3
Internetnutzung	1	2,3333
Metadaten	2	4

Kriterium 4.1 -ROHDATEN ANALYSE (Seite 56)

Kriterium	Gewicht	Bewertung
Analyse		
Rohdaten Analyse		**3,8**
Image Erkennung	1	3
Dateisystem Unterstützung	4	4

Kriterium 4.1.1 -IMAGE ERKENNUNG (Seite 56)
Neben einem eigenen Image-Format werden Raw- und dd-Images unterstützt.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.1.2 -DATEISYSTEM UNTERSTÜTZUNG (Seite 58)
Folgende Dateisystem können laut Produktbeschreibung interpretiert werden: FAT12 (Floppy), FAT16, FAT32, NTFS, HFS, HFS+, UFS, Sun Solaris, EXT2, Reiser, Palm, CDFS, Joliet, UDF and ISO 9660. Zumindest bei ReiserFS ist bekannt, dass es Probleme mit dem Anzeigen der Dateinamen aufweist. Weiter Lücken sind nicht bekannt bzw. wurden nicht ermittelt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2 -Daten Extraktion und Wiederherstellung (Seite 60)

Kriterium	Gewicht	Bewertung
Analyse		
Daten Extraktion und Wiederherstellung		**4**
Gelöschte Daten	4	4
Unzugeordnete Bereiche	4	4
Slack Bereiche	4	4
Auslagerungsdateien und Swap-Partitionen	2	4
Verschlüsselte und komprimierte Daten	2	4
Alternate Data Streams	1	4

Kriterium 4.2.1 -Gelöschte Daten (Seite 61)
Beim Anlegen des Falls wird automatisch versucht, alle gelöschten Dateien und Verzeichnisse zu rekonstruieren. Diese werden in einem gesonderten Bereich der Case Ansicht dargestellt und stehen allen Analysemethoden zu Verfügung. Diese Funktion steht für alle unterstützten Dateisysteme zu Verfügung.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2.2 -Nicht zugeordnete Bereiche (Seite 63)
Die nicht zugeordneten Bereiche werden ähnlich den gelöschten Daten, bei der Erstellung des Falls automatisch ermittelt und in einer zusammenhängenden Einheit in der Fall Ansicht repräsentiert. Der Bereich steht also für die restlichen Analysemethoden zu Verfügung. Es existieren diverse EnScripts (z.B. file finder, jpg finder, Photoshop PSD Extractor, ...), um in diesen Bereich spezielle Untersuchungen anzustellen.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2.3 -Slack Bereiche (Seite 64)
Beim Betrachten der einzelnen Dateien, wird der Slack Bereich graphisch hervorgehoben und angezeigt. Die Unterscheidung RAM und File Slack bleibt dabei dem Ermittler überlassen. Eine Analyse der MFT ist ebenfalls möglich.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2.4 -Auslagerungsdateien und Swap-Partitionen (Seite 66)
Linux/Unix Swap-Partitionen und die diversen Windows Auslagerungsdateien, werden in der Case Ansicht als normale Ressourcen bereitgestellt und stehen somit den allgemeinen Analysemethoden zu Verfügung. Die bei der Untersuchung von unzugeordneten Bereichen eingesetzten EnScripts können auch hier angewandt werden.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2.5 -Verschlüsselte und komprimierte Daten (Seite 68)
Vom Windows NTFS Dateisystem komprimierte Bereiche werden automatisch erkannt, dekomprimiert und den anderen Analysemethoden zu Verfügung gestellt. Hier besteht in der Case Ansicht kein Unterschied zwischen einfachen und komprimierten Dateien. Dateien im (G)ZIP und TAR Format „View File Structure" werden dekomprimiert und stehen dann in der Case Ansicht als als normale Daten zu Verfügung. Mittels eines EnScripts kann dieser Vorgang der Dekomprimierung für alle Dateien des untersuchten Falls automatisiert werden. Dies ist aber mit Vorsicht zu genießen, da sie zum Einen den Fall um einiges aufblähen und unübersichtlich in der Darstellung machen, zum Anderen eventuell Instabilitäten auftreten können (siehe Kriterium 2.1 oben).

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2.6 -Alternate Data Streams (Seite 69)
Alternate Data Streams werden von EnCase erkannt und in der Case Ansicht neben der zugehörigen Ressource angezeigt und entsprechend gekennzeichnet (`Dateiname • Streamname`). Dementsprechend stehen sie für die restlichen Analysemethoden uneingeschränkt zu Verfügung.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.3 -Suchverfahren (Seite 71)

Kriterium	Gewicht	Bewertung
Analyse		
Suchverfahren		**2,125**
Index Erstellung	2	0
Reguläre Ausdrücke	3	4
Phonetische Suche	1	0
Wortabstandssuche	1	1
Dateityp Anomalien	1	4

Kriterium 4.3.1 -Index Erstellung (Seite 71)
Encase bietet keinerlei Möglichkeiten einen Index zu erstellen.

Maßstab

Ausprägung	Kriterium wird	Punkte
E	nicht erfüllt	0

Kriterium 4.3.2 -Reguläre Ausdrücke (Seite 75)
Ein (umfangreiche) reguläre Sprache für die Suche wird angeboten und im Anhang des Benutzerhandbuchs beschrieben.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.3.3 -Phonetische Suche (Seite 77)
Eine phonetische Suche ist nicht implementiert. Ebenfalls existiert keine Möglichkeit einen externen Suchalgorithmus einzubinden.

Maßstab

Ausprägung	Kriterium wird	Punkte
C	nicht erfüllt	0

Kriterium 4.3.4 -Wortabstandssuche (Seite 79)
Es existiert das EnScript „Double Word finder", das Suchbegriffe findet, welche sich in einem einstellbaren Abstand zueinander befinden. Weitere Möglichkeiten existieren nicht.

Maßstab

Ausprägung	Kriterium wird	Punkte
D	kaum erfüllt	1

Kriterium 4.3.5 -Dateityp Anomalien (Seite 80)
Es kann explizit nach dieser Art von Anomalien gesucht werden. Dazu ist es notwendig, beim Start einer Suche anzugeben, dass die Datei Signatur mit überprüft werden soll.

Eine Überprüfung erfolgt dann anhand einer internen Tabelle, in welcher Dateisignaturen und ihre zugehörigen Dateiendungen abgelegt sind und welche vom Benutzer erweitert werden kann. Als Ergebnis erhält man einen von vier Fällen.

1. **Unknown:** Weder Dateiendung, noch Signatur sind bekannt.
2. **Match:** Dateiendung und Signatur stimmen überein.
3. ***[Alias]:** Die Signatur der Datei ist bekannt, die Endung der überprüften Datei passt aber nicht zu dieser Signatur.
4. **!Bad Signature:** Dateiendung ist in der Tabelle bekannt, für die Signatur der Datei ist aber keine bekannte Signatur in der Tabelle anzufinden.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.4 -PRÜFSUMMENBILDUNG (Seite 82)

Kriterium	Gewicht	Bewertung
Datenanalyse		
Prüfsummenbildung		**3**
Datenreduzierung	2	3
Existenzprüfung	2	3

Kriterium 4.4.1 -DATENREDUZIERUNG (Seite 84)
Die Datenreduzierung mittels Prüfsummen wird innerhalb der Suchfunktion ermöglicht und kann sich über einen auswählbaren Datenbereich erstrecken. Es werden sowohl öffentliche Datenbanken (z.B. der NSRL [NSR04]) als auch selbst angelegte Hashdatenbanken in beliebiger Anzahl unterstützt. Die Erstellung einer eigenen Datenbank mittels ausgewählter Dateien ist möglich. Allerdings ist EnCase auf den md5 Algorithmus beschränkt, eine Unterstützung von SHA-1 besteht derzeit nicht.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.4.2 -EXISTENZPRÜFUNG (Seite 85)
EnCase bietet ebenfalls die Möglichkeit, mittels der Prüfsumme die Existenz einer Datei in einer Datenbank zu überprüfen. Es gelten dabei die schon im Datenreduzierung Kriterium angesprochenen Eigenschaften.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.5 -Internet Benutzung (Seite 87)

Kriterium	Gewicht	Bewertung
Analyse		
Internet Benutzung		**2,3333**
Internetbrowser	2	3
E-Mail Anwendungen	3	2
Messanger	1	2
Peer to Peer Netze	X	

Kriterium 4.5.1 -Internetbrowser (Seite 88)
Mittels des Internet History EnScript ist es möglich den Verlauf des Internet Explorers und der temporären Internet-Dateien auszuwerten. Befinden sich noch einzelne HTML Dateien dieser besuchten Webseiten im lokalen Cache werden diese Fragmente übersichtlich dargestellt. Für die Netscape Browser (Version 4-6) werden ähnliche EnScripts angeboten, welche das Benutzerverhalten (Wann welche Seite besucht wurde) auflisten. Weiter Funktionalitäten in Bezug auf andere Browser (z.B. Firefox) oder Browserrelavante Daten (z.B. Cookies) sind nicht bekannt, könnten aber durchaus mittels EnScript realisiert werden. Die Analyse der Index.dat wird ermöglicht.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.5.2 -E-Mail Anwendung (Seite 90)
EnCase bietet mittels der „View File Structure“ Funktion die Möglichkeit sowohl die Mailbox von Outlook Express (.DBX) als auch Outlook (.PST) zu interpretieren. Dabei wird die Struktur der Mailbox, wie sie auch in der original Anwendung vorzufinden wäre, rekonstruiert. Eine Unterstützung weiterer Mailbox Formate ist nicht bekannt.

Maßstab

Ausprägung	Kriterium wird	Punkte
C	im mittlerem Umfang erfüllt	2

Kriterium 4.5.3 -Messenger (Seite 92)
Mittels eines EnScripts ist es möglich die Kontakte des AIM (AOL Instant Messanger) auszulesen. Bei ICQ ist es möglich, neben der Kontaktliste, auch den Nachrichten und Dateiaustausch zu extrahieren. Für deren Betrachtung wird zusammen mit dem EnScript das externe Programm „ICQ Explorer“ über die EnCase Webseite angeboten, welches die Auswertung der extrahierten Informationen erleichtert. Für den MSN Messenger wird ein EnScript angeboten, das die Suche nach Daten ermöglicht, die mittels des MSN erstellt wurden. Dies ist aber nur eine Erleichterung für das Auffinden, das auch mit einer

Suchanfrage möglich wäre. Weitere Analyse dieser Dateien erfolgt nicht, daher wird eine Unterstützung von MSN nicht zugesprochen. Eine Unterstützung für Jabber ist nicht bekannt.

Maßstab

Ausprägung	Kriterium wird	Punkte
C	im mittlerem Umfang erfüllt	2

Kriterium 4.6 -Metadaten (Seite 95)

Kriterium	Gewicht	Bewertung
Analyse		
Metadaten		**4**
MAC-Zeiten	2	4

Kriterium 4.6.1 -MAC-Zeiten (Seite 96)

Mittels der „Timeline View" können die Informationen der MAC-Zeiten auf graphische Weise übersichtlich dargestellt werden. Es ist möglich eine beliebige Auswahl der drei Attribute darzustellen, wobei der Zeitrahmen frei gewählt werden kann. Eine Navigation zwischen Präsentation und entsprechender Datei ist mittels einfachen Mausklick möglich.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

5.3.2 The Sleuth Kit / Autopsy Forensic Browser

WurzelkriteriumKriterium

Kriterium	Gewicht	Bewertung
Werkzeug der Computerforensik		**2,8598**
Anwender Support	2	2,8
Bedienung des Werkzeugs	3	3,2078
Protokollierung	2	3
Analyse	4	2,5585

Kriterium 1 -Anwender Support (Seite 37)

Kriterium	Gewicht	Bewertung
Anwender Support		**2,8**
Dienstzugang	2	1
Reaktionsverhalten	3	4

Kriterium 1.1 -Dienstzugang (Seite 37)
Über die Webseite wird die Anmeldung an eine Mailing-Liste angeboten. Der Zugriff über archivierte EMails dieser Liste wird ebenfalls ermöglicht. Weitere Kontaktmöglichkeiten werden nicht angeboten.

Maßstab

Ausprägung	Kriterium wird	Punkte
D	kaum erfüllt	1

Kriterium 1.2 -Reaktionsverhalten (Seite 38)
Eine Reaktion auf Anfragen erfolgt meist innerhalb von 24 Stunden. In der Regel sogar von Brian Carrier persönlich.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 2 -Bedienung des Werkzeugs (Seite 40)

Kriterium	Gewicht	Bewertung
Bedienung des Werkzeugs		
Robustheit	3	4
Dokumentation	4	2,5714
Automatisierung	3	3
Projektverwaltung	1	4

Kriterium 2.1 -Robustheit (Seite 41)
Während der Testphase von TSK kam es zu keinen Fällen, in welchen die Robustheit des Werkzeugs angesprochen wurde. Innerhalb der Bug-Liste sind ebenfalls keine Situationen

aufgeführt, mit denen eine solche Situation herbeigeführt werden könnte. Auch im Einsatz am LKA sind keine solchen Fälle bekannt. Da das TSK aus lauter Kommandozeilentools besteht, wäre es denkbar, dass eines dieser Tools in einen undefinierten Zugang übergeht (z.B. mit einem Segmentation Fault) und dadurch ein Analyseschritt abgebrochen werden müsste. Dies wäre mit der Erscheinungsform A im Schlüssel gleichzusetzen, da in solchen Fällen das Weiterarbeiten mit der Shell in der Regel ohne Probleme möglich ist.

Beim Einsatz des Autopsy Forensic Browser kam es unter Linux zu den gleichen Ergebnissen. Beim Einsatz einer CYGWIN Umgebung, welche nicht im kompletten Umfang installiert wurde, treten teilweise Fehlermeldungen über das nicht Vorhandensein einer dll-Datei auf. Durch eine Nachinstallation kann dieses Problem behoben werden. Beim Auftreten der Fehlermeldung beendet sich das Programm nicht, und der restliche Funktionsumfang bleibt erhalten. Es könnte also ebenfalls der Schlüsse A vergeben werden.

Aufgrund der Offenheit beider Programme ist also eine gute Abschätzung über die Arbeitsweise möglich. Das Kriterium wird daher nicht gestrichen und eine Bewertung durchgeführt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 2.2 -Dokumentation (Seite 43)

Kriterium	Gewicht	Bewertung
Bedienung des Werkzeugs		
Dokumentation		**2,5714**
Funktionsbeschreibung	4	3
Tutorials	1	4
Online Hilfe	2	1

Kriterium 2.2.1 -Funktionsbeschreibung (Seite 44)
Die einzelnen Tools des TSK sind mit den üblichen manual pages ausgestattet. Auf der Webseite findet sich ein Überblick aller Tools mit den Verweis auf diese manual pages. In diesen sind die Funktionsweisen und Parameter ausreichend beschrieben. Eine Beschreibung des Formats der Ausgabe bzw. der Ergebnisse fehlt aber generell. Der Punkt auf Ergiebigkeit kann also nicht vergeben werden. An der Struktur und Vollständigkeit ist hingegen nichts auszusetzen.

Die Funktionen von Autopsy werden innerhalb eines mitgelieferten HTML Dokuments erläutert. Die Funktionen werden ausreichend in textueller Form beschrieben. Gerade bei der Verwendung eines Hypertext Mediums als Dokument wäre sinnvoll, Bilder als zusätzliche Hilfe einzusetzen. In Anbetracht des schlechten Ergebnisses für TSK wird für die zusammenfassende Bewertung des Werkzeugs also kein Punkt vergeben. Innerhalb der Beschreibung ist eine übersichtliche Struktur zu erkennen, in der man sich leicht zurecht findet. Ebenfalls konnten keine Lücken in Bezug auf die Dokumentation festgestellt werden.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 2.2.2 -TUTORIALS (Seite 46)
Auf der Webseite stehen einige „offizielle„ Befunde zu Fallstudien des Honeynet Projects zu Verfügung, welche eine komplette Schritt-für-Schritt-Anleitung zur Lösung dieses Problems anzeigen. Des Weiteren steht eine Einführung zur grundlegenden Analyse eines Bitstream-Images und zur Analyse von MAC-Zeiten zur Verfügung. Schließlich wird zweimonatlich der „The Sleuth Kit Informer“ herausgegeben, welcher grundlegende Bereiche der Computerforensik im Zusammenhang mit dem TSK beschreibt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 2.2.3 -ONLINE HILFE (Seite 47)
Bei den Tools des TSK stehen diesbezüglich die manual pages jederzeit zu Verfügung. In Autopsy ist der Zugang zur Funktionsbeschreibung jederzeit über eine eigene Schaltfläche zugänglich. Weiterführende Hilfsmittel sind nicht implementiert.

Maßstab

Ausprägung	Kriterium wird	Punkte
D	kaum erfüllt	1

Kriterium 2.3 -AUTOMATISIERUNG (Seite 49)
Der Output der einzelnen Tools ist ohne Probleme als Input wieder zu verwenden (mittels der standard Pipe |). Der Zugriff auf die Tools kann ohne Probleme mit den auf dem System vorhandenen Skript- oder Programmiersprachen erfolgen. Für Autopsy ist keine Automatisierung vorgesehen.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 2.4 -PROJEKTVERWALTUNG (Seite 50)
TSK bietet aufgrund seiner Intention diesbezüglich keine Funktionalität und überlässt diese Aufgabe vollständig Autopsy. Dieses bietet eine übersichtliche Darstellung für einzelne Untersuchungen, welche mehrere Bitstream-Images enthalten können. Es wird sogar die Möglichkeit gegeben, mehrere Ermittler zu verwalten. Die Verwaltung der Daten funktioniert dabei transparent im Sinne der Kriteriumsbeschreibung. Die Ergebnisse der

Untersuchung werden übersichtlich dargestellt, wobei die Limitierungen von HTML bzw. dem Browser zu berücksichtigen sind (z.B. unterschiedliche Darstellung bei unterschiedlichen Browsern, Probleme bei großen Dateien, usw.). Die Möglichkeit eigene Notizen zu den einzelnen Analyseschritten zu setzen, ist ebenfalls möglich.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 3 -Protokollierung der Untersuchung (Seite 52)
Die Arbeit mit TSK kann vollständig mit dem standard Linux Tool `script` erfolgen. Hiermit ist es auch möglich, eine selektive Protokollierung durchzuführen, allerdings muss diese Entscheidung vor dem Funktionsaufruf erfolgen.

Autopsy bietet die Möglichkeit, ein Protokoll über den aktuell untersuchten Sektor oder die aktuelle Datei auszugeben. Diese enthält alle notwendigen Informationen. Eine selektive Speicherung und gesammelte Anzeige ist mittels der Notizfunktion möglich, hierbei ist aber eine direkte Übernahme aus dem Teilprotokoll nur per copy&paste möglich. Dieser Punkt kann also nicht gewertet werden, da auf diese Weise auch eine externe Protokollierung erfolgen könnte. Alle in Autopsy ausgeführten Aktionen werden Benutzerspezifisch in der Datei exec.log innerhalb der Projektverwaltung gespeichert.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4 -Analyse (Seite 54)

Kriterium	Gewicht	Bewertung
Datenanalyse		**2,5585**
Rohdaten Analyse	4	3,8
Daten Extraktion und Wiederherstellung	4	2,8235
Suchverfahren	3	3
Prüfsummen	3	2
Internetnutzung	1	0
Metadaten	2	1

Kriterium 4.1 -Rohdaten Analyse (Seite 56)

Kriterium	Gewicht	Bewertung
Analyse		
Rohdaten Analyse		**3,8**
Image Erkennung	1	3
Dateisystem Unterstützung	4	4

Kriterium 4.1.1 -Image Erkennung (Seite 56)
The Sleuth Kit unterstützt nur reine Bitstream-Images, keine weiteren Formate. Hierbei ist zu beachten, dass in der aktuellen Version aus dem Image zunächst mittels `mmls` eventuell vorhandene Partitionen extrahiert werden müssen, da ansonsten keine Analyse möglich ist. An diesem Umstand wird aber aktuell gearbeitet, und er soll in der nächsten Version nicht mehr vorliegen.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.1.2 -Dateisystem Unterstützung (Seite 58)
Es werden die Dateisysteme NTFS, FAT, (Berkley) FFS , EXT2FS, und EXT3FS unterstützt.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2 -Daten Extraktion und Wiederherstellung (Seite 60)

Kriterium	Gewicht	Bewertung
Analyse		
Daten Extraktion und Wiederherstellung		**2,8235**
Gelöschte Daten	4	4
Unzugeordnete Bereiche	4	3
Slack Bereiche	4	3
Auslagerungsdateien und Swap-Partitionen	2	2
Verschlüsselte und komprimierte Daten	2	0
Alternate Data Streams	1	4

Kriterium 4.2.1 -Gelöschte Daten (Seite 61)
Mittels des Tools `fls` können alle gelöschten Dateien angezeigt werden, welche zur Wiederherstellung geeignet sind.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.2.2 -Nicht zugeordnete Bereiche (Seite 63)
Mittels `dls` und `icat` ist die Bereitstellung der unzugeordneten Bereiche möglich. Innerhalb von Autopsy wird eine Liste der unzugeordneten Bereiche angezeigt, über welche ein einfacher Zugriff möglich ist. Die restlichen Analysemethoden können ebenfalls auf

diese Daten angewandt werden. Spezielle Analyse-Funktionen für diese Bereiche stehen nicht zu Verfügung.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.2.3 -Slack Bereiche (Seite 64)
Mittels `dls -s` kann der File-Slack und RAM-Slack ohne Probleme ausgegeben werden. Eine Unterstützung den MFT-Slack existiert nicht.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	größtenteils erfüllt	3

Kriterium 4.2.4 -Auslagerungsdateien und Swap-Partitionen (Seite 66)
Es besteht kein Unterschied zwischen Auslagerungsdateien und anderen Dateien des Dateisystems. Zusätzliche Funktionalitäten sind nicht vorgesehen.

Maßstab

Ausprägung	Kriterium wird	Punkte
B	im mittlerem Umfang erfüllt	2

Kriterium 4.2.5 -Verschlüsselte und komprimierte Daten (Seite 68)
Eine automatische Unterstützung von komprimierten Daten ist nicht vorgesehen. Es bleibt dem Anwender überlassen, sich hier eine (externe) individuelle Lösung selber anzufertigen (z.B. ein Skript, welches die entsprechenden Dateien findet und in ein spezielles Verzeichnis unter Berücksichtigung der Verzeichnisstruktur dekomprimiert).

Maßstab

Ausprägung	Kriterium wird	Punkte
D	nicht erfüllt	0

Kriterium 4.2.6 -Alternate Data Streams (Seite 69)
Mittels `fls` werden ADS erkannt und können ohne Probleme weiterverarbeitet werden.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.3 -SUCHVERFAHREN (Seite 71)

Kriterium	Gewicht	Bewertung
Analyse		
Suchverfahren		**3**
Index Erstellung	2	4
Reguläre Ausdrücke	3	4
Phonetische Suche	1	0
Wortabstandssuche	1	0
Dateityp Anomalien	1	4

Kriterium 4.3.1 -INDEX ERSTELLUNG (Seite 71)
Es existiert ein Patch von Paul Bakker, welcher die indexbasierte Suche für das SLK und Autopsy implementiert hat. Dieses bindet sich nahtlos in die bestehenden Tools ein und wird innerhalb des Sleuthkit Informers [Bak04] offiziell vorgestellt. Für die Bewertung wird es daher als Bestandteil des SLK angesehen.

Die Möglichkeit, Parameter für die Erstellung des Index einzustellen (z.B. maximale/minimal Länge der Zeichenkette), ist gegeben. Des Weiteren wird die Fragmentierung der Daten wird bei der Erstellung beachtet.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.3.2 -REGULÄRE AUSDRÜCKE (Seite 75)
Die Suche mittels regulären Ausdrücken wird bei TSK über das standardmäßig im System mitgelieferte Tool `grep` realisiert. Dieses bietet eine reguläre Sprache, mit der umfangreiche Muster beschrieben werden können.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.3.3 -PHONETISCHE SUCHE (Seite 77)
Es wird keine Unterstützung für eine phonetische Suche angeboten. Die Arbeitsweise von TSK würde die Implementierung oder die Verwendung eines externen Algorithmus bzw. Tools auf einfache Weise ermöglichen.

Maßstab

Ausprägung	Kriterium wird	Punkte
C	nicht erfüllt	0

Kriterium 4.3.4 -WORTABSTANDSSUCHE (Seite 79)
Wird standardmäßig von TSK nicht unterstützt. Die Verwendung externer Programme (z.B. `glark` [Pac04]) wäre aber einfach möglich.

Maßstab

Ausprägung	Kriterium wird	Punkte
E	nicht erfüllt	0

Kriterium 4.3.5 -DATEITYP ANOMALIEN (Seite 80)
Die Suche nach Dateityp Anomalien erfolgt mit Hilfe von `sorter`. Wird eine bekannte Signatur gefunden, so wird überprüft, ob eine passende Datei-Endung vorliegt. Ist dies nicht der Fall, so wird ein Treffer ausgegeben. Als Basis für die Überprüfung wird das magic file des zu Grunde liegenden Systems verwendet. Für die Datei-Endung wird eine eigene Liste geführt. Beide Dateien können ohne weiteres editiert werden.

Maßstab

Ausprägung	Kriterium wird	Punkte
A	voll erfüllt	4

Kriterium 4.4 -PRÜFSUMMENBILDUNG (Seite 82)

Kriterium	Gewicht	Bewertung
Datenanalyse		
Prüfsummenbildung		**2**
Datenreduzierung	2	2
Existenzprüfung	2	2

Kriterium 4.4.1 -DATENREDUZIERUNG (Seite 84)
Die Suche in einer Datenbank nach einer Prüfsumme erfolgt mittels `hfind`, welches sowohl den MD5, als auch den SHA-1 Algorithmus unterstützt. Die Erstellung von eigenen Datenbanken ist nur über die Kommandozeile mittels den entsprechenden Hashfunktionen (z.B. `md5sum /bin/* /sbin/* > bin-md5.db`) möglich. Eine Auswahl von bestimmten Dateien ist daher nur über die entsprechenden Filter der Kommandozeile möglich. Gestaltet sich dies bei wenigen Verzeichnissen noch leicht, so können bei einer Selektion von bestimmten Daten durchaus komplizierte Filterausdrücke nötig sein. Für diese Eigenschaft wird daher kein Punkt vergeben.

`hfind` unterstützt bei einem Aufruf nur die Angabe von einer Datenbank, hier müsste also eine Verkettung mit Hilfe der Shell erfolgen. Autopsy unterstützt die Verwendung von drei Datenbanken (Die Datenbank von NSRL [NSR04] und jeweils eine eigene für bekannte und gesuchte Dateien). Man müsste also von Hand seine eigenen Datenbanken zusammenfügen. Der Punkt kann also ebenfalls nicht vergeben werden.

Maßstab

Ausprägung	Kriterium wird	Punkte
C	im mittlerem Umfang erfüllt	2

Kriterium 4.4.2 -Existenzprüfung (Seite 85)
Die Bewertung der Existenzprüfung erfolgt analog zur Datenreduzierung.

Maßstab

Ausprägung	Kriterium wird	Punkte
C	im mittlerem Umfang erfüllt	2

Kriterium 4.5 -Internet Benutzung (Seite 87)
Es stehen keinerlei Funktionen zu Analyse der Internetbenutzung zu Verfügung.

Kriterium 4.6 -Metadaten (Seite 95)

Kriterium	Gewicht	Bewertung
Analyse		
Metadaten		**1**
MAC-Zeiten	2	1

Kriterium 4.6.1 -MAC-Zeiten (Seite 96)
Mittels `fls` und `ils` können die MAC Daten ausgelesen und an `mactime` übergeben werden. Dieses leistet dann eine Interpretation der Daten. Die Ausgabe erfolgt in einer ASCII Tabelle, welche formatbedingt nicht sehr übersichtlich ist. In Autopsy wird eine HTML Tabelle angezeigt, welche ihren Zweck erfüllt. Die Einschränkung auf einen Zeitrahmen kann nur in Intervallen von einem Tag erfolgen. Für eine weitere Einschränkung wird zu einer Weitergabe der Daten an ein externes Programm geraten. Für eine positive Bewertung des Punktes ist dies aber ein zu grober Zeitraum, da sich interessante Vorgänge in der Regel innerhalb weniger Stunden oder sogar in einem kürzeren Zeitraum abspielen. Innerhalb von TSK/Autopsy ist es nicht möglich die Anzeige weiter einzuschränken. Ebenso ist es nicht möglich, aus der Präsentation auf einfache Weise auf die entsprechenden Daten zuzugreifen.

Maßstab

Ausprägung	Kriterium wird	Punkte
D	kaum erfüllt	1

5.4 Interpretation des Ergebnisses

EnCase erhält eine Bewertung von **3,2067**, The Sleuth Kit / Autopsy Forensic Browser erhält eine Bewertung von **2,8598** (siehe Abbildung 5.2). EnCase ist daher für das angegebene Szenario der Analyse von Bitstream-Images besser geeignet. Diese Aussage und die Werte sollten aber noch kurz diskutiert werden.

Das gute Abschneiden von EnCase kann mittels seiner Intention erklärt werden, ein umfangreiches Werkzeug für die forensische Untersuchung zu liefern. Es zeigt in keinen der Hauptkriterien Schwächen, wie es bei TSK der Fall ist, welches sich auf die Bereitstellung von Daten spezialisiert. Gerade bei der Interpretation von Daten (Internetnutzung, Metadaten) liegt TSK deutlich hinter EnCase zurück.

Viel schwer wiegender sind aber die Ergebnisse bei der Datenextraktion und Wiederherstellung. In diesem äußerst wichtigen Bereich kann EnCase bei den einzelnen Teilkriterien punkten. Hier zeigt sich an den Kriterien „verschlüsselte und komprimierte Daten“ und „Auslagerungsdateien“ wiederum deutlich die gerade genannte Ausrichtung der Werkzeuge. Die fehlenden Punkte in den anderen Teilkriterien sind vor allem auf Unterschiede bei der Bereitstellung von zusätzlichen Funktionalitäten zurückzuführen (EnScripts für spezielle Analyseschritte).

Generell ist die ermittelte Punktzahl aber nicht überzubewerten. Einerseits fehlen die Vergleichsmöglichkeiten. Hier wäre die Bewertung von Werkzeugen anderer Hersteller (z.B. Vogon [Vog04], New Technologies [New04]) sinnvoll, um die Werte besser einschätzen zu können. Andererseits kann auch keine Aussage im Vergleich zu den Wertgrenzen gemacht werden. Eine Punktzahl von 4 beschreibt zwar den besten Wert, der Wert von 0 kann aber nicht als schlechtester Wert angesehen werden. Dieser Wert würde bedeuten, dass gar kein Kriterium erfüllt worden ist. Das wäre aber gleichbedeutend damit, dass keine Funktionalität angeboten wird. Ein solches Werkzeug dürfte aber kaum als ein Werkzeug für die Analyse von Bitstream-Images angeboten werden.

Schließlich kann die gute Bewertung von EnCase auch durch seinen Einfluss während der Erstellung des Kriterienkatalogs erklärt werden. Ein Großteil der Informationen über die Arbeitsweise von Werkzeugen der Computerforensik stammen aus Gesprächen mit Herrn Köllner vom LKA Bayern. Ebenfalls wurden die Bewertungsgrundlagen und Gewichtungen im intensiven Gespräch mit ihm geklärt. Da im LKA aber vor allem EnCase als Werkzeug im Einsatz ist, kann hier ein Einfluss nicht ausgeschlossen werden.

Kriterium	Titel	Gewicht	EnCase	TSK
	Bewertung des Werkzeugs		3,2067	2,8598
1	Anwender Support	2	3,6	2,8
1.1	Dienstzugang	2	3	1
1.2	Reaktionsverhalten	3	4	4
2	Bedienung des Werkzeugs	3	2,2208	3,2078
2.1	Robustheit	3	0	4
2.2	Dokumentation	4	2,8571	2,5714
2.2.1	Funktionsbeschreibung	4	4	3
2.2.2	Tutorials	1	4	4
2.2.3	Online Hilfe	2	0	1
2.3	Automatisierung	3	3	3
2.4	Projektverwaltung	1	4	4
3	Protokollierung der Untersuchung	2	4	3
4	Analyse	4	3,3475	2,5585
4.1	Rohdaten Analyse	4	3,8	3,8
4.1.1	Image Erkennung	1	3	3
4.1.2	Dateisystem Unterstützung	4	4	4
4.2	Daten Extraktion und Wiederherstellung	4	4	2,8235
4.2.1	Gelöschte Daten	4	4	4
4.2.2	Nicht zugeordnete Bereiche	4	4	3
4.2.3	Slack Bereiche	4	4	3
4.2.4	Auslagerungsdateien und Swap-Partitionen	2	4	2
4.2.5	Verschlüsselte und komprimierte Daten	2	4	0
4.2.6	Alternate Data Streams	1	4	4
4.3	Suchverfahren	3	2,125	3
4.3.1	Index Erstellung	2	0	4
4.3.2	Reguläre Ausdrücke	3	4	4
4.3.3	Phonetische Suche	1	0	0
4.3.4	Wortabstandssuche	1	1	0
4.3.5	Dateityp Anomalien	1	4	4
4.4	Prüfsummenbildung	3	3	2
4.4.1	Datenreduzierung	2	3	2
4.4.2	Existenzprüfung	2	3	2
4.5	Internet Benutzung	1	2,333	0
4.5.1	Internetbrowser	2	3	0
4.5.2	E-Mail Anwendung	3	2	0
4.5.3	Messenger	1	2	0
4.5.4	Peer to Peer Netze	X		
4.6	Metadaten	2	4	2
4.6.1	MAC-Zeiten	2	4	2
4.6.2	Applikationsabhängige Metadaten	X		

Tabelle 5.2: Bewertung der Werkzeuge

6 Zusammenfassung und Ausblick

Ziel der vorliegenden Diplomarbeit war die Evalierung von Werkzeugen der Computerforensik. Hierfür wurde ein Kriterienkatalog erstellt und beispielhaft auf zwei Werkzeuge angewandt. Das Einsatzgebiet der Werkzeuge wurde hierbei, aufgrund des weiten Themenbereiches der Computerforensik, auf das Szenario der Bewertung von Bitstream-Images eingegrenzt.

Die Methodik zur Erstellung von Kriterienkatalogen wurde von [Bre02] übernommen und an das aktuelle Szenario angepasst. Diese ermöglicht eine flexible Anpassung des Katalogs an ein gegebenes Szenario und bietet insbesondere einen einfachen Mechanismus zur Aufnahme von weiteren Kriterien bzw. ganzen Kriteriengruppen in den Kriterienkatalog, ohne dass die Bewertung aller Kriterien komplett überarbeitet werden muss.

Eine der Prämissen bei der Erstellung des Kriterienkatalogs bestand darin, dass die Anwendung des Katalogs auch ohne lange Einarbeitungszeit in das Werkzeug erfolgen kann. Die Bewertung der einzelnen Kriterien gestaltete sich folglich als schwierig, da zur Festellung eines Erfüllungsgrades deswegen keine Tests oder andere umfangreiche Auswertungsschritte verwendet werden konnten. Es wurde daher ein System angewandt, welches ermöglicht, die einzelnen Kriterien, anhand von quantitativen Überlegungen, auf effiziente Weise zu bewerten. Als Ergebnis erhält man einen schlanken Kriterienkatalog, dessen Anwendung, in Abhängigkeit des eigenen Wissens und der zu Verfügung stehenden Quellen, relativ zügig durchzuführen ist. Dabei zeigte sich, dass das numerische Ergebnis der Anwendung gar nicht so sehr interessiert, sondern der Prozess der Bewertung schon ausreichend Informationen liefert.

Durch dieses Vorgehen entfällt aber jeder qualitative Charakter bei der Bewertung der einzelnen Kriterien. Gerade dieser ist aber oft bei der Einschätzung eines Kriteriums und somit des ganzen Werkzeugs erwünscht. Eine Lösung hierfür wäre einerseits die Erweiterung jedes einzelnen Kriteriums um weitere Teilkriterien, so dass mehrere Teilaspekte bei der Beurteilung des Kriteriums berücksichtigt werden. Dies würde die Zahl der Kriterien aber drastisch steigern und für den vorliegenden Fall auf deutlich über 100 anwachsen lassen. Andererseits müsste der Bewertungsmaßstab verfeinert werden, so dass eine differenziertere Aussage möglich ist. Die Überprüfung eines Kriteriums wäre dann aber nur noch mit ausführlichen Tests möglich und nicht mehr durch einfache Entscheidungsvorgänge. Diesen Ansatz schlägt das Computer Forensic Tool Testing Projekt (CFTT) [CFT04] ein, welches einen Rahmen für die Bewertung von Werkzeugen anbietet. Die Evaluierung einer Funktion des Werkzeugs, die im aktuellen Katalog in etwa einem Kriterium entspricht, anhand der CFTT Richtlinien, würde aber bereits zu einem Kriterienkatalog mit den Ausmaßen der vorliegenden Arbeit führen. Ein umfassender Kriterienkatalog, welcher nach diesen Richtlinien erstellt wurde, dürfte aber einige interessante Aspekte über die Werkzeuge der Computerforensik liefern. Die vorliegende

Methodik würde hierfür sogar eine brauchbare Grundlage bieten, da es ohne Probleme möglich wäre, die einzelnen Kriterienbereiche in unabhängigen Projekten zu bearbeiten und anschließend in einem vollständigen Kriterienkatalog zusammenzuführen.

Die Aufteilung in unabhängige Projekte liefert auch die Ideen für zukünftige Arbeiten in diesem Bereich. Die gefunden Kriterien, die nicht in den Katalog aufgenommen wurden (z.B. betriebswirtschaftliche Kriterien, juristische Aspekte), bieten sich zum Beispiel als Basis für weitere Untersuchungen an. Der Umfang einer Analyse eines solchen Kriteriums dürfte durchaus dem der vorliegenden Arbeit entsprechen. Analog kann natürlich auch für ein wichtiges Kriterium aus dem verwendeten Kriterienkatalog (z.B. Suchverfahren) eine genauere Untersuchung angesetzt werden. Ein weiteres Themengebiet ergibt sich aus der Problematik der Bewertung von Kriterien. Es existiert einerseits nur das umfassende Rahmenwerk des CFTT Projekts, andererseits nur das sehr einfache Schema der vorliegenden Arbeit. Hier einen Mittelweg auszuarbeiten, wäre eine ideales Thema einer weiteren Forschungsarbeit.

Literaturverzeichnis

[Bak04] Bakker, Paul. Searchtools, Indexed Searching in Forensic Images. *The Sleuth Kit Informer*, 16, 2004.
Available from World Wide Web:
http://www.sleuthkit.org/informer/sleuthkit-informer-16.html.

[Bor04] Kai Bormann. Phonetische Ähnlichkeitssuche im Englischen, 2004.
Available from World Wide Web:
http://www.cl.uni-heidelberg.de/~bormann/documents/phono/phon_sim_search.pdf.

[Bre02] Brenner, M. Erstellung eines Kriterienkatalogs zur Beurteilung des Anwender Supports in der BMW Group. Diplomarabeit, Ludwig-Maximilians-Universität München, 2002.

[BS004] Liste der Betriebssysteme. Wikipedia, 2004.
Available from World Wide Web:
http://de.wikipedia.org/wiki/Liste_der_Betriebssysteme.

[Bun03a] Kriminalstatistik zur Computerkriminalität. Bundeskriminalamt, 2003.
Available from World Wide Web:
http://www.bka.de/pks/pks2003/p_3_21.pdf.

[Bun03b] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutzhandbuch*. Bundesamt für Sicherheit in der Informationstechnik, 2003.
Available from World Wide Web:
http://www.bsi.bund.de/gshb/deutsch/GSHB2003.zip.

[Bun03c] Bundesamt für Sicherheit in der Informationstechnik. Leitfaden IT-Sicherheit, 2003.
Available from World Wide Web:
http://www.bsi.bund.de/gshb/Leitfaden/GS-Leitfaden.pdf.

[Car02] Carrier, Brian. Open source digital Forensics Tools: The Legal Argument, 2002.
Available from World Wide Web:
http://www.atstake.com/research/reports/acrobat/atstake_opensource_forensics.pdf.

[Car04a] Carriar, Brian. The Sleuth Kit, 2004.
Available from World Wide Web:
http://www.sleuthkit.org/index.php.

[Car04b] Carrier, Brian. Digital Forensics Tool Testing Images, 2004.
Available from World Wide Web:
`http://dftt.sourceforge.net/`.

[Car04c] Carvey, H. The Dark Side of NTFS, 2004.
Available from World Wide Web:
`http://patriot.net/~carvdawg/docs/dark_side.html`.

[CFT04] Computer Forensics Tool Testing (CFTT). National Institute of Standards and Technology, 2004.
Available from World Wide Web:
`http://www.cftt.nist.gov/`.

[Cur02] Curtis, Jason. Internet Explorer und WinXP: Verhängnisvolle index.dat, 2002.
Available from World Wide Web:
`http://www.zdnet.de/enterprise/print_this.htm?pid=20000261-20000013c`.

[Cyg04] Cygwin, Eine Linuxartige Umgebung für Windows Betriebssysteme, 2004.
Available from World Wide Web:
`http://www.cygwin.com/`.

[De 02] De Vel, Olivier and Corney, Malco and Anderson, Alison and Mohay, George. Language and Gender Author Cohort Analysis of E-Mail for Computer Forensics, 2002.
Available from World Wide Web:
`http://www.dfrws.org/dfrws2002/papers/Papers/Olivier_DeVel.pdf`.

[Dig04] Digital Forensic Research Workshop, 2004.
Available from World Wide Web:
`http://www.dfrws.org`.

[Eck03] Eckert, Claudia. *IT-Sicherheit*. Oldenbourg, 2003.

[FV01] Farmer, Dan and Venema, Wietse. Computer Forensics Column, 2001.
Available from World Wide Web:
`http://www.porcupine.org/forensics/column.html`.

[FV04] Farmer, Dan and Venema, Wietse. The Coroner's Toolkit (TCT), 2004.
Available from World Wide Web:
`http://www.porcupine.org/forensics/tct.html`.

[Ges04] Geschonneck, Alexander. *Computer Forensik*. dpunkt.Verlag, 2004.

[Gie00] Giemsa, F. Evaluation von Outsourcing–Beziehungen für die IT–Hotline der BMW AG. Diplomarbeit, Ludwig-Maximilians-Universität München, 2000.

[goo04] Googlefight - Vergleich von zu Verfügung stehenden Quellen im Internet. Abondance, 2004.

Available from World Wide Web:
http://www.googlefight.com.

[Hey02] Heyne, Frank. FAQ: Alternate Data Streams in NTFS, 2002.
Available from World Wide Web:
http://www.heysoft.de/nt/ntfs-ads.htm.

[Hon04] The Honeynet Project. The Honeynet Project, 2004.
Available from World Wide Web:
http://www.honeynet.org/misc/chall.html.

[Ilo04] ILook Investigator. Internal Revenue Service Criminal Investigation Electronic Crimes Program, 2004.
Available from World Wide Web:
http://www.ilook-forensics.org/.

[Ind04] Index.dat - What is Index.dat File? AceSoft.net, 2004.
Available from World Wide Web:
http://www.acesoft.net/delete_index.dat_files.htm.

[Int03] International Journal of Digital Evidence, 2003.
Available from World Wide Web:
http://www.ijde.org/archives_home.html.

[Int04a] International Telecommunication Union. Enhanced Telecom Operations Map, 2004.
Available from World Wide Web:
http://www.itu.int/ITU-T/studygroups/com04/tmc/etom/index.html.

[Int04b] Internet Struktur Daten. FGW Online GmbH, 2004.
Available from World Wide Web:
http://www.fgw-online.de/Aktuelles/PM_Strukturdaten/web_III_04.pdf.

[ITI04] ITIL Online. Office of Government Commerce, 2004.
Available from World Wide Web:
http://www.itil.co.uk.

[Joh03] Johansson, Christian. Computer Forensic Text Analyses with Open Source Software. Master's thesis, Blekinge Institute of Technology, 2003.
Available from World Wide Web:
http://www.fukt.bth.se/~uncle/papers/master/thesis.pdf.

[Kau03] Kausche, Niels. Konstruktion eines Hilfesystems für JWAM. Master's thesis, Universität Hamburg, 2003.
Available from World Wide Web:
http://swt-www.informatik.uni-hamburg.de/publications/files/Stud/studienarbeit.pdf.

[Lee04] Leetspeak - Ersetzen von Buchstaben durch ähnliche Zeichen. Wikipedia, 2004.
Available from World Wide Web:
http://de.wikipedia.org/wiki/Leet.

[Met03] Minimieren von Metadaten in Microsoft Word 2002. Microsoft, 2003.
Available from World Wide Web:
http://support.microsoft.com/kb/290945/DE/.

[Met04] Minimieren von Metadaten in Microsoft Word-Dokumenten. Microsoft, 2004.
Available from World Wide Web:
http://support.microsoft.com/kb/223790/DE/.

[Nat95] National Archives and Records Administration. Using the Census Soundex. General Information Leaflet 55, 1995.
Available from World Wide Web:
http://www.archives.gov/research_room/genealogy/census/soundex.html.

[Nat04] National Security Agency. Security Recommendation Guides, 2004.
Available from World Wide Web:
http://www.nsa.gov/snac/.

[New04] New Technologies. Forensic & Security Software, 2004.
Available from World Wide Web:
http://www.forensics-intl.com/.

[NSR04] National Software Reference Library (NSRL), 2004.
Available from World Wide Web:
http://www.nsrl.nist.gov/.

[NTF04] Ntfs.com, 2004.
Available from World Wide Web:
http://www.ntfs.com/.

[oSN02] National Institute of Standards and Technology (NIST). Secure hash standard, 2002.
Available from World Wide Web:
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf.

[Pac04] Pace, Jeff. glark, a replacement for (or supplement to) the grep family, 2004.
Available from World Wide Web:
http://glark.sourceforge.net/.

[Phr04] Phrack ...a Hacker magazine by the community, for the community... Phrack, 2004.
Available from World Wide Web:
http://www.phrack.org/.

[Pom04] Pommerening, Klaus. Datenschutz und Datensicherheit: Kryptographische Basistechniken, 2004.
Available from World Wide Web:
http://www.uni-mainz.de/~pommeren/DSVorlesung/KryptoBasis/Hash.html.

[Reg04] Reguläre Ausdrücke. Wikipedia, 2004.
Available from World Wide Web:
http://de.wikipedia.org/wiki/Reguläre_Ausdrücke.

[Riv92] Rivest, Ron. RFC 1321 - The MD5 Message-Digest Algorithm, 1992.
Available from World Wide Web:
http://www.faqs.org/rfcs/rfc1321.html.

[Sch99] Scheiter, C. Erstellung eines Kriterienkatalogs zum Vergleich verschiedener Netzkonzepte für BMW und Rover. Diplomarbeit, Technische Univeristät München, 1999.

[Sch00] Schulz. Pflege des ext2fs-Dateisystems, 2000.
Available from World Wide Web:
http://www.linux-magazin.de/Artikel/ausgabe/2000/04/Ext2fs/ext2fs.html.

[See03] Seeger, Prof. Dr. Bernhard. Index und Speicherstrukturen, 2003.

[SK02] Siebert, Gunnar and Kempf, Gunnar. *Benchmarking: Leitfaden für die Praxis*. Hanser Wirtschaft Verlag, 2002.

[Sof04a] Guidance Software. Encase forensic edition, 2004.
Available from World Wide Web:
http://www.guidancesoftware.com/products/EnCaseForensic/.

[Sof04b] Guidance Software. The encase message boards, 2004.
Available from World Wide Web:
http://www.guidancesoftware.com/support/messageboard/.

[Str04] Streams - A NTFS file stream information tool. Sysinternals, 2004.
Available from World Wide Web:
http://www.sysinternals.com/ntw2k/source/misc.shtml.

[Tou95] Touch, Joe. RFC 1810 - Report on MD5 Performance, 1995.
Available from World Wide Web:
http://www.faqs.org/rfcs/rfc1810.html.

[Vir04] Virtuelle Speicherverwaltung. Wikipedia, 2004.
Available from World Wide Web:
http://de.wikipedia.org/wiki/Virtuelle_Speicherverwaltung.

[Vog04] Forensic Bulletin Online. Vogon International Limited, 2004.
Available from World Wide Web:
http://www.vogon-international.com/computer%20evidence/bulletin-00.htm.

[W2K00] W2K.Stream Virus. Symantec, 2000.
Available from World Wide Web:
`http://securityresponse.symantec.com/avcenter/venc/data/w2k.stream.html`.

[Win04] Windows auf 96 Prozent aller Rechner. Futurezone / APA, 2004.
Available from World Wide Web:
`http://futurezone.orf.at/futurezone.orf?read=detail&id=211494`.