HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Marius Julian Walter Zimmer

Ein forensischer Leitfaden zu Spezialverfahren der Datenrettung von Festplatten unter Nutzung des PC3000-Express System

Mittweida, 2022

Fakultät Angewandte Computer – und Biowissenschaften

BACHELORARBEIT

Ein forensischer Leitfaden zu Spezialverfahren der Datenrettung von Festplatten unter Nutzung des PC-3000 Express System

Autor:
Herr

Marius Julian Walter Zimmer

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO18w3-B

Erstprüfer:
Prof. Dipl.-Ing. (BA) Ronny Bodach

Zweitprüfer:
B. Sc. Bruce Kenworthy

Einreichung:
Leipzig, 14.01.2022

Verteidigung/Bewertung:
Mittweida, 2022

Faculty Applied Computer Sciences and Biosciences

BACHELOR THESIS

A forensic guide to special procedures for data recovery from hard drives using the PC-3000 Express system

author:
Mr.

Marius Julian Walter Zimmer

course of studies:
General and Digital Forensic Science

seminar group:
FO18w3-B

first examiner:
Prof. Dipl.-Ing. (BA) Ronny Bodach

second examiner:
B. Sc. Bruce Kenworthy

submission:
Leipzig, 14.01.2022

defence/ evaluation:
Mittweida, 2022

Bibliografische Beschreibung:

Zimmer, Marius Julian Walter:
Ein forensischer Leitfaden zu Spezialverfahren der Datenrettung von Festplatten unter Nutzung des PC-3000 Express System. - 2022.
– 18 Seiten Verzeichnisse, 102 Seiten Inhalt, 0 Seiten Anhänge
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022

Referat:

Diese Arbeit präsentiert einen forensischen Leitfaden zu Spezialverfahren der Datenrettung von Festplatten unter Nutzung des PC-3000 Express Systems. Die Grundlage bilden essentielle Informationen rund um eine Festplatte und die Bedienung des PC-3000 Express Systems. Anschließend wird ein in drei Teile gegliederter forensischer Leitfaden vorgestellt, der dem Leser mit jeder Unterteilung eine Konkretisierung auf das Thema Spezialverfahren der Datenrettung von Festplatten präsentieren soll. Auf der Grundlage des forensischen Leitfadens werden im Anschluss zwei Festplatten untersucht und mit Hilfe des PC-3000 Express Systems und kompatiblen Ersatzteilspendern erfolgreich gesichert.
Ziel der Arbeit ist es, einen zukünftigen Benutzer in die Arbeit mit dem PC-3000 Express System einzuführen. Dabei soll der Arbeitsablauf bei der Untersuchung einer Festplatte fest an den Ablauf einer forensischen Untersuchung gebunden sein. So kann unabhängig vom forensischen Tätigkeitsfeld sichergestellt werden, dass ein Benutzer zukünftig auftretende Probleme von Festplatten effektiv und lösungsorientiert handhaben kann.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

PC	Personalcomputer
IT	Informationstechnik
BSI	Bundesamt für Sicherheit in der Informationstechnik
PCB	Printed Circuit Board/Logikplatine
SATA	Serial Advanced Technology Attachment
bzw.	beziehungsweise
HDD	Hard Disk Drive
CHS	Cylinder Head Sector
LBA	Logical Block Address
BIOS	Basic Input Output System
CMOS	Complementary metal-oxide semiconductor
ROM	Read Only Memory
MB	Megabyte
TB	Terabyte
SMART	Self Monitoring and Reporting Technology
P-List	Permanent/Primary/Production-List
G-List	Growing List
ATA	Advanced Technology Attachment
IDE	Integrated Drive Electronics
PATA	Parallel Advanced Technology Attachment
PIO	Programmed Input Output
ns	Nanosekunden

DMA	Direct Memory Access
bsp.	beispielsweise
SSD	Solid State Drive
FIT	File Information Table
ggf.	gegebenenfalls
RAM	Random Access Memory
SA	Service Area
SAP	Servo Adaptive Parameters
NAND	Nicht Und
SSHD	Solid State Hybrid Drive
FW	Firmware

1 Übersicht

In diesem ersten Kapitel wird zunächst Einleitendes zum Thema erläutert. Anschließend wird die Motivation dieser Arbeit beschrieben sowie die angestrebten Ziele. Die Kapitelübersicht soll einen knappen Überblick für den Aufbau der Arbeit liefern. Im letzten Abschnitt wird die Arbeit thematisch eingeordnet.

1.1 Einleitung

Neben einem kommerziellen Nutzen für Unternehmen zur langfristigen Aufbewahrung von Daten, hat die Festplatte unlängst den Heimanwenderbereich erobert. Am 13.09.1956 wurde damals die erste Festplatte der Welt vorgestellt. Diese kam auf eine Speicherkapazität von knapp 5 Megabyte und brachte rund eine Tonne Gewicht auf die Waage. [14] Ihre anschließende Weiterentwicklung nimmt einen rasanten Verlauf und stellt eines der faszinierendsten Kapitel in der Geschichte des Computers dar. Ab 2007 gelingt es dem Hersteller Hitachi, eine Festplatte mit einer Kapazität von einem Terabyte (TB) auf den Markt zu bringen. Damit hat sich die Kapazität von Festplatten im Laufe der Jahre weit über den Faktor 100.000 gesteigert und ihre Leistung um das Zehntausendfache. [15]

Mit dieser rasanten Entwicklung gingen sowohl optisch als auch technisch viele Änderungen einher. Heute ist die Festplatte etablierter Bestandteil eines jeden Desktop Personalcomputers oder Notebooks und hat damit einer breiten Masse der Bevölkerung dieser Welt, den bezahlbaren Zugang zu einem permanenten, sicheren und schnellen zu Hause für ihre Daten ermöglicht. Dementsprechend blickt die Festplatte auf eine relativ lange und erprobte Geschichte zurück und hat sich einen Ruf von Langlebigkeit und Zuverlässigkeit erarbeitet. Heute wie auch früher nutzen die Menschen Festplatten, um permanent Daten speichern zu können und im digitalisierten Zeitalter des 21. Jahrhunderts damit ihr Leben zu vereinfachen. Der Unterschied zu früher wird, neben rapide anwachsenden Speicherkapazitäten der Festplatten, vor allem darin deutlich, wie viele Daten abgespeichert werden (müssen). „Mit der Verbreitung des PCs (und damit auch von Festplatten) wird der Computer einerseits selber Instrument von Straftaten, anderseits als allgegenwärtiger Speicher der über ihn vollzogenen Aktivitäten aufschlussreiche Quelle und wichtiges Rechercheinstrument bei der Verfolgung von Vergehen.“ [16, S. 659] Deshalb steigt in den letzten Jahrzehnten auch die Zahl von Internet – und Computerkriminalität stark an. Dabei handelt es sich um ein

globales Phänomen, das nicht vor verschlossenen Türen Halt macht und über Ländergrenzen hinweg existiert. Überall dort, wo Menschen im Besitz von Computern, Smartphones und anderen Informationstechnik-Geräten sind, findet auch Internet – und Computerkriminalität statt. In der IT-Forensik sind Festplatten ein essenzieller Bestandteil von Untersuchungen und fallen dabei in den Bereich der Datenträgerforensik. Wenn sich auf einer Festplatte verfahrensrelevante Daten befinden, wird sie dem kriminalistischen Sprachgebrauch nach zum Spurenträger. [17, S. 2] Speziell die IT-Forensik zielt darauf ab, Daten überhaupt erst zugänglich zu machen, sie aufzubereiten und verfahrensrelevante Spuren zu ermitteln, die später in gerichtsverwertbaren Gutachten zur Aufklärung von Straftaten eingesetzt werden können. Auf der Grundlage von Leitfäden für eine forensische Untersuchung beschäftigt sich die vorliegende Arbeit mit Spezialverfahren der Datenrettung von Festplatten.

1.2 Motivation und Zielsetzung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schreibt zum Begriff der Datensammlung folgendes: „Die Erzeugung eines forensischen Datenträgerabbildes bildet als Maßnahme der Datensammlung die Grundlage für die nachfolgenden Abschnitte des forensischen Prozesses, insbesondere der Untersuchung und Analyse.“ [18, S. 235] Da die anfänglich erwähnte Verbreitung sowie Bedeutsamkeit von Festplatten in einer digitalen Welt noch lange Bestand haben wird und auch im IT-forensischen Zusammenhang eine zentrale Bedeutung spielt, setzt diese Arbeit zu Spezialverfahren der Datenrettung genau an diesem Punkt der Datensammlung an. Dabei konzentriert sich die Arbeit vor allem auf Fälle, in denen die Daten von Festplatten nicht nach vordefinierten Mustern gesichert werden können.

Da die Festplatte auf eine lange und erprobte Geschichte zurückblicken kann, existieren schon viele Arbeiten, die sich mit der Festplatte als Datenträger im forensischen Kontext beschäftigen oder im allgemeinen Zusammenhang mit der Datenwiederherstellung stehen. Dem gegenüber steht nun die vorliegende Arbeit zu Festplatten, die mit Hilfe des PC-3000 Express Systems repariert und gesichert werden. In Kombination mit einem forensischen Kontext lässt sich so das Zustandekommen der vorliegenden Arbeit rechtfertigen. Vorige Arbeiten, die ebenfalls das PC-3000 Express System oder ähnliche Systeme nutzten, beschäftigten sich hauptsächlich mit der Manipulation und dem Verstecken von Daten vor forensischen Untersuchungen auf einer Festplatte. Darüber hinaus sind ergiebige und korrekte Veröffentlichungen zu Festplatten durchaus vorhanden, beschäftigen sich im Kern aber aufgrund der Komplexität einer Festplatte meist mit sehr spezifischen Einzelthemen. Deshalb kann diese Arbeit auch als eine Verknüpfung von individuellen und

festplattenspezifischen Themen betrachtet werden. Die Arbeit soll einen zukünftigen Benutzer des PC-3000 Express Systems sehr detailliert durch zwei konkrete Beispiele leiten. Dabei wird er durch einen teils etablierten und teils selbst erstellten Leitfaden unterstützt, der den Rahmen einer forensischen Untersuchung vorgibt und im Vorfeld wertvolle Hinweise zur Untersuchung einer Festplatte liefern kann.

1.3 Kapitelübersicht

Spezialverfahren der Datenrettung sind ein komplexer Prozess. Neben der hier verwendeten Hardware-Software Lösung in Form des PC-3000 Express Professionell Systems ist vor allem Wissen rund um eine Festplatte nötig. Aus diesem Grund liegt dieser Arbeit zuerst ein umfassender Grundlagenteil bei, der von der Festplatte an sich handelt, aber auch die Integration einer Festplatte in ein Computersystem beschreibt und mit der Bedienung einer Festplatte durch PC-3000 Express endet. Bevor eine Festplatte im Rahmen einer forensischen Untersuchung gesichert werden kann, beschreibt diese Arbeit einen forensischen Leitfaden zu Spezialverfahren der Datenrettung. Im forensischen Leitfaden kommen vor allem Anforderungen an eine forensische Untersuchung von Festplatten zum Tragen, als auch die themenspezifische Evaluierung einer Festplatte erst ohne und dann mit Spezialwerkzeugen wie PC-3000 Express. Der anschließende Kern dieser Arbeit setzt sich mit der Durchführung von zwei Beispielen zu Spezialverfahren der Datenrettung auseinander. Davor wird kurz das methodische Vorgehen im Rahmen des Leitfadens erläutert. Nach den Beispielen werden die erhaltenen Ergebnisse präsentiert und im Anschluss daran die vorliegende Arbeit diskutiert und mit einem Fazit sowie Ausblick abgeschlossen.

1.4 Abgrenzung von Spezialverfahren der Datenrettung

Spezialverfahren der Datenrettung wären gedanklich für viele wahrscheinlich gleichbedeutend mit der Datenwiederherstellung. Genau aus diesem Grund soll eine gewisse Abgrenzung stattfinden, wenngleich die Datenwiederherstellung natürlich Teil von Spezialverfahren der Datenrettung ist. Die Wiederherstellung von Daten, auch als Data Recovery bekannt, ist ein Prozess, um verlorengegangene, beschädigte, versehentlich gelöschte oder nicht verfügbare Daten zu rekonstruieren. [19] Diese Art der Definition von Datenwiederherstellung hat einen starken Bezug auf reine Daten. Der Datenbezug bei einem Wiederherstellungsprozess innerhalb der IT-Forensik hat in der Regel natürlich oberste Priorität. Allerdings beginnt die einfachste Form einer Datenwiederherstellung meistens mit dem Wiederherstellen von Daten aus einem Backup. Mit einem gewissen Grundverständnis für einen solchen Prozess ist die Datenwiederherstellung relativ einfach zu bewerkstelligen.

Jedoch lässt sich mit Hilfe des Wiederherstellens aus einem Backup die Abgrenzung gut erklären. Spezialverfahren der Datenrettung sind in den wenigsten bzw. oft gar keinen Fällen dazu in der Lage, auf Backups zurückzugreifen. Gerade die in der vorliegenden Arbeit angewandten Methoden sind dazu bestimmt, Daten einer Festplatte, für die scheinbar kein Backup vorliegt, überhaupt erst wieder zugänglich zu machen. Dabei beziehen sich die Methoden neben kommerziellen und hoch entwickelten Hardware-Software-Lösungen vor allem auch auf physische Eingriffe bei den Festplatten. In Abgrenzung zu einem Backup, dass jeder einfach und bequem von zu Hause aus wiederherstellen kann, sind Spezialverfahren der Datenrettung nicht ohne eine Menge Fachwissen, spezielle Geräte und Techniken durchführbar. Unabhängig von der Einfachheit der Wiederherstellung eines Backups, kann Datenverlust verschiedene Formen annehmen und auch der Prozess einer Datenwiederherstellung wird damit zu einer komplexen Herausforderung. Gewissermaßen bauen die Spezialverfahren der Datenrettung dann auf der Datenwiederherstellung auf und bilden einen Übergang.

2 Grundlagen

Zum besseren Verständnis des in dieser Arbeit angeführten Leitfadens sowie der beiden Beispiele zu Spezialverfahren der Datenrettung, werden in diesem Kapitel einige Grundlagen erläutert. Zunächst wird die Festplatte an sich näher betrachtet, um dann die Integration einer Festplatte in ein Computersystem kennenzulernen und mit der Bedienung einer Festplatte durch PC-3000 Express abzuschließen.

2.1 Aufbau und Funktionen einer Festplatte

Die Festplatte oder auch Hard Disk genannt, ist ein nicht-flüchtiger Speicher in einem Computersystem und stellt damit das wichtigste Speichermedium eines Computers dar. Üblicherweise befindet sich auf einer Festplatte das Betriebssystem, installierte Software und natürlich die Daten, die mit bestimmten Programmen erzeugt werden. „Die richtige Benennung für Festplatte ist eigentlich das Festplattenlaufwerk, da die Festplatte nur in einem entsprechend stabilen und kompakten Gehäuse mit einer speziellen technischen Ausstattung kombiniert und nur so funktionstüchtig ist.“ [20] Die gängigsten Größen von Festplatten sind 2,5 Zoll, die beispielsweise in Notebooks Anwendung finden und 3,5 Zoll, die in Desktop PC´-s eingesetzt werden. Heutzutage sind Festplatten in der Regel mit mehreren Gigabytes oder Terabytes an Speicherplatz ausgestattet.

2.1.1 Logikplatine – Printed Circuit Board (PCB)

Wird eine Festplatte von unten betrachtet, fällt direkt ein Teil der Festplatte auf, der einem Stück grünem Glas ähnelt (siehe Abbildung 1).

Abbildung 1: Festplatte von hinten [1]

Auf diesem befinden sich viele Leitungen, eine Menge Kupfer und zwei Anschlüsse. Der kleinere der Anschlüsse ist der SATA oder Serial AT Attachment-Anschluss und dient im Wesentlichen der Kommunikation mit einem Rechner. Der größere Anschluss versorgt die Festplatte mit Strom. Die Aufgabe des PCB ist es, alle darauf befindlichen elektronischen Komponenten zusammen zu halten und zu verbinden. [2] Das PCB ist die einzige Komponente, die sich außerhalb des eigentlichen Gehäuses befindet. Eine fest verschraubte und solide Metallplatte schützt die sensiblen Komponenten, die Luft und vor allem die Benutzerdaten im Inneren der Festplatte vor Verunreinigungen und Beschädigungen. Aus diesem Grund verfügt jede Festplatte über ein kleines Luftloch, um einen Druckausgleich zwischen der Luft von außerhalb und innerhalb der Festplatte zu gewährleisten. Der Schutz der inneren Komponenten ist deshalb so wichtig, weil vor allem die Köpfe einer Festplatte zwar extrem belastbar, aber dennoch hoch sensibel sind. Kleinste Verschmutzungen auf der Plattenoberfläche könnten dazu führen, dass die Köpfe kaputt gehen oder auf den Plattenoberflächen Kratzer hinterlassen und Daten verloren gehen. Nun zu den wichtigsten Komponenten auf dem PCB. Dafür muss es abgeschraubt und umgedreht werden:

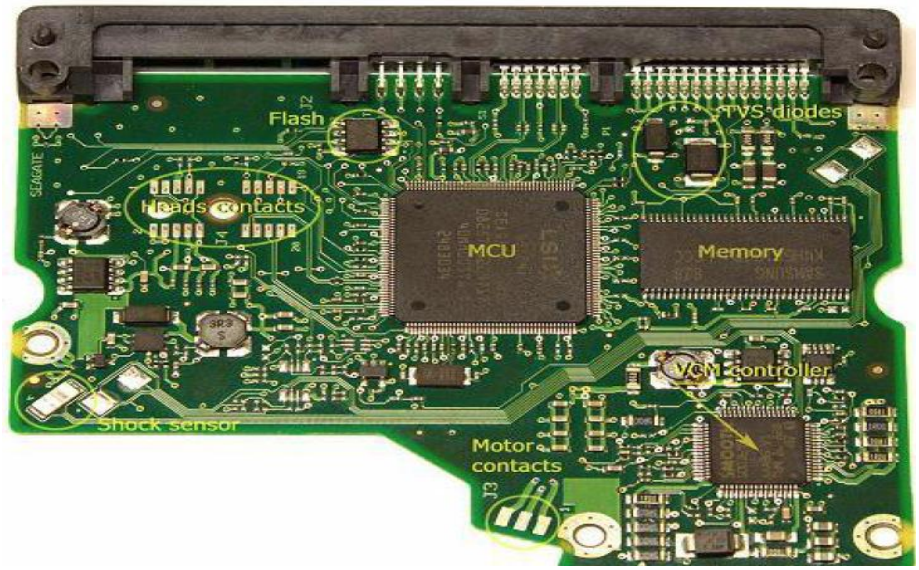


Abbildung 2: Übersicht Bestandteile eines PCB [2]

Der größte Chip auf einem PCB ist der Mikrocontroller (MCU). (siehe Abbildung 2) Er besteht normalerweise aus einem Prozessor, der alle Berechnungen durchführt. Dazu kommt ein Lese -/Schreibkanal, der während eines Leseprozesses analoge Signale der Köpfe in digitale Informationen umwandelt und umgekehrt digitale Informationen in analoge, wenn die Festplatte schreiben soll. [2]

Der zweitgrößte Chip stellt in der Regel einen Speicherchip dar (Memory). (siehe Abbildung 2) Normalerweise definiert die Größe eines Speicherchips auch die Größe seines Cache. Allerdings unterteilt sich der Speicher einmal in Cache Speicher und einen Teil, der bestimmte Module der Firmware des Herstellers enthält. Deshalb ist der Cache meistens etwas kleiner als die Gesamtspeicherkapazität des Chips erwarten lässt. [2]

Der am meisten Strom verbrauchende und gleichzeitig drittgrößte Chip auf dem PCB ist ein sogenannter Spulen-Motor-Controller oder auch Stellmotor-Chip (Voice coil motor-controller). (siehe Abbildung 2) Seine Aufgabe ist einerseits die Rotation der Scheiben durch den Motor zu kontrollieren und andererseits die Bewegung der Arme beziehungsweise Köpfe. [2]

Ein vierter Chip fungiert als Flash Speicher (Flash). (siehe Abbildung 2) Er speichert Teile der Firmware. Sobald die Festplatte mit Strom versorgt wird, lädt der Mikrocontroller den Inhalt des Flash Speichers in den Speicher (Memory) und initialisiert die Festplatte. Manchmal findet sich kein separater Flash Speicher auf dem PCB. Das bedeutet lediglich, dass sich der Inhalt des Flash Speichers im Mikrocontroller befindet. [2]

2.1.2 Aufbau der Kopf – und Platteneinheit

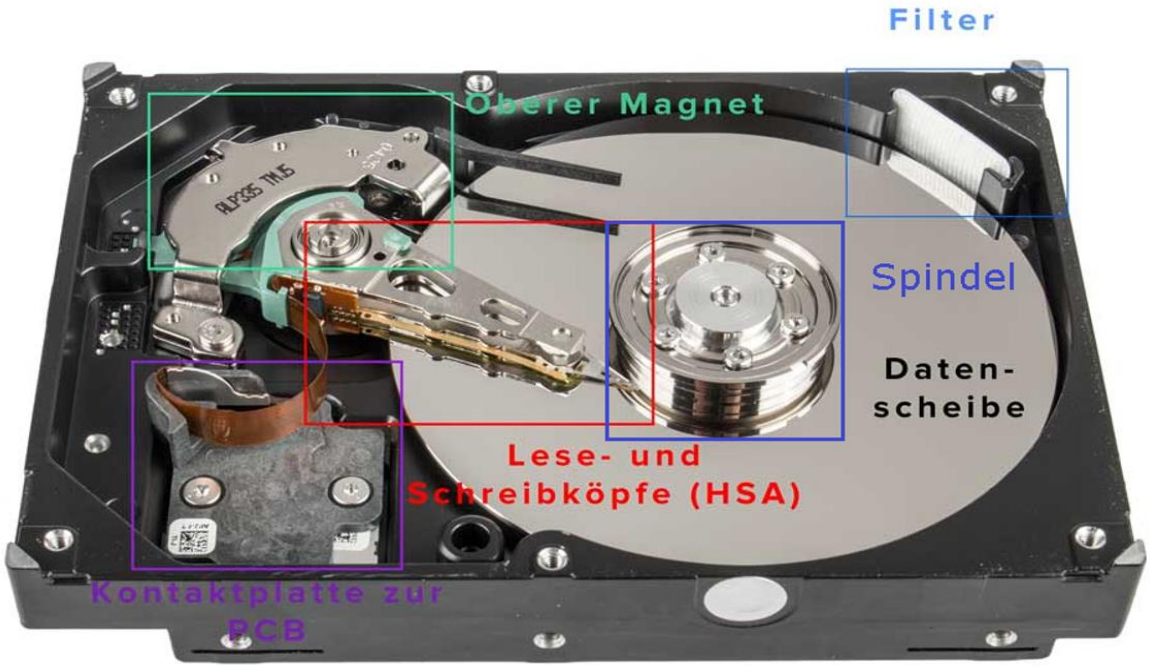


Abbildung 3: Innenleben einer Festplatte [3]

Um an die Kopf - und Platteneinheit heranzukommen, muss die Abdeckung der Festplatte entfernt werden. Das Grundgerüst eines jeden Festplattenlaufwerks bilden die Festplatten (Datenscheiben) selbst. (siehe Abbildung 3) Hierbei handelt es sich um kreisrunde, flache Scheiben, die mit einer speziellen Eisenoxid-Schicht überzogen sind. [21] Diese Beschichtung dient dem Zweck, eine Oberfläche zu schaffen, auf der Daten magnetisch als Eins oder Null oder auch magnetisch nach Norden oder Süden ausgerichtete Bits gespeichert werden. [22] „Die Anzahl der Scheiben richtet sich nach der Kapazität der Festplatte und der Speicherdichte der Scheiben selbst.“ [23] Die Scheiben sind wiederum an einer Spindel befestigt, die von einem Motor angetrieben wird, der je nach Modell Drehzahlen zwischen 4200 bis 15000 Umdrehungen pro Minute erreicht. [23] Umso schneller die Festplatte dreht, desto schneller findet der sogenannte Schreib-/Lesekopf die Daten auf der Festplatte. Zwischen den Platten ist ein Abstandsring, welcher einerseits die Platten voneinander trennt und andererseits den Köpfen genug Platz zum Arbeiten gibt. [9] Während sich die Platte dreht, befindet sich ein Kopf auf jeder Seite der Platte, der entweder Daten lesen oder schreiben kann. [24] Das Besondere dabei ist, dass durch die Rotation der Scheibe ein Luftstrom zwischen dem Kopf und der Plattenoberfläche entsteht, sodass der entsprechende Kopf wenige Nanometer über der Scheibe schwebt. Dabei umgibt der Luftstrom alle Kopfteile über der Scheibe wie die Flügel eines Flugzeugs, wodurch sich der Luftstrom kontrollieren lässt. [12] Da die Luft im Inneren des Gehäuses leicht durch Staubpartikel

verschmutzt werden könnte und dadurch den Köpfen gefährlich wird, werden in den Festplatten auch Filter eingesetzt, die die Luft sauber und trocken halten. Der Kopf befindet sich an einer Aufhängung am Ende eines Arms, der Teil der sogenannten Kopfteilbaugruppe (head stack assembly - HSA) ist und die Arme bewegen sich in einem bestimmten Radius über der Platte hin und her. Dabei lesen und schreiben die Köpfe fest definierte Spuren, die kreisartig auf der Scheibe angeordnet sind. Die Spuren sind inzwischen so schmal, dass die Hersteller heutzutage mehrere hunderttausend dieser Spuren auf wenigen Zentimetern Platz unterbringen können. Während die Köpfe arbeiten, werden sie durch Positionsdaten, (Servorinformationen) die während der Herstellung geschrieben werden, mittig über der Spur gehalten. [12] Am Ende des Arms befindet sich ein Verstärker (Preamp) der die Signale der Köpfe verstärkt. Schließlich ist der Arm über ein flexibles Flachbandkabel mit der Armelektronik verbunden und diese wiederum mit der Logikplatine der Festplatte. Darüber hinaus ist der Arm mit einer Spule und einem Drehpunkt verbunden, die zusammen eine Einheit bilden. Spule und Drehpunkt werden von zwei sehr starken Magneten jeweils unter und über der Einheit in Position gehalten. Damit der Arm sich nicht über einen bestimmten Radius hinwegbewegt, sind zusätzlich kleine Stopper eingebaut, die nur einen bestimmten Aktionsradius zulassen.

2.1.3 Funktionen des Schreib/Lesekopfes

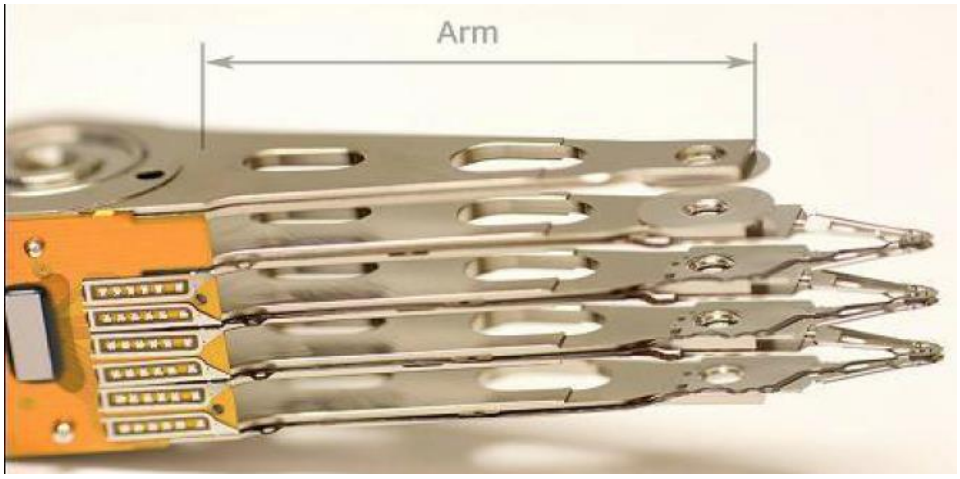


Abbildung 4: Arm mit Aufhängung der Köpfe und Drehpunkt (links oben) [9]

Es ist nun bekannt, dass sich die Köpfe an einer Aufhängung am Ende eines Armes befinden (siehe Abbildung 4) und über der Platte schweben, wenn sie sich dreht. Allgemein bekannt ist auch, dass Elektrizität und Magnetismus zusammen existieren und wenn Strom durch einen Draht fließt, ein orthogonales Magnetfeld entsteht. [12] „Elektromagnetische Effekte wie Induktion oder magnetische Flusswechsel entstehen durch die relative

Bewegung zwischen elektrischen und magnetischen Komponenten. Dies geschieht am einfachsten mit einer rotierenden Bewegung, wobei gilt: Je schneller, desto effektiver. Denn je schneller eine magnetische Flussänderung beispielsweise in einer Spule erfolgt, desto größer der induzierte Strom und damit auch das Signal.“ [25] „Schreib-/Leseköpfe bestehen aus ringförmigen Elektromagneten mit einem Weicheisenkern und einer umgebenden Spule.“ [25] Dazu kommt jetzt am Ende der Köpfe ein Wandler, der zusammen mit den beiden Köpfen ein grob geformtes Dreieck ergibt, dass man sich als die Größe eines Bits vorstellen kann. (siehe Abbildung 5) Ein Wandler hat grundsätzlich die Aufgabe, eine Energieart in eine andere umzuwandeln. Bei einem Schreibvorgang wird der Bitfluss (siehe Abbildung 5) durch den rechten Pol des Schreibkopfes fokussiert und das entsprechende Medium darunter magnetisiert. Dabei bedeutet eine Null zu schreiben, keine Änderung des magnetischen Vektors und eine Eins eine Vektoränderung. [12]

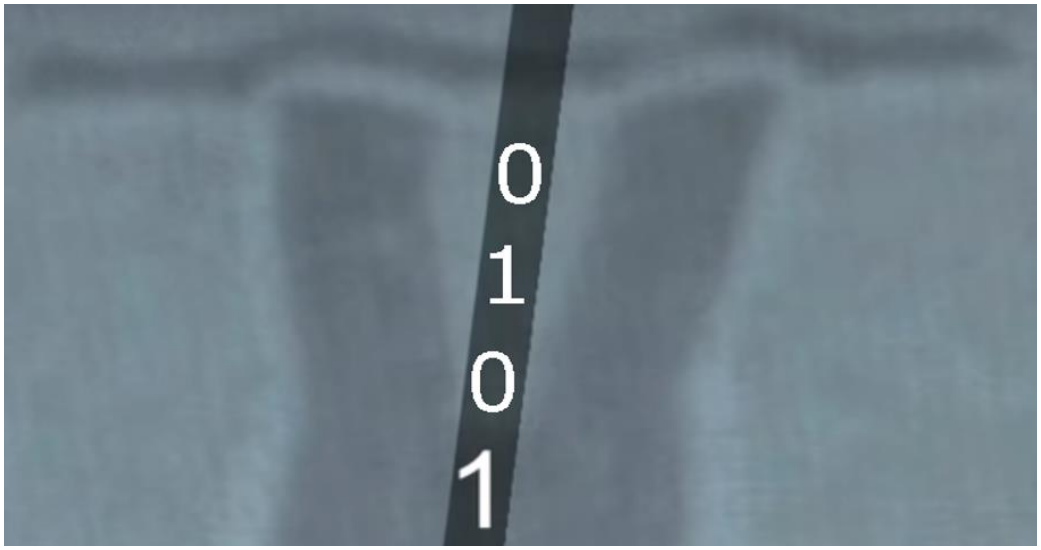


Abbildung 5: Bitfluss durch Schreib/Lesekopf [12]

Die Eigenschaften von Elektrizität und Magnetismus macht sich auch die Spule am Arm zunutze, die sich zwischen zwei Magneten befindet. Die treibende Kraft des Stroms oder umgekehrt des Magnetismus zwingt das hintere Ende der Spule, sich in die eine oder andere Richtung zu bewegen. Wenn die Festplatte ausgeschaltet wird, schwenkt der Arm ab und die Köpfe gelangen zu einer Parkposition, damit sie sich nicht mehr über einer der Scheiben befinden. Wird die Festplatte wieder eingeschaltet und der Benutzer möchte sich zum Beispiel ein Bild ansehen oder abspeichern, dann schwenken die Arme wieder über die Platte und fliegen in einem bestimmten Radius über den Spuren. Dieser Radius wird festgelegt, indem dem Laufwerk eine Adresse zum Ziel gegeben wird. Das ist dann im Beispiel genau die Position, die das Bild oder einen Teil des Bildes enthält, bei dem der Benutzer veranlasst hat, es zu speichern oder anzuzeigen. Bei einem Lesevorgang erkennt

der Wandler für einen bestimmten Bereich die Richtung des Magnetismus und kann daraus schließen, ob es sich um eine Eins oder eine Null handelt, welche wieder jeweils ein Bit darstellen. Der Kopf nimmt dann eine bestimmte Folge dieser Bits auf und überträgt sie elektrisch nach oben über einen Kanal zum Signalverstärker und anschließend werden die Daten über den Mikrocontroller des PCB so rekonstruiert, dass der Benutzer sie wieder als Bild erkennt. [12]

2.1.4 Organisation der Daten auf einer Festplatte

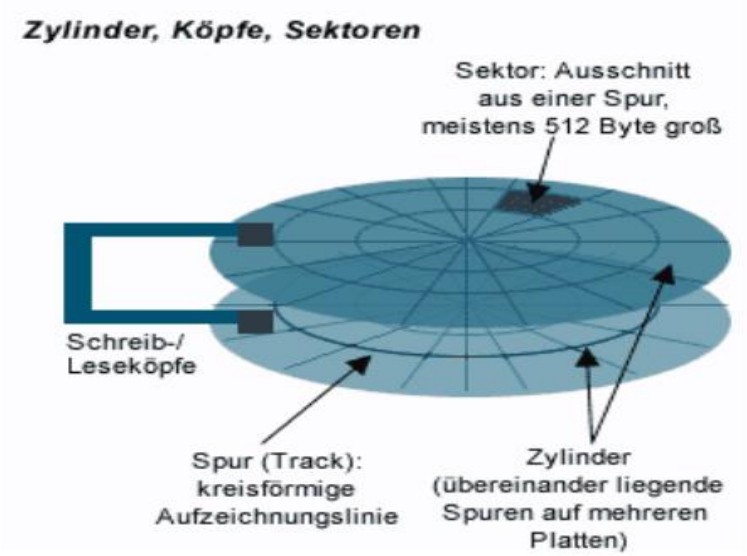


Abbildung 6: Einteilung der Daten auf einer Festplatte [4]

Das Grundprinzip der Organisation von Daten auf einer Festplatte ähnelt dem eines Koordinatensystems, indem über bestimmte Aufteilungen durch verschiedene Parameter eine konkrete Stelle genau beschrieben werden kann. (siehe Abbildung 6) Wie bereits aus Kapitel 2.1.2 hervorgegangen ist, setzt sich eine Platte aus mehreren Spuren zusammen. Bevor eine Festplatte zum Endbenutzer gelangt, wird sie zunächst vom Hersteller einer sogenannten Low-Level Formatierung unterzogen. Dabei wird jede Platte von außen nach innen in gleichmäßige konzentrische Kreise, auch Spur genannt, unterteilt. (siehe Abbildung 6) Innerhalb einer solchen Spur wird eine weitere Unterteilung in einzelne Kreisabschnitte vorgenommen, die als Sektoren bezeichnet werden. (siehe Abbildung 6) Ein Sektor ist ein physikalischer Bereich auf der Platte. Darüber hinaus existieren in Abhängigkeit eines Dateisystems noch die sogenannten Blöcke. Ein Block enthält zusätzliche Metadaten-Informationen und stellt damit eine logische Verwaltungseinheit dar. [26] Wichtig bei der Unterteilung einer Spur in Sektoren ist, dass jeder Sektor die gleiche Größe aufweist. Mehrere zusammenhängende Sektoren werden als Cluster bezeichnet. Das hat den Vorteil, dass

dadurch das System weiß, dass ein bestimmtes Cluster Daten enthält und somit der Platz auf der Platte belegt ist und nicht überschrieben werden darf. Dazu kommen jetzt noch die sogenannten Zylinder. Wenn eine Festplatte mehrere Platten benutzt, dann existiert die gleiche Spur über mehrere Platten hinweg und wird als Zylinder bezeichnet. (siehe Abbildung 6) [20, 27, 28]

Die effektivste Methode, Daten zu speichern wäre, die Daten in nebeneinander liegende Sektoren bzw. ein zusammenhängendes Cluster zu schreiben. Da Dateien aber stets unterschiedlich groß sind, kann das für die Zuweisung von Dateien verantwortliche Dateisystem nicht immer garantieren, dass eine Datei zusammenhängend abgespeichert wird. Das bedeutet, dass sich Teile einer Datei oftmals über verschiedene Bereiche einer Platte, über einen Zylinder oder einen anderen abweichenden Zylinder erstrecken können. Eine solche Datei würde man als fragmentiert bezeichnen. [27] Hierbei wichtig zu erwähnen ist, dass sich „die mehreren Arme eines Laufwerks zusammen im Gleichschritt bewegen und die Köpfe auf allen Platten gleichzeitig an derselben relativen Position befinden.“ [29] Daraus ergibt sich, dass die Zugriffszeit für eine fragmentierte Datei deutlich höher ist, da für die einzelnen Fragmente der Datei auch jedes Mal die Arme sowie die Köpfe neu positioniert werden müssen. Lange Zeit galt für einen Sektor die Größe von 512 Byte als Standard. In modernen HDD´s wird allerdings seit einigen Jahren vermehrt auf eine Sektorgröße von 4096 (4k) Byte gesetzt. Eine Sektorgröße von 4k Byte weist einen größeren zusammenhängenden Datenbereich auf und besitzt für diesen einen Datenbereich unter anderem zusätzliche Wiederherstellungsinformationen. Für eine Sektorgröße von 512 Byte müssten, im Vergleich zu 4k Byte, acht Sektoren mit jeweils individuellen Wiederherstellungsinformationen gespeichert werden. Damit sparen die Hersteller bei der Verwendung von 4k Byte Sektorgröße Platz und die Kapazität von Festplatten lässt sich dadurch steigern. Sowohl 512 Byte als auch 4096 Byte sind Potenzen der Zahl Zwei. Dies ist auf die beiden Grundzustände zurückzuführen, die eine Festplatte eigentlich speichert, Eins und Null oder vereinfacht „an“ und „aus.“ [27] Das anfänglich erwähnte Koordinatensystem fand früher in der sogenannten CHS – also Cylinder, Head, Sector – Adressierung Verwendung. Damit war es möglich, jeden Sektor einer Festplatte eindeutig zu adressieren. Allerdings brachte die CHS-Adressierung Einschränkungen durch beschränkte Adressräume mit sich und war bei einer maximalen Kapazität von knapp acht GB ausgereizt. [30] Dafür wurde dann die LBA – Logical Block Addressing – Adressierung eingeführt. Hierbei wird die Festplatte als eine lange Liste von Blöcken aufgefasst, bei der jeder Block von Null beginnend durchnummeriert ist. Die physikalische Adresse eines Blocks bleibt weiterhin eine Kombination aus entsprechendem Zylinder, einer bestimmten Spur auf einem bestimmten Kopf und der Sektornummer innerhalb der Spur. Ausschließlich die Festplattenhardware mit einem speziell

dafür konzipierten Chip weiß, welchem Sektor welche LBA-Werte zugehörig sind. Demnach ordnet der Chip den physikalischen Adressen eine logische Blocknummer zu, die nach außen hin zu anderen Geräten kommuniziert wird. [31] Vorteil dieser logischen Blockadressierung ist vor allem, dass während dem Betrieb defekte Sektoren durch vom Hersteller festgelegte Zusatzsektoren (auch Spare Sektoren oder Spare Bereich genannt) ausgetauscht werden können. Die Koordination von defekten Sektoren und Zusatzsektoren und vielen weiteren Analyse - und Wartungsaufgaben einer Festplatte übernimmt die Firmware im Service Area der Hersteller, die im nächsten Kapitel näher betrachtet wird.

2.2 Firmware und Service Daten einer Festplatte

Auf jeder Festplatte, die in einem PC, Laptop oder Server verwendet wird, wurde vor der Auslieferung im Werk Firmware installiert. [32] Firmware ist eine Art Software oder auch Programm, das in die Hardware der Festplatte integriert ist und den korrekten internen Betrieb der Festplatte steuert. Sie ermöglicht unter anderem die Interaktion mit einem Host-Computer. (Betriebssystem der Festplatte) [33] Allerdings befindet sich die Firmware in Bereichen, die für ein Betriebssystem oder allgemein den Benutzer nicht zugänglich sind. Firmware enthält die grundlegendsten Parameter der Hardware und Software einer Festplatte und bietet damit vor allem anderen den Zugang auf niedrigster Ebene zu einer Festplatte. [34]

2.2.1 Allgemeines zur Firmware

Um das Prinzip der Firmware zu vereinfachen, kann sich die Festplatte wie ein Computer vorgestellt werden und die Firmware entspricht dabei dem Betriebssystem des Laufwerks. [34] Rein technisch gesehen wird immer ein Computer-zu-Laufwerk-Dialog mit Basic Input Output System (BIOS) Tests gestartet und sobald das Laufwerk im Complementary metal-oxide semiconductor (CMOS = physikalischer Träger des BIOS) des Motherboards erkannt wird, ist die Festplatte als Systemkomponente bereit, ihre Funktion zu erfüllen. Wenn aber aus irgendeinem Grund der interne Prozess der Laufwerksinitialisierung durch die Firmware gestört ist, kann das CMOS die ausgefallene Festplatte nicht mehr identifizieren. Der Computer würde ein solches Laufwerk dann überspringen und/oder gibt eine Fehlermeldung aus. [5]

Gleichermaßen gilt für die Festplatte, dass ihre Funktionalität eingeschränkt ist oder sie funktioniert gar nicht mehr. Es kommt sehr häufig vor, dass die Firmware einer Festplatte fehlerhaft ist und sie nicht mehr funktioniert. Würde man den Fehler in der Firmware

beheben, könnte man die Festplatte wieder ohne jegliche Verluste betreiben. Ohne Weiteres lässt sich jedoch nicht feststellen, ob die Firmware einer Festplatte fehlerhaft oder beschädigt ist. Jedoch gibt es einige Anzeichen, die darauf hindeuten können, dass eine Festplatte Firmware-Probleme hat:

- Laufwerk wird nicht initialisiert

- Klickgeräusche

- Laufwerk reagiert langsam oder läuft nicht richtig

- Laufwerk wird vom Computer nicht erkannt

- Ungenaue Laufwerksmodellnummer oder Laufwerkskapazität [35, 36]

2.2.2 Die Rolle der Firmware in einer Festplatte

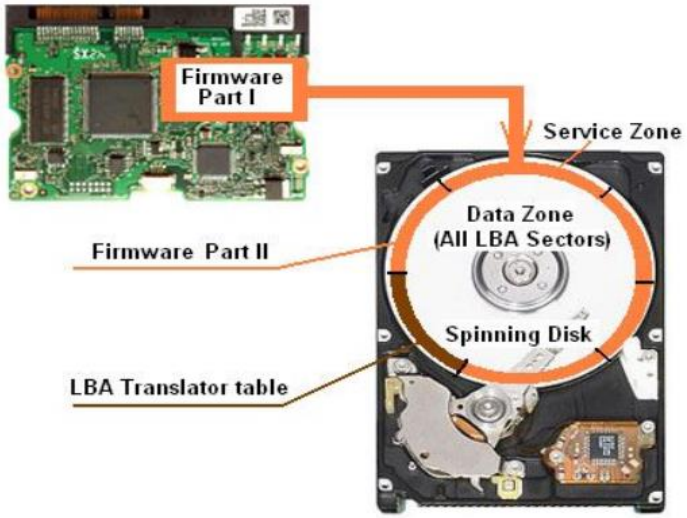


Abbildung 7: Positionen der Firmware in einer Festplatte [5]

In der Regel gibt es bei einer Festplatte zwei Anlaufstellen für die Firmware. Einerseits existiert ein kleiner, aber sehr wichtiger Teil der Firmware auf dem PCB, der in den integrierten Speicherchip in Form von Read Only Memory (ROM) geschrieben ist. Der andere größere Teil des Firmware Programms befindet sich auf speziellen Servicespuren der Platten, der auch als Systembereich oder Servicebereich bezeichnet wird. (SA) (siehe Abbildung 7) [5] Die Größe der Bereiche die Firmware enthalten variiert stark. Dabei kommt es maßgeblich darauf an, von welchem Hersteller die Festplatte ist, welcher Unterteilung in Form einer sog. Familie (Herstellungsserie) sie zugeordnet ist und welche Kapazität und Firmware-Version die Festplatte hat. Zum Beispiel ein WD2500KS-00MJB0-Laufwerk

(Western-Digital, Hawk-Familie, 250 Gigabyte, Firmware Version 02AEC) hat zwei Kopien seiner Servicebereichsmodule (auf Plattenoberflächen der Köpfe Null und Eins) zugeordnet, die jeweils etwa 6 MByte groß sind. Die Größe des reservierten Bereichs auf jeder Oberfläche beträgt ungefähr 23 MByte. Daraus ergibt sich bei sechs Flächen des Laufwerks (Köpfe Null bis Fünf) ein insgesamt reservierter Bereich von 138 MByte, von denen zwölf MByte (8,7 Prozent) für die Servicedaten belegt sind. Im Vergleich dazu hat ein WD10EACS-00ZJB0-Laufwerk (Western-Digital, Hulk-Familie, 1 TB) zwei Kopien seiner Servicebereichsmodule, jedes ungefähr 26 MByte groß. Die Größe des reservierten Bereichs auf jeder Oberfläche beträgt ungefähr 56 MByte und ergibt bei acht Flächen (Köpfe Null bis Sieben) einen insgesamt reservierten Bereich von knapp 450 MByte, von denen 52 MByte (11,5 Prozent) für die Servicedaten verwendet werden. [37]

Wenn die Festplatte eingeschaltet wird, startet der kleine Teil der Firmware auf dem PCB den gesamten Prozess des Bootens der Festplatte. Der Bootprozess sendet den Befehl, den Motor einzuschalten und die Köpfe über die sich drehende Oberfläche zu bewegen, um die Servoinformationen zu erfassen und die Geschwindigkeit anzupassen. Anschließend beginnt das Laden des Mikrocodes aus der Servicezone in den Speicher des Laufwerks. Dieser geladene Code von den Platten muss mit dem Firmware-Code von der Platine übereinstimmen. Andernfalls wird die Integrität des Softwaresystems des gesamten Laufwerks verletzt. Wenn beim Laden des gesamten Mikrocodes (auf der Platine oder auf der Festplatte) etwas schief geht, startet das Laufwerk nicht normal. Die Festplatte kann ihren Motor stoppen oder anfangen zu klicken oder einfach einfrieren, das heißt nicht mehr auf Befehle von außen zu reagieren. [5] Wenn der Mikrocode alle Service-Befehle fehlerfrei ausführt und der Startvorgang des Laufwerks alle Selbsttest- und Initialisierungsvorgänge besteht, ist die Festplatte bereit, Daten zu lesen und zu schreiben und in einer universellen digitalen Sprache mit anderen Computerkomponenten, Betriebssystem und Benutzersoftware zu kommunizieren. [5]

2.2.3 Spezielle Firmware Funktionen

Firmware besteht aus einer Gruppe von Modulen, die Daten enthalten, die für bestimmte Funktionen der Festplatte verantwortlich sind. [36] Dabei sind die Module nach Prioritäten von A (hoch) bis D (niedrig) sowie unbenannt (nicht relevant, unpriorisiert) eingestuft. Wird ein Modul der Priorität D oder unbenannt beschädigt, so kann man grundsätzlich davon ausgehen, dass die Festplatte ohne dieses Modul weiterhin funktioniert. Ein beschädigtes Modul der Priorität B oder sogar A würde hingegen dafür sorgen, dass die Festplatte Fehler liefert oder nicht mehr funktioniert. Einige der Module sind auch dafür vorgesehen, andere

Module zu reparieren, wenn sie beschädigt sind. [36] Um einzelne Module wiederherzustellen, ist es möglich, von einer intakten Festplatte der gleichen Familie Einträge einzelner Module zu sichern und damit defekte Module der anderen Festplatte zu ersetzen.

Festplatten-Firmware im Allgemeinen enthält Folgendes:

Servoinformationen, Low-Level Formatinformationen, residenter Mikrocode, Tuning-Parameter, SECU (Sicherheitssystem-Module), Fehlertabelle, Festplattenmodell, Seriennummer, Kapazität, Hersteller und Produktionsdatum, Fehlerprotokoll, SMART-Tabelle und vieles mehr. [34, 38]

Im normalen Betrieb führt die Firmware im Hintergrund eine Reihe von Schlüsselfunktionen aus. Eine davon ist S.M.A.R.T, die „Self Monitoring Analysis and Reporting Technology." Dabei wird eine Reihe von herstellerabhängigen Kriterien protokolliert und überwacht. Diese dürfen einen bestimmten Schwellenwert nicht überschreiten, damit die Festplatte innerhalb bestimmter Parameter reibungslos arbeiten kann. Zu den Werten zählen unter anderem Lesefehler, Suchfehler, Betriebstemperatur und die Betriebszeit des Laufwerks. Diese Art der Selbstüberwachung der Festplatte dient vor allem dazu, einen möglichen Laufwerksausfall vorhersagen zu können. [33, 38]

Die Firmware ist auch für die Überwachung der Fehlerkontrolle verantwortlich. Wenn eine Festplatte produziert wird, existieren bereits Sektoren auf dem Laufwerk, die nicht verwendet werden können. Im Allgemeinen existieren zwei Fehlertabellen auf einer Festplatte. Beide Tabellen werden zum Verzeichnen der defekten Sektoren der Festplatte verwendet und verhindern, dass die Festplatte fehlerhafte Sektoren benutzt. [34] Fehler, die zum Zeitpunkt der Produktion entstehen, werden in der P-Liste (P=Permanent/Primary/Production) aufgezeichnet. Nachdem die Festplatte ausgeliefert wurde, sollten sich die Werte innerhalb der P-Liste nicht mehr ändern. Mit zunehmendem Alter und Betrieb einer Festplatte entsteht Verschleiß, der dazu führt, dass weitere fehlerhafte Sektoren entstehen. Die G-Liste (G=Growing=Wachstum) ist dafür verantwortlich alle fehlerhaften Sektoren aufzunehmen, die noch nicht in der P-Liste enthalten sind. [34, 39]

Wird ein fehlerhafter Sektor in die G-Liste aufgenommen, dann wird dieser Sektor einem Ersatzsektor aus dem reservierten Bereich zugeordnet. Eine sogenannte Alt-List (Name herstellerabhängig) enthält die Einträge für die Neuadressierung von defekten Sektoren aus dem Spare-Bereich. Alle Vorgänge werden transparent von der Festplatten-Firmware abgewickelt und treten „unterhalb" der Betriebssystemebene auf, ohne dabei den Laufwerkszugriff zu verlangsamen. Wenn die fehlerhaften Sektoren bei der Auslieferung einer

Festplatte ab Werk dokumentiert wurden und die Fehlertabellen implementiert sind, wird darauf basierend der sogenannte Translator in einem eigenen Modul implementiert. Dieser übernimmt dann fortan das automatische Fehlermanagement basierend auf den Fehlertabellen. [34, 39]

Abschließend lässt sich festhalten, dass die Firmware ein bewusst schwer zugänglicher Teil einer Festplatte ist. Die Firmware sorgt für den normalen und fehlerfreien Betrieb einer Festplatte. Etwaige Firmware-Fehler stellen eine große Herausforderung dar. Die Fähigkeit solche Fehler zu beheben, verlangt häufig eine umfangreiche Bibliothek an Firmware/Spender-Laufwerken zum Vergleich und zum Austausch ausgefallener mechanischer Teile, sowie fundiertes Wissen über den Aufbau und die Funktionen von Festplatten und spezielle Hardware und Software zur Wiederherstellung. [39]

2.3 Schnittstelle einer Festplatte

Die Art der Verbindung zwischen einer Festplatte und einem Computersystem (Motherboard und Hauptprozessor) ist immer durch einen bestimmten Standard definiert. [40] Einen solchen Standard stellt das Advanced Technology Attachment, kurz ATA dar. Dabei handelt es sich um einen US-amerikanischen Industriestandard, der durch die unabhängige und internationale Zusammenarbeit von verschiedenen Komitees (bsp. T10 für SCSI und T13 für ATA) sowie von führenden Computersystem – und Massenspeicher-Herstellern entstanden ist und stetig weiterentwickelt wird und wurde. [41]

2.3.1 Einordnung IDE, ATA, PATA und SATA

ATA stellt ein Signalprotokoll dar und war in seinen ersten Ausführungen für den parallelen IDE-Bus (Integrated Drive Electronics) und die dazugehörigen IDE-Festplatten bestimmt. Eigentlich war IDE die erste Ausführung von ATA (ATA-1), bis ATA als einheitlicher Standard übernommen wurde. „Das Signalprotokoll definiert eine Menge technischer Eigenschaften von Speichergeräten. Darüber hinaus können Hersteller auch eigene Eigenschaften definieren.“ [42] Jede Version von ATA spezifizierte ein Protokoll auf Datenblockebene, eine parallele elektrische Schnittstelle und eine physikalische Schnittstelle. [43] Die erste in den 80er Jahren veröffentlichte Version von ATA, ATA-1, erreichte eine Datentransferrate von 16,6 MB/s. Unter ATA-2 wurde dann das inzwischen überall verbreitete LBA-Verfahren eingeführt und ATA-3 brachte schließlich erweiterte Sicherheitsfunktionen sowie Diagnosefunktionen in Form von SMART. Die aktuellste Version stellt inzwischen ATA-8 dar. [44] Wie bereits erwähnt, galt das Protokoll früher immer für Bussysteme mit parallel geführten

Signalleitungen. Da allerdings das Verlangen nach höheren Übertragungsgeschwindigkeiten bis heute noch kein Ende nimmt, ergaben sich für die parallele Datenübertragung technische Schwierigkeiten, die bis zu ihrem Maximum von knapp 130 MB/s ausgereizt waren. [45] Daraufhin mussten die Hersteller reagieren und entwickelten den bis heute fest etablierten SATA, also den Serial ATA Standard. Um in dieser Übergangsphase während der Jahrtausendwende den alten Standard vom Neuen zu unterscheiden, wurde PATA, also Parallel ATA Standard als Bezeichnung für die alte Version der Schnittstelle verwendet.

Die größte optische Veränderung die SATA mit sich brachte, war das Schrumpfen des Datenkabels von 40 Leitungen bei PATA auf nun 7 Leitungen bei SATA. (siehe Abbildung 8) Dabei dient jeweils ein Adernpaar dieser Leitungen der Datenübertragung, ein zweites dem Datenempfang und drei Leitungen dem Masseanschluss. Vorteile gegenüber PATA waren also vor allem schmalere Kabel und damit auch Kosteneinsparungen bei der Herstellung, Hot-Swapping (also der Austausch von Festplatten im laufenden Betrieb) und schnellere Datentransfers durch höhere Signalraten. Außerdem behinderten die sperrigen Flachbandkabel von PATA Laufwerken häufig den Luftstrom im Gehäuse. (siehe Abbildung 8) [40, 41] Die Weiterentwicklung von SATA, SATA 6G, unterstützt heutzutage eine Schreibgeschwindigkeit von fast 500 MB/s bei herkömmlichen Festplatten. [44]

Abbildung 8: PATA (links) und SATA (rechts) Anschlüsse [6]

2.3.2 Aufbau und Integration der ATA Schnittstelle

Um zu verstehen, wie sich ein ATA Kommando auf eine Festplatte auswirkt, sollte der grundlegende Aufbau einer entsprechenden Prozesskette bekannt sein. Angenommen ein Benutzer führt einen Dateizugriff über ein Anwendungsprogramm aus, dann ruft dieses das Betriebssystem auf den Plan. Das Betriebssystem wiederum greift dann auf entsprechende Gerätetreiber und eventuell auf das BIOS zurück. Bis zu diesem Punkt befindet sich die Prozesskette noch auf Software-Ebene. Die entsprechenden Gerätetreiber und das BIOS

greifen nun direkt auf die Hardware zu. Die Schnittstelle zwischen Software und Hardware stellt dabei ein standardisierter ATA-Registersatz, manchmal auch als ATA Task File bezeichnet, dar. Im Falle der Festplatte ist der ATA-Registersatz direkt mit der Laufwerkselektronik verbunden. Um auf diesen Registersatz zuzugreifen, benutzt der Host einen zentral gesteuerten Ein – und Ausgabe - Bus, der auch als ATA-Kanal bezeichnet wird. Da SATA eine Punkt-zu-Punkt-Schnittstelle darstellt, ist an einen Kanal auch nur ein Gerät angeschlossen. [46]

Der eben erwähnte Host im System wird durch zwei Komponenten verkörpert. Einerseits den Prozessor und andererseits einen speziellen Hostadapter, der sich entweder direkt auf dem Motherboard befindet oder durch eine Steckkarte angeschlossen ist. Im Hostadapter befindet sich dann eine Kopie des Registersatzes, auf die wiederum der Prozessor zugreifen kann. Um die Registerinhalte zwischen Hostadapter und angeschlossenem Gerät (also Festplatte) immer aktuell zu halten, findet ein extrem schneller bitserieller Austausch durch die Schnittstelle statt. Damit der Hauptprozessor entlastet wird, besteht eine Arbeitsteilung zwischen Prozessor und Hostadapter. Dafür existieren verschiedene Betriebsarten. Die erste Betriebsart, PIO (Programmed Input/Output), ist im Zusammenhang mit dem Legacy Mode bekannt, denn alle Hostadapter sind anfänglich auf den Legacy Mode eingestellt. Im PIO-Modus übernimmt der Prozessor alle Aufgaben selbst. Mit programmseitigen Ein – und Ausgabe - Zugriffen überträgt er Kommandos, Daten und Zustandsmeldungen. Der Hostadapter wirkt dabei lediglich unterstützend und übernimmt die Adressdecodierung und hat die Aufgabe, „das jeweils gewählte PIO-Zeitraster des ATA-Interfaces zu unterstützen." [46, S. 10] Die PIO Betriebsarten gibt es in den Modi PIO Mode 0 bis 4. Im PIO Mode 1 ist eine maximale Datenrate von 3,33 MB/s möglich und die minimale Zykluszeit beträgt 600 Nanosekunden (ns). Im PIO Mode 4 ist eine maximale Datenrate von 16,67 MB/s möglich und die minimale Zykluszeit beträgt 120 ns. Die einzelnen Modi unterscheiden sich also in der maximalen Datenrate und der Spezifikation der minimalen Zykluszeit, wobei in jedem Zyklus 2 Bytes übertragen werden. Die 2 Byte ergeben wiederum 16 Bit und sind darauf zurückzuführen, dass PATA anfänglich eine maximale Busbreite von 16 Bit zur Verfügung hatte. [46]

Die zweite Betriebsart ist der DMA-Modus (Direct Memory Access). Hierbei sendet der Prozessor ausschließlich Kommandos und Zustandsmeldungen und die eigentliche Datenübertragung wird vom Hostadapter autonom ausgeführt. Der DMA Modus dient ausschließlich der Datenübertragung. Im Single Word DMA Mode 2 (veraltet) wird ein 16 Bit Wort übertragen und erreicht so eine minimale Zykluszeit von 240 ns und eine maximale Datenrate von 8,33 MB/s. Im Multiword DMA Mode 2 werden mehrere 16 Bit Worte

aufeinanderfolgend übertragen und erreicht damit eine minimale Zykluszeit von 120 ns und eine maximale Datenrate von 16,67 MB/s. Mit der Einführung von neuartigen Signalprotokollen konnte die Datenübertragung anhand von Ultra-DMA bzw. Ultra-ATA nochmal deutlich gesteigert werden. Inzwischen unterstützt Ultra DMA Mode 6 (Ultra DMA/133) eine minimale Zykluszeit von 30 ns und eine maximale Datenrate von 133 MB/s. [46]

2.3.3 Umsetzung eines ATA Kommandos

Wie bereits erwähnt, basiert ATA auf einem US-amerikanischen Industriestandard namens ANSI, des Amercian National Standards Institute. Das für ANSI zuständige Gremium ist wiederum das Technische Komitee T13 vom Standardisierungskomitee NCITS, also International Committee for Information Technology Standards. Das technische Komitee T13 veröffentlicht seither unter anderem das Architekturmodell sowie das Kommando Set der verschiedenen ATA Versionen.

Aus der Webseite vom T13 Komitee geht hervor, dass die aktuellste Publikation zu den ATA Kommandos am 23.07.2015 in Form von ATA/ATAPI Command Set – 4 veröffentlicht wurde. [47] Unter Punkt 7.12 geht es um den „Identify Device (Identifikationsdaten des Laufwerks) – EHh, PIO Data-In“ Befehl. Hierbei geht es um eines der grundlegendsten Kommandos einer Festplatte, das im sogenannten „General feature set“ enthalten ist. Das „General feature set“ stellt die Basis für alle ATA Geräte dar, die diesen Standard nutzen und enthält zudem den Befehl zur Erhebung von Diagnosedaten und über „Set Features“ können alle weiteren zusätzlichen Befehle über die das Kommando Set verfügt integriert werden. Identify Device stellt ein 28 Bit Kommando für ATA Geräte dar. Es spezifiziert, dass ein Gerät einen 512 Byte großen Datenblock an den Host senden soll. Darüber hinaus ist genaustens geregelt, wie der Befehl unter bestimmten Bedingungen oder bei Fehlern reagiert und welche Eingaben erfüllt werden müssen, um eine entsprechende Ausgabe zu erhalten. Um den Rahmen der Abhandlung an dieser Stelle nicht zu sprengen, wird sich darauf beschränkt, dass der Befehl durch die Übergabe von ECh im PIO Modus ein Register im ATA-Registersatz anspricht und das Laufwerk auffordert, den 512 Byte großen Datenblock an den Host zu senden. In diesem Datenblock sind dann die Informationen zur Identifikation des Laufwerks enthalten. Dabei wird der Datenblock „Wort-weise“ gelesen. Ein Wort beinhaltet 2 Byte und ein Byte enthält wiederum 8 Bits. So definiert der ATA Standard, dass sich an bestimmten Stellen im Datenblock bestimmte Informationen befinden, die dann gelesen, ausgewertet und ausgegeben werden. Dementsprechend befindet sich an den Stellen von Wort 10-19 eine Kopie der Seriennummer des Laufwerks. An den Stellen von Wort 23-26 die Firmware Versionsnummer und an den Stellen von Wort 27-46 die

Modellnummer. An den Stellen von Wort 60-61 ist angegeben, wie viele logische Sektoren für einen Benutzer adressierbar sind oder auch an Wort 92 die Identifikation dafür, ob ein Master Passwort in Benutzung ist. Im letzten und abschließenden Grundlagenteil wird definiert, was ein Master-Passwort überhaupt ist und wie PC-3000 Express neben ATA Kommandos auch herstellerspezifische Kommandos automatisch umsetzt. Doch bevor dieser Abschnitt näher erläutert wird, sollte einem Benutzer des PC-3000 Systems bewusst sein, was das System überhaupt ist und wie die Benutzeroberflächen von PC-3000 Express und dem Data Extractor funktionieren. [48]

2.4 PC-3000 Express System

Laut ACELab ist das PC-3000 Express System eine Hardware-Software-Lösung zur Diagnose und Reparatur von Festplattenlaufwerken. Hierbei sind sowohl SATA- als auch PATA-Schnittstellen inbegriffen, sowie verschiedenste Festplatten-Hersteller, Kapazitäten von 500 MB bis zu 8 TB und Formfaktoren von 1,8 Zoll und 2,5 Zoll Laptop Laufwerken bis zu 3,5 Zoll Desktop Laufwerken werden abgedeckt. [7]

2.4.1 Aufbau des Systems

Das PC-3000 Express Professionell System besteht in einem Gesamtpaket aus drei Teilen. In jedem Fall ist dabei hardwareseitig ein PC-Erweiterungs-Board enthalten (siehe Abbildung 9), welches über zwei Anschlüsse in ein bestehendes System integriert wird. Die Verbindung zum Hauptprozessor erfolgt über einen PCI Express Steckplatz und verspricht eine Datenübertragungsrate von bis zu 2,5 GB/s. Über dieses Board können simultan bis zu vier Diagnoseports angesteuert werden. Dabei sind vier externe SATA Ports und zwei interne PATA Ports vorgesehen. Dabei können zwei der vier Ports entweder für SATA oder für PATA Anschlüsse verwendet werden. Eine Vier-Kanal Stromversorgung schützt vor zu hohen Spannungen und Stromüberlastungen. Des Weiteren beinhaltet das Gesamtpaket softwareseitig die beiden Komponenten PC-3000 Express und Data Extractor Express, welche je nach Bedarf auch einzeln nutzbar sind. Dabei beschränkt sich PC-3000 Express auf die Reparatur von Festplatten und der Data Extractor Express auf die Datenextraktion.

Abbildung 9: PC-3000 Express PC Erweiterungs-Board [7]

2.4.2 Funktionen des Systems

Ein spezialisiertes Datenrettungs-Unternehmen aus den USA, mit über 40 Standorten, schreibt auf seiner Webseite in einem Blogartikel über Firmware Folgendes:

„Da sich die Firmware einer Festplatte direkt auf physische Laufwerkskomponenten auswirkt, sollten Sie eine ausgefallene Festplatte nicht betreiben. Versuchen Sie nicht, Dateien mit Datenwiederherstellungssoftware wiederherzustellen; Ihr Laufwerk kann mit beschädigter Firmware nicht richtig booten, und keine kommerziellen Datenwiederherstellungstools können Probleme mit der Festplatten-Firmware effektiv umgehen.“ [35]

Die Erfahrung während der Arbeit mit dem PC-3000 Express Professionell System hat allerdings gezeigt, dass durchaus kommerzielle Hardware-Software Lösungen am Markt existieren, die sogar mit teilweise hohen Erfolgswahrscheinlichkeiten Probleme mit der Festplatten Firmware effektiv umgehen können.

Um solche Probleme effektiv zu umgehen, bietet PC-3000 zwei Modi zur HDD-Diagnose: Standardmodus (Benutzer) und Technologiemodus (Werksmodus). Für den Technologiemodus werden teilweise (bsp. bei Seagate und Samsung) spezielle Adapter verwendet, über die dann ein Zugriff auf die interne HDD-Software und die Benutzerdaten ermöglicht wird. Darüber hinaus existieren für verschiedene Hersteller, Festplatten-Architekturen und -Familien insgesamt 16 speziell angepasste Dienstprogramme. Durch sie wird jeweils Zugang zu den Festplatten, auch unter fehlerhaften Bedingungen ermöglicht, Schäden können ermittelt bzw. ausgeschlossen und letztendlich Benutzerdaten gesichert werden. Für etwaige Datenrettungs-Unternehmen, denen keine Tools bekannt sind, die mit Firmware Problemen umgehen können, ist in jedem Fall interessant, dass PC-3000 unter anderem:

Servicebereiche überprüfen und wiederherstellen, Fehlertabellen modifizieren und beschädigte Festplattenmodule reparieren kann. Eigenen Recherchen zufolge, benutzen viele bekannte Datenrettungsunternehmen weltweit das PC-3000 Express Professionell System oder andere ähnliche Produkte der Firma ACE Lab. (z.B. PC-3000 Portable) [7]

2.5 PC-3000 Benutzeroberflächen

Da sich das PC-3000 Express Professionell System softwareseitig aus zwei Komponenten zusammensetzt, erklärt dieses Kapitel die Benutzeroberfläche für PC-3000 Express und anschließend für den Data Extractor.

2.5.1 PC-3000 Express

Wie die meisten anderen Programme auch, muss PC-3000 Express zunächst vom Computer aus gestartet werden. Anschließend trifft der Benutzer auf einen recht umfangreichen Startbildschirm mit vielen Informationen und Auswahlmöglichkeiten. Von hier aus gilt es, die richtigen Parameter für die zu bearbeitende Festplatte auszuwählen und sie zu initialisieren.

2.5.1.1 Startbildschirm und Auswahl der Festplattenparameter

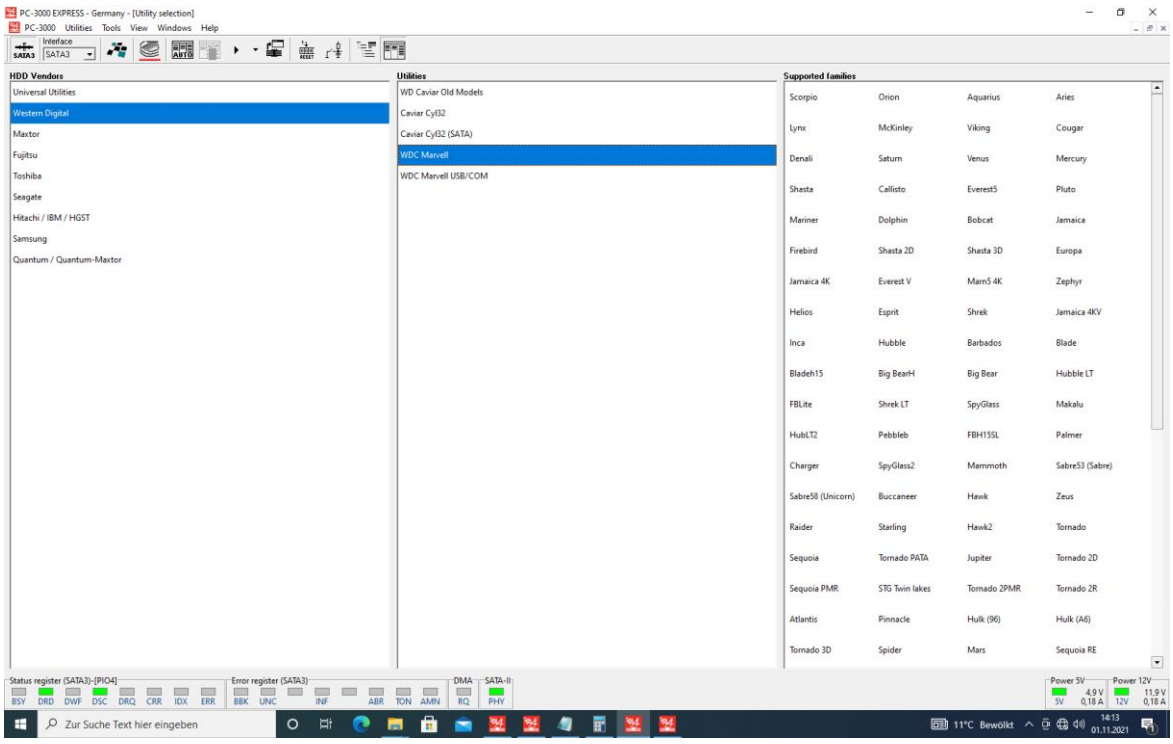


Abbildung 10: Startbildschirm PC-3000 Express [8]

In diesem Abschnitt werden die wichtigsten Funktionen zum Startbildschirm von PC-3000 Express erklärt und chronologisch von links oben nach rechts unten beschrieben. (siehe Abbildung 10)

Die erste Funktion nennt sich „Utilities“ und bietet verschiedene Optionen, die Festplatte zu initialisieren. Beispielsweise legt der Benutzer eigene Parameter fest und startet die Festplatte oder nutzt die „Autodetect“ Funktion und lässt PC-3000 Express die korrekten Parameter ermitteln. Über die Funktion „Tools“ sind Einstellungen verfügbar, der Zugang zur PC-3000 Datenbank von Festplatten oder auch die Energieüberwachung. Durch „View“ lässt sich der Startbildschirm individuell anpassen und bsp. Farben ändern. Von „Windows“ aus kann der Benutzer zwischen verschiedenen Anwendungsfenstern von PC-3000 Express wechseln und „Help“ bietet die klassische Unterstützung bei offenen Fragen oder auch Support. [9, 49, 50]

Einer der wichtigsten Buttons ist anhand von „SATA3“ erkennbar und regelt die Stromzufuhr der Festplatte (leuchtet dann grün) bzw. schaltet die Festplatte aus, wenn der Button erneut benutzt wird. Da über das Erweiterungs-Board von PC-3000 bis zu vier Festplatten gleichzeitig angeschlossen werden können, gibt „Interface SATA3“ Aufschluss darüber, welcher Anschluss gerade in Benutzung ist. Der nächste Button ähnelt dem „Symbol einer Fahne“ und gibt dem Benutzer die Wahl zwischen dem Startbildschirm für HDD´s oder Solid State Drives. Daneben befindet sich ein „Pfeil mit roter Markierung“, der den Data Extractor öffnet. Der Button „AUTO“ startet die bereits erwähnte „Autodetection“ per Schnellzugriff. Das ausgegraute Feld ist nur im SSD Modus verfügbar und damit nicht weiter relevant. Nach Betätigung des „Play“ Symbols wird die aktuelle Auswahl der Parameter ausgeführt. Rechts neben dem Play Button findet sich „Start Win Disk“ und dient dazu, die momentan zu bearbeitende HDD unter Windows anzeigen zu lassen, da PC-3000 eigentlich ein geschlossenes System ist. Daran schließen sich dann die Funktionen „Soft Reset“ und „Hard Reset“ an. Ein Soft Reset startet die Festplatte neu, während bei einem Hard Reset die Festplatte zurückgesetzt wird. Daneben findet sich dann „HDD Reference.“ Sollte aus welchen Gründen auch immer, eine Auswahl von Parametern nicht möglich sein, könnte durch „HDD Reference“ z.B. mit Hilfe der Modellnummer eine Parameterauswahl stattfinden. Den gleichen Zweck erfüllt auch der letzte Button in dieser Reihe, „Supported Families“, also unterstützte Herstellerserien. [9, 49, 50]

Den meisten Platz in der Startbildschirm-Ansicht belegen die drei Tabellen in der Mitte mit den Bezeichnungen „HDD Vendors“, also Hersteller, „Utilities“, also Architekturen und „Supported Families“, also Herstellerserien. Ganz links unten sind die Status – und Error-Register der Festplatte zu sehen. Die nachfolgende Übersicht erklärt die Bedeutung und

Funktionen dieser Register (siehe Tabelle 1 und 2). Zu guter Letzt ist ganz unten rechts erkennbar, welchen Strom die Festplatte gerade beansprucht. Dabei gibt es eine Unterteilung in 5 V und 12 V. 2,5 Zoll Festplatten nutzen ausschließlich den 5 V Anschluss, während 3,5 Zoll Festplatten beide Anschlüsse benutzen. [9, 49, 50]

Tabelle 1: Übersicht Status Register [12]

Abkürzung	Beschreibung	Bedeutung
BSY	Busy - Beschäftigt	HDD ist beschäftigt/arbeitet
DRD	Drive Ready – Laufwerk bereit	HDD ist bereit Kommandos auszuführen
DWF	Drive Write Fault - Schreibfehler	Fehler beim Schreiben oder Versuch zu schreiben mit falschen Parametern
DSC	Drive Seek Complete – Laufwerk-Positionierung vollendet	Die Köpfe haben sich über die gewünschte Oberfläche bewegt
DRQ	Data Request – Daten-Anfrage	Anfrage zur Datenübertragung zum/vom Speicher
CRR	Corrected Data – Korrigierte Daten	Ein Fehler wurde intern von der Festplatte korrigiert
IDX	Index	Die Festplatte greift auf ein Register zu
ERR	Error - Fehler	Es gibt einen Fehler

Tabelle 2: Übersicht Error Register [12]

Abkürzung	Beschreibung	Bedeutung
BBK	Bad Mark Block – fehlerhafter Block	Ein Block wird als fehlerhaft markiert
UNC	Uncorrected Data – Nicht korrigierte Daten	ECC konnte bestimmte Daten nicht korrigieren
INF	ID Not Found – ID nicht gefunden	Der gewählte Zylinder, Kopf und Sektor wurden nicht gefunden / ECC Fehler im Sektor Header
ABR	Abort- Abbruch	Ein Kommando wird abgebrochen, bsp. falsche Parameter
T0N	Track 0 Not Found – Spur 0 nicht gefunden	Spur 0 kann nicht gefunden werden
AMN	Address Mark Not Found – Adressen Markierung nicht gefunden	Adressen Markierung der Sektordaten wurde nicht gefunden, aber der Sektor konnte identifiziert werden
DMA -RQ	Direct Memory Access Request – Anfrage für direkten Speicherzugriff	Anfrage für den Modus des direkten Speicherzugriffs ohne Beteiligung des Hauptprozessors
SATA-II - PHY	Serial AT Attachment -II – Physical – Serielles Übertragunsprotokoll - Physisch	Die Festplatte ist physisch über SATA-II verbunden

2.5.1.2 Initialisierung einer Festplatte

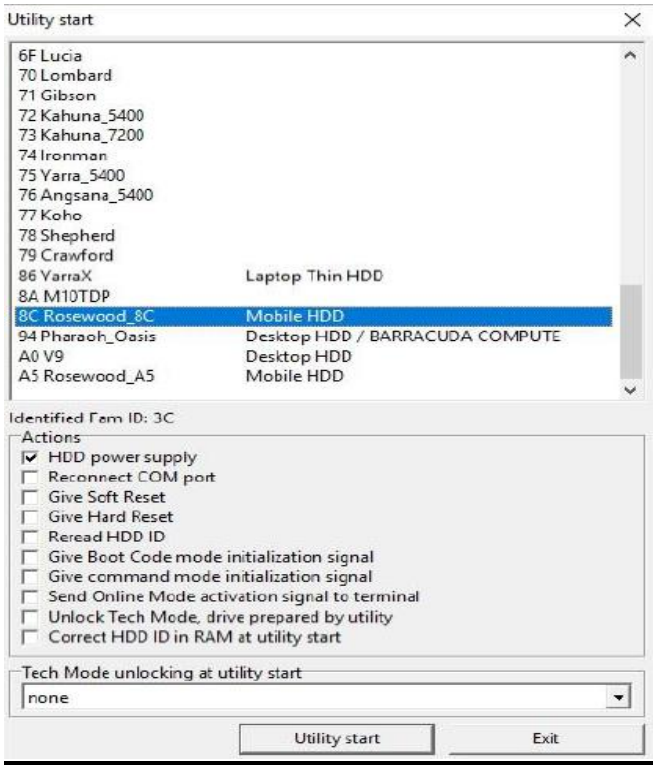


Abbildung 11: Initialisierungsfenster PC-3000 Express [9]

Nachdem in den meisten Fällen die Parameter zur Initialisierung einer Festplatte per Schnellzugriff durch PC-3000 Express intern ermittelt wurden, initialisiert die Festplatte. Daraufhin gelangt der Benutzer in einen Auswahl Dialog für die Herstellerserien, die im Regelfall automatisch anhand der HDD Identifikationsdaten erkannt werden. In diesem Dialog besteht außerdem die Möglichkeit, weitere Parameter anzugeben, welche festlegen, wie sich die Festplatte beim Starten verhalten soll. Darunter zählen z.B. wieder Soft – und Hard Reset oder auch ein Signal dafür, den Boot Code Mode zu initialisieren. Die Auswahl unten „Tech Mode unlocking at utility start“, wird standardmäßig bei der Benutzung von PC-3000 Express ausgeführt und erweitert die Ausführung von Funktionen im Vergleich zum Benutzermodus. „Utility start“ bringt den Benutzer schließlich in das Hauptmenü. Das Beispiel bezieht sich hier auf eine Seagate Festplatte. An dieser Stelle ist wichtig, dass sich der Dialog nach der Initialisierung, je nach Hersteller und Festplatte ändern kann, der grundlegende Aufbau und die Funktion des Dialoges bleiben aber gleich. Außerdem ist anhand dieses Beispiels eine Initialisierung unter optimalen Bedingungen beschrieben, die je nach Zustand der Festplatte anders ausfallen könnte. [9, 49, 50]

Sobald „Utility Start“ ausgewählt wurde, greift PC-3000 Express für die automatische Konfiguration auf das Laufwerk zu und fordert unter anderem folgende Informationen an:

```
Family ID: 8C

Selected family..... : 8C, Rosewood_8C
Model by ID..... : ST1000LM035-1RK172

Tech Key...

Requesting FW Pkg ver ..... RW07A8.SDM2.AA6973.SBM3

Detecting SA Phys Sct Size...
Result..... : 4096

Detecting UA Phys Sct Size...
Result..... : 4096

Detecting Max Head number...
Phys. heads..... : 2

Obtaining Saved Mode Pages File information...
Reading Saved Mode Pages...
Parsing Saved Mode Pages...

LBA alignment..... : 0
```

Abbildung 12: Logmeldungen zur Initialisierung [9]

2.5.1.3 Das Hauptmenü

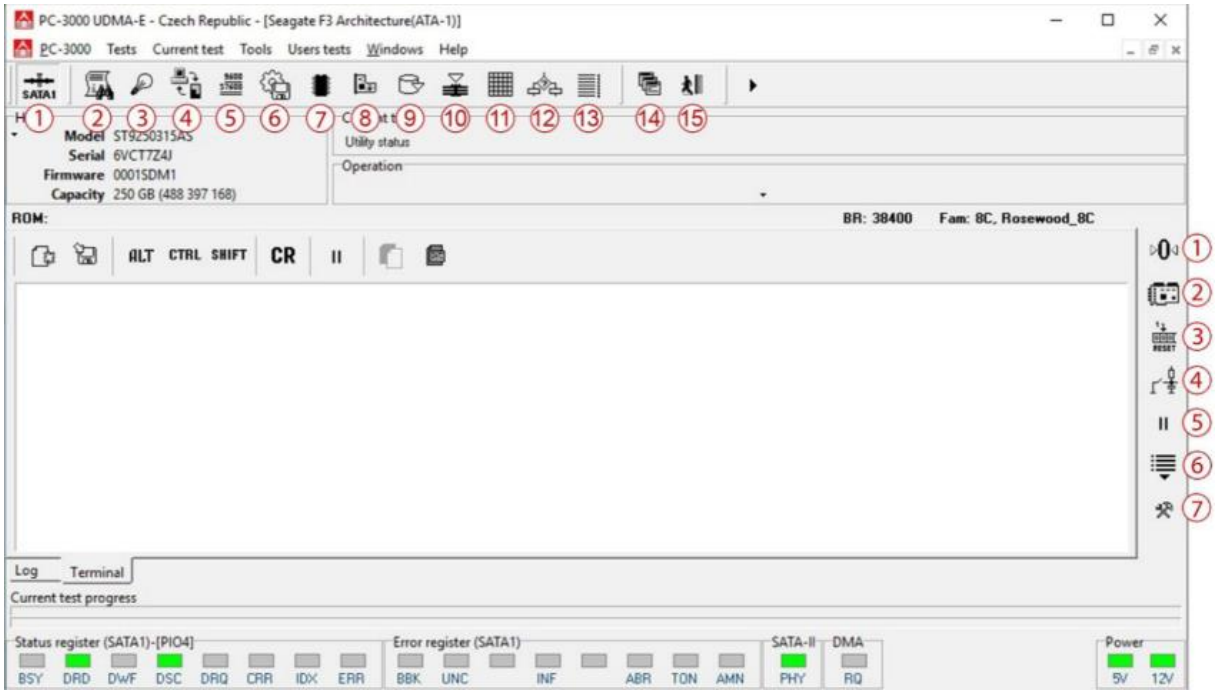


Abbildung 13: Hauptmenü PC-3000 Express [9]

Ein Blick auf den untersten Teil des Hauptmenüs reicht, um festzustellen, dass sich an den Status – und Error Registern sowie der Stromnutzung nichts geändert hat. (siehe Abbildung 13) Darüber befindet sich eine Fortschrittsleiste. Über der Fortschrittsleiste finden sich alle geöffneten Untermenüs, von denen standardmäßig der Log und das Terminal (wenn verfügbar) geöffnet sind. Die Informationen werden dann je nach Inhalt im großen weißen Fenster angezeigt. Beim Blick nach ganz oben kommen dem Benutzer ebenso die Reiter „Help“ und „Windows“ bekannt vor. Auch „Tools“ findet sich hier wieder, ist allerdings mit anderen Unterfunktionen ausgestattet. Darunter fallen zum Beispiel die Möglichkeit zur Bearbeitung von Sektordaten, Abrufen von Laufwerks Identifikationsdaten oder SMART Daten. Die oberste Reihe wird durch drei verschiedene „Test“ Reiter komplett. “Tests“ liefert ein umfangreiches Menü mit notwendigen Operationen zur Bearbeitung von HDD´s. Eine dieser Optionen beinhaltet den „Utility status“ und öffnet eine Übersicht zum Status des Laufwerks und bietet dem Benutzer die Möglichkeit, verschiedene Informationen wie Modullisten, Random Access Memory oder ROM neu einzulesen. Dazu kommt auch ein Untermenü „Service information“, dass alle möglichen Operationen zur Modifikation der Service Daten auf dem PCB oder den Platten beinhaltet. „Current test“ loggt die am häufigsten bzw. zuletzt ausgeführten Befehle, startet Kommandos und kann eine Statusübersicht erzeugen. Durch „Users tests“ besteht für den Benutzer die Möglichkeit, individuelle Befehle oder auch Skripte auszuführen. Unterhalb der oberen Symbolleiste werden die aktuell ermittelten Identifikationsdaten des Laufwerks dargestellt und rechts daneben, welcher Befehl ausgeführt wird (Current test) und wie PC-3000 Express den Befehl ausführt. (Operation) Nachfolgend eine Übersicht zu den beiden Symbolleisten oben und rechts: [9, 49, 50]

Tabelle 3: Obere Symbolleiste [9]

Nummer	Beschreibung
1	Stromversorgung
2	Schaltfläche zum Öffnen des Laufwerk-Statusdialogs (der den aktuellen Laufwerks-Status anzeigt und die erneute Abfrage bestimmter Parameter vom Laufwerk ermöglicht)

Tabelle 3 (Fortsetzung): Obere Symbolleiste [9]

3	Mikrocode hoch – oder runterladen
4	Erneute Verbindung zum COM-Port (erforderlich, wenn der USB-zu-COM-Adapter nicht mehr reagiert)
5	Erkennen und umschalten der Datenaustauschrate zwischen HDD und Terminal
6	HDD Resourcen Backup
7	Menü zum Lesen/Schreiben des ROM, Änderung der HDD-ID im ROM, Entsperren des Technologie/Werksmodus;
8	Gruppe von Funktionen zur Kommunikation mit dem Controller, wie Fehlertabellen lesen/schreiben oder das Ändern von Parametern im RAM
9	Gruppe von Funktionen zur Arbeit mit dem Servicebereich, wie Lesen/Schreiben von Modulen
10	Logisches Scannen der Festplatte
11	Lesen/Schreiben der Fehlertabellen wie G-List, P-List usw.
12	Funktionen zum Beheben typischer Fehler
13	Benutzerdefinierte Befehle
14	Wechseln zwischen Anwendungsfenstern
15	Verlassen der Anwendung
16	Ausführen-Button

Tabelle 4: Rechte Symbolleiste [9]

Nummer	Beschreibung
1	Neukalibrierung der HDD
2	PC-3000 Express Controller Zurücksetzen
3	Software Reset
4	Hardware Reset
5	Pausieren/Standby (Schlafmodus)
6	Ausführen-Button (die Schaltfläche ermöglicht die Ausführung der Befehle zum Entsperren des Werksmodus)
7	Einstellungen/Benutzerdefinierte Befehle

2.5.2 Data Extractor

Der Data Extractor ist ein professionelles Software-Programm zur Datenextraktion – und -sicherung. Das Tool ermöglicht die Datenwiederherstellung von allen Laufwerken, die an die Anschlüsse des PC-3000 Erweiterungs-Board angeschlossen sind sowie von jedem weiteren Datenspeichergerät, dass durch die Anschlüsse bedient und vom Betriebssystem erkannt werden kann. Die Anwendungsgebiete des Data Extractor sind die Wiederherstellung von physisch defekten Laufwerken sowie von Laufwerken, bei denen logische Strukturen beschädigt sind oder auch eine Kombination aus beiden Anwendungsgebieten. Die Daten eines fehlerhaften Laufwerks können durch eine vollständige oder teilweise Kopie direkt auf eine andere Festplatte oder in Form von Image-Dateien gesichert werden. Auch die Erstellung von Klonen ist möglich. [51]

2.5.2.1 Startbildschirm und Projekterstellung

Um mit dem Data Extractor zu arbeiten, wird das Programm entweder direkt über ein entsprechendes Programm-Icon vom PC gestartet oder im Startbildschirm/Hauptmenü von PC-3000 Express über den Schnellzugriff bzw. Utilities ausgewählt.

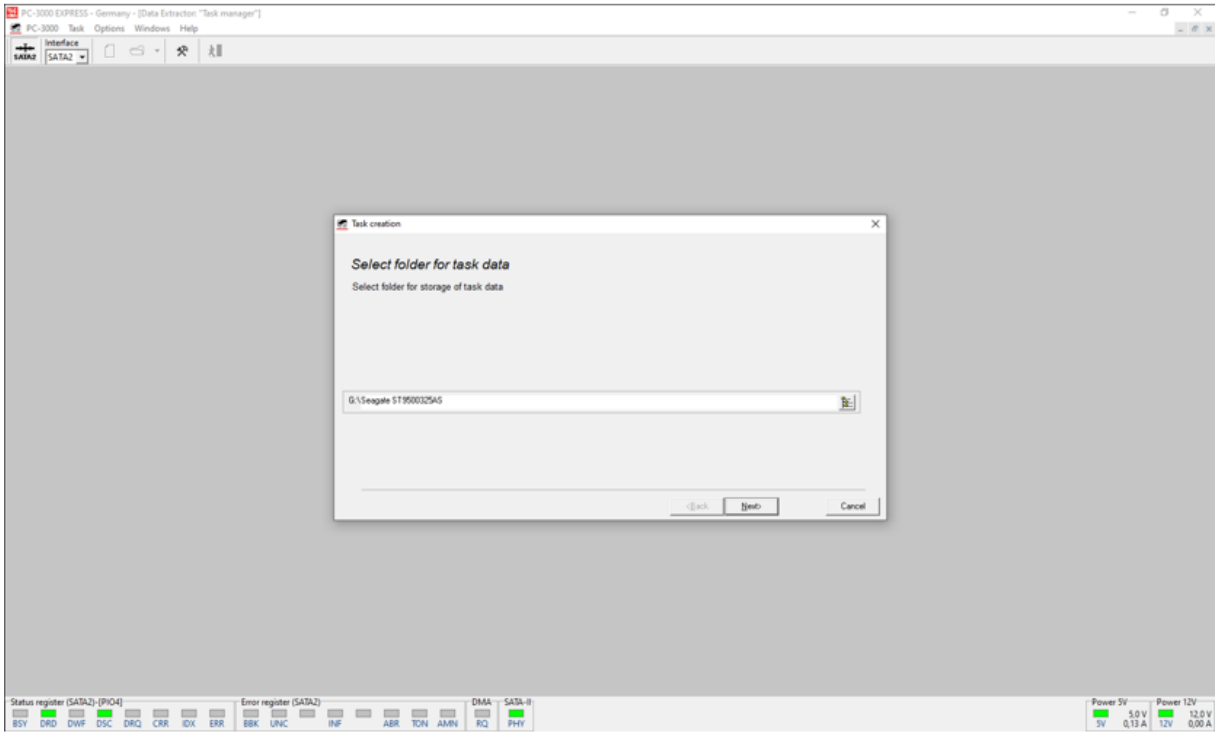


Abbildung 14: Task creation Data Extractor [8]

Auch im Data Extractor bleibt dem Benutzer die Anzeige der Status – und Error-Register sowie die Stromanzeige erhalten. (siehe Abbildung 14) Oben links über das Task-Menü kann ein neues Projekt erstellt, ein bestehendes geöffnet oder aus den letzten Projekten gewählt werden. Rechts daneben über Optionen lassen sich Projekt-Parameter und zusätzliche Informationen modifizieren. Außerdem sind hierüber Grep-Ausdrücke (erweiterte Suche/Filter) verfügbar und die letzte Funktion referenziert und vergleicht Rohdaten. Windows und Help sind genauso wie bei PC-3000 Express unverändert. Direkt darunter befindet sich die Schnellzugriff-Leiste, aus der ebenso ganz links, die Stromzufuhr und daneben die Wahl der Schnittstelle bekannt sind. Über das ausgegraute Blatt Papier lässt sich später ein neues Projekt erstellen und daneben über den Ordner ein bestehendes Projekt öffnen. Am Ende der Leiste finden wir die Einstellungen und die Möglichkeit, den Data Extractor zu verlassen. Über die in der Mitte befindliche „Task creation“ wird zunächst die zu bearbeitende Festplatte ausgewählt und ein Projektordner erstellt. Anschließend wird die

Schnittstelle ausgewählt, die dann links oben angezeigt wird. Anschließend öffnen sich die Projektoptionen. [51] (siehe Abbildung 15)

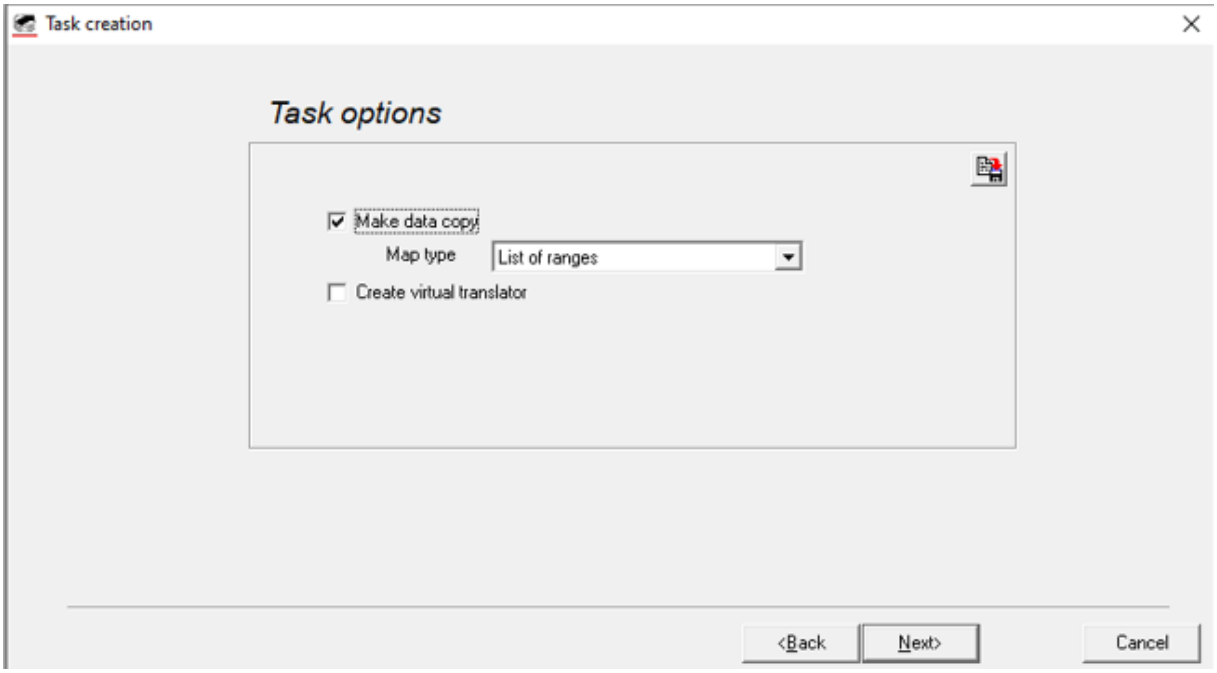


Abbildung 15: Task options Data Extractor

Wenn die Option „make data copy“ (Erstellen von Datenkopien) aktiviert ist, bedeutet die weitere Bearbeitung von Daten immer das Arbeiten mit der Datenkopie. Während der Erstellung einer Kopie generiert das Programm eine Karte mit allen Leseergebnissen, die es dem Benutzer ermöglicht, den Status aller Daten auf dem Laufwerk zu evaluieren. Zum Beispiel wenn ein Sektor erfolgreich gelesen wurde, dann führt ein erneuter Leseversuch nicht dazu, dass das ohnehin beschädigte Laufwerk erneut auf den Sektor zugreift, sondern über die Kopie. Die Option „Create virtual translator“ sollte aktiviert werden, wenn ein beschädigtes Laufwerk Probleme mit dem Übersetzermodul hat. Anschließend kann ein Ziel für die Kopie der Daten festgelegt werden und die individuelle Größe einer Datei. [51]

2.5.2.2 Projekt Parameter

Wie bereits erwähnt können über die Optionen die Projekt-Parameter modifiziert und je nach Festplatte angepasst werden. Diese sind nicht nur durch ihre Quantität, aber auch durch ihren Inhalt sehr relevant. Beispielhaft werden einzelne Funktionen näher erklärt:

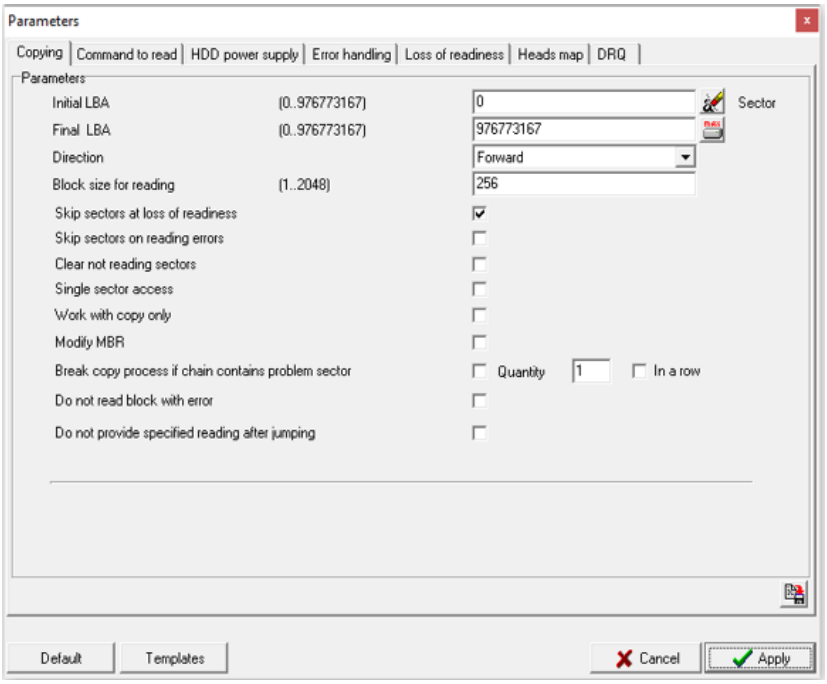


Abbildung 16: Copying Fenster Data Extractor [8]

Das Kopieren (Copying)-Fenster (siehe Abildung 16) geht bereits mit einer ganzen Reihe von Funktionen einher, wie zum Beispiel dem „Direction“, also Richtungs-Parameter. Dieser kann in zwei Fällen sehr relevant sein. Einerseits wenn die Festplatte einen Kratzer auf der Oberfläche besitzt und dieser sich relativ am Anfang der Platte befindet. Dann befindet sich der größte Teil der nicht vom Kratzer betroffenen Daten am Ende und es ist sinnvoll zunächst die unbeschädigten Daten rückwärts zu sichern. Andererseits existieren Laufwerke, die Daten ohne Zwischenspeicherung besser lesen, wenn sie beschädigt sind. Dabei wird durch das Rückwärtslesen der Zwischenspeicher zurückgesetzt und ermöglicht manchmal die Wiederherstellung größerer Bereiche. Der Parameter „Skip sectors on reading/readiness errors“ ermöglicht eine schnellere und schonendere Sicherung der Daten, wenn eine Datensicherung abbrechen sollte. Bei jedem Sektorfehler der aufgetreten ist, überspringt das Programm Sektoren, die bereits Probleme verursacht haben. Anschließend werden alle lesbaren Sektoren gesichert, ohne Zeit mit Lesefehlern zu verlieren und das beschädigte Laufwerk zu überfordern. [51]

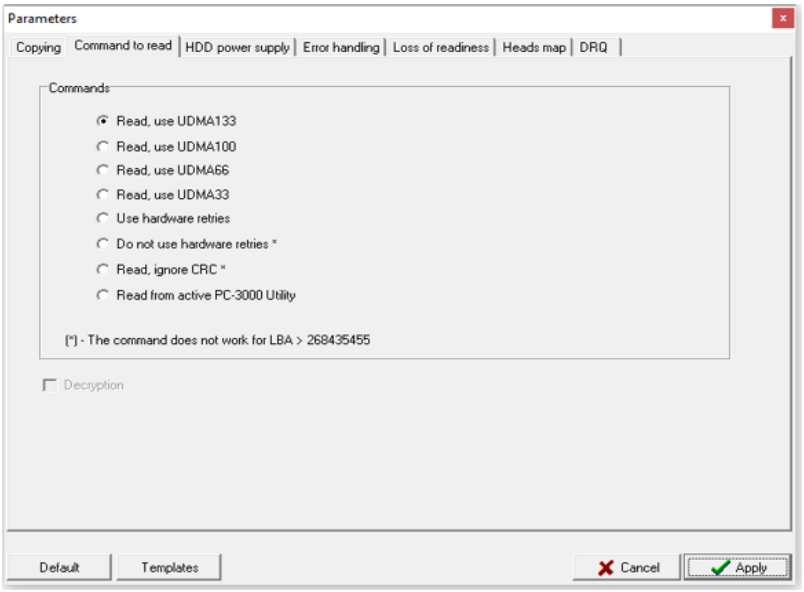


Abbildung 17: Command to read Data Extractor [8]

Das „Command to read“ (Kommando zum Lesen)-Fenster (siehe Abbildung 17) bezieht sich auf verschiedene Betriebsarten wie im UDMA133 bis UDMA33 Modus. Die „hardware retries“ können je nach Laufwerksmodell effektiv eingesetzt werden und bestimmen anhand von Hardware-Wiederholungen das Aktivieren oder Deaktivieren der Rückgabe von Fehlern durch die Festplatte. Mit „Read, ignore CRC“ erzwingt der Benutzer das Lesen von Daten ohne die Integrität zu hinterfragen. „Read from active PC-3000 utility“ ermöglicht das Lesen über spezialisierte Dienstprogramme die in der Software enthalten sind. [51]

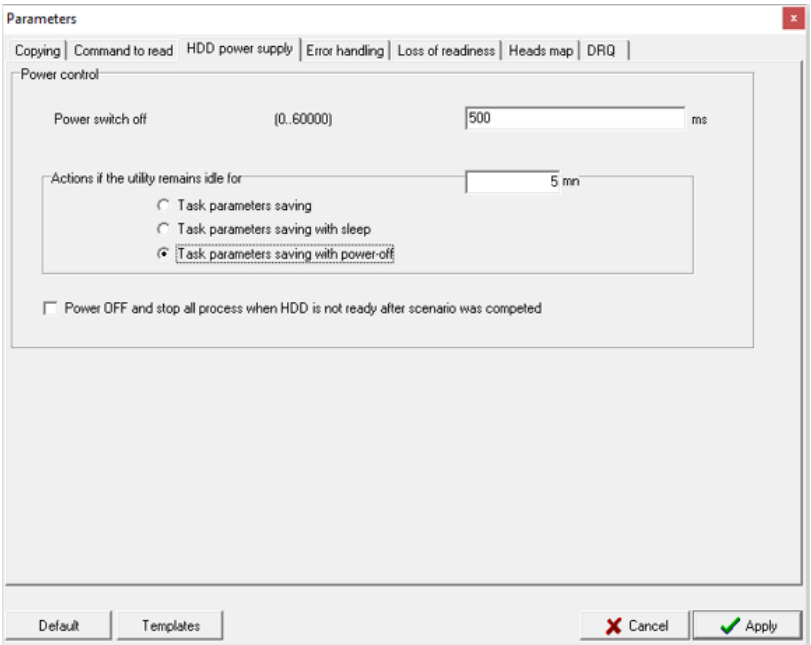


Abbildung 18: HDD power supply Data Extractor [8]

Durch „HDD power supply“, also HDD Stromversorgung, (siehe Abbildung 18) wird in Einzelfällen entschieden, was mit der Festplatte geschieht, wenn aus irgendeinem Grund die Sicherung beendet wurde oder wenn die Sicherung auf natürliche Weise beendet worden ist und ob die aktuellen Parameter-Einstellungen gespeichert werden sollen. [51]

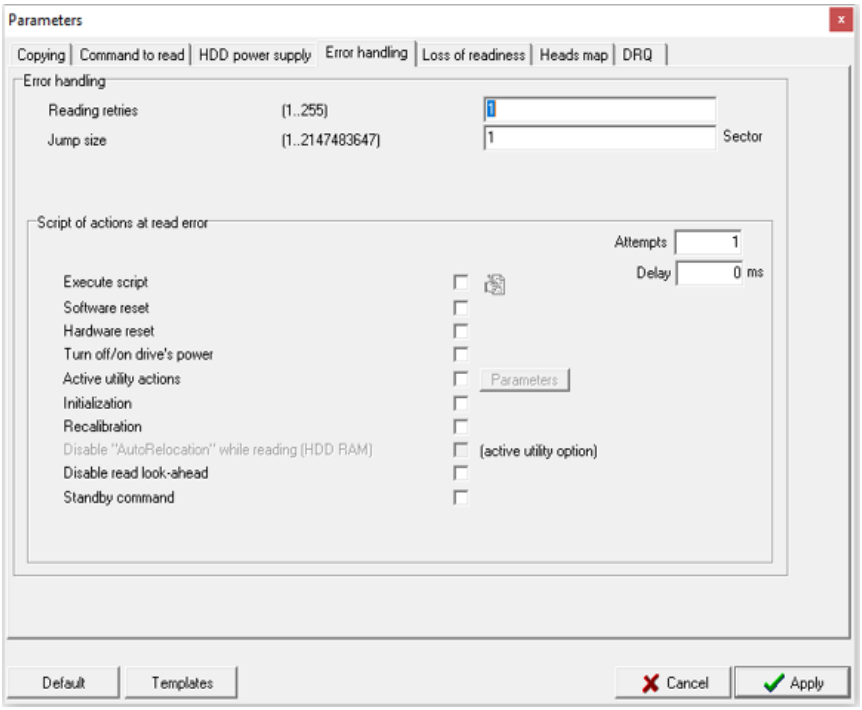


Abbildung 19: Error handling Data Extractor [8]

Das „Error handling“ – Fenster (Fehlerbehandlung), (siehe Abbildung 19) ist einer der wichtigsten Parameter, da fast alle Einstellungen beim Lesen von Daten berücksichtigt werden. „Reading retries“ (Lesewiederholungen) bestimmt zum Beispiel die Anzahl der Leseversuche für einen fehlerhaften Sektor. Darüber hinaus können diverse Einstellungen aktiviert/deaktiviert werden, wenn Lesefehler auftreten, wie zum Beispiel Software – oder Hardware-Resets. [51]

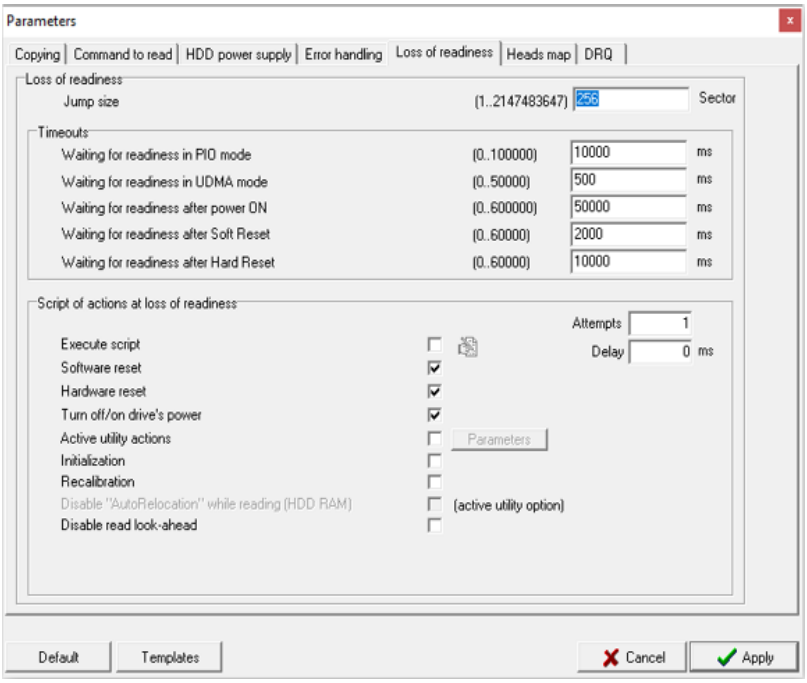


Abbildung 20: Loss of readiness Data Extractor [8]

Genauso wichtig wie die Fehlerbehandlung ist das „Loss of readiness“-Fenster (Abbruch der Bereitschaft der Festplatte), (siehe Abbildung 20) dass vor allem dann relevant ist, wenn eine Festplatte Klickgeräusche erzeugt. So definiert die „Jump size“ (Sprunganzahl), wie viele Sektoren übersprungen werden sollen, wenn die Festplatte innerhalb eines bestimmten Zeitfensters nicht mehr reagiert. Ebenso werden hierüber Aktionen festgelegt, die die Festplatte ausführt, wenn die Bereitschaft verloren geht. [51]

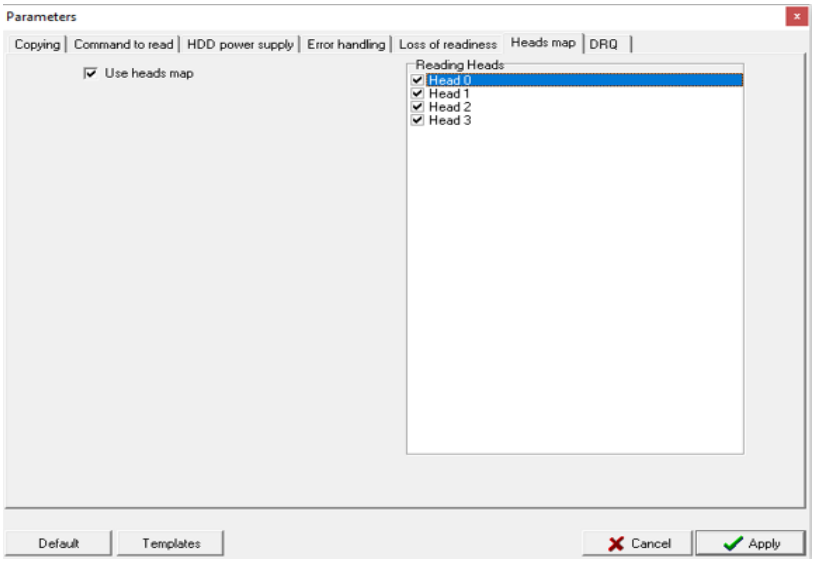


Abbildung 21: Heads map Data Extractor [8]

Bevor eine Karte der Köpfe (Heads map) (siehe Abbildung 21) verwendet werden kann, muss sie initialisiert und erzeugt werden. Die Karte kann entweder für einzelne Köpfe, oder für alle Köpfe erstellt werden. Hierfür werden vorher die Grenzen der Karte innerhalb eines bestimmten LBA-Bereiches eingeteilt. Ist die Karte fertiggestellt, ist es auch möglich auszuwählen, von welchen Köpfen konkret gelesen werden soll. Ebenso ist es möglich, nur den Teilbereich innerhalb eines einzelnen Kopfes abzurufen und zu sichern. [51]

2.6 Funktionsbeispiel PC-3000

Im Abschnitt 2.3 wurde bereits erwähnt, dass bei der Veröffentlichung von ATA-3 Sicherheitsfunktionen für Festplatten hinzugefügt wurden. Diese sind im Kommando Set anhand vom „Security feature set“ beschrieben. Die wichtigste Funktion ist die Möglichkeit ein ATA-Passwort zu setzen und damit Zugang zu Benutzerdaten auf einer Festplatte stark einzuschränken. Dieser Abschnitt soll den Umgang von PC-3000 Express mit Festplatten, die durch ein Passwort geschützt sind, erklären. Dabei ist die Verwendung von ATA Kommandos enthalten und die Möglichkeit der Nutzung herstellerspezifischer Befehle. Stellvertretend sollen die beiden Umgangsmöglichkeiten aufzeigen, wie PC-3000 Express über die Benutzeroberfläche ausgewählte Befehle verarbeitet und mit einer Festplatte kommuniziert.

2.6.1 Security Feature Set

Der ATA-Standard sieht für dieses Kommando Set zwei Arten von Passwörtern vor und arbeitet auf der Grundlage von „Security-Befehlen.“ Ein sogenanntes aktives „Benutzerpasswort“ regelt den Zugriff auf Benutzerdaten auf niedrigster Ebene. Damit der Passwortschutz aktiv wird, muss der Benutzer zunächst ein Benutzerpasswort durch „Security Set password“ setzen. Nach einem Neustart der Festplatte ist der Zugang zu Benutzerdaten nur durch Eingabe des Benutzerpasswortes gestattet. Während des Entsperrvorgangs wird ein „Security Unlock“-Befehl an die Festplatte gesendet, der den Typ (User oder Master) und das Passwort selbst enthält und auf Eingabe des korrekten Passwortes wartet. Im entsperrten Zustand ist es dem Benutzer dann auch möglich, einen „Security Disable Password“-Befehl auszuführen, um den Passwortschutz bis zum nächsten Setzen eines Passwortes zu deaktivieren. [10, 13, 52]

Über dem Benutzerpasswort steht ein sogenanntes „Masterpasswort.“ Dieses wird auf der Festplatte während der Herstellung gespeichert und kann über mitgelieferte Datenblätter ermittelt werden. Das Masterpasswort dient dazu, die Festplatte auch dann zu entsperren, wenn das Benutzerpasswort nicht mehr bekannt ist oder um administrativen Zugriff zu

ermöglichen. Das mitgelieferte Masterpasswort ist herstellerspezifisch und teilweise recht primitiv, wie zum Beispiel ein einfaches ASCII Leerzeichen. Eine Benutzung des Masterpasswortes sieht wiederum zwei verschiedene Sicherheitsniveaus vor, hoch und maximal. Das Sicherheitsniveau bestimmt, welche Security-Befehle in Kombination mit dem Masterpasswort erlaubt sind. Wenn ausschließlich das Masterpasswort bekannt ist, muss sich die Festplatte in einem hohen Sicherheitsniveau befinden. Dann kann das Masterpasswort mit den gleichen Befehlen wie das Benutzerpasswort zum entsperren verwendet werden. Bei aktivem maximalen Sicherheitsniveau der Festplatte, hilft auch das Masterpasswort nicht mehr. In diesem Zustand sind lediglich zwei Befehle in fester Reihenfolge ausführbar. Der erste ist der „Security Erase Prepare“-Befehl und führt eine Abfrage gegenüber dem Benutzer aus, ob er den nachfolgenden Befehl tatsächlich ausführen möchte. Denn der zweite Befehl „Security Erase Unit“ führt dazu, dass der gesamte Inhalt der Festplatte (außer defekte Sektoren) mit 0x00 überschrieben wird und somit die Daten gelöscht werden. Der eigentliche Sinn von „Security Erase Unit“ ist das Wipen alter, ungenutzter Daten auf der Festplatte, um sie mit neuen Daten zu füllen. Sowohl zum Knacken des Benutzerpasswortes als auch eines individuellen Masterpasswortes wäre eine Wörterbuch-Attacke denkbar. Allerdings lässt der Security Unlock Befehl nur maximal fünf Passworteingaben zu und schützt damit effektiv gegen diese Art von Angriff. [10, 13, 52]

2.6.2 PC-3000 Express Security Subsystem

Die Ausführung der oben erwähnten Befehle wird über vier Auswahlmöglichkeiten innerhalb der PC-3000 Express Benutzeroberfläche gewährleistet. Unter → „Tools“ → „HDD Security subsystem“ steht zur Auswahl:

Tabelle 5: Verfügbare Security Befehle [13]

Befehl	Beschreibung
Open HDD	Anhand von ATA definiert, wird ein „Open HDD“ Befehl (Security Unlock) an die Festplatte gesendet. Die Ausführung öffnet ein Fenster, um den Typ und das Passwort selbst zu definieren.
Clear password	Sendet einen Befehl, um den Typ des Passworts und das Passwort selbst, dass sich im Speicher befindet, zu entfernen.
Password setting	Sendet das „Security Set password“ Kommando und lässt den Benutzer Passworttyp und Passwort selbst festlegen.
Security erase	Sendet das „Security Erase Prepare/Unit“ Kommando. Die Ausführung des Kommandos wird nur durch das Entsperren der Festplatte mit Masterpasswort möglich.

Zur Verdeutlichung der vorteilhaften Funktionen von PC-3000 Express:

Eine Festplatte des Herstellers Western Digital, WDC WD5000AAVS-00ZTB0, 500 GB Speicherkapazität, wurde durch das Programm „HDAT2“ mit dem ATA-Benutzerpasswort „geheim“ belegt. Zur Kontrolle wurde die Festplatte an einen anderen Rechner mit Windows Betriebssystem angeschlossen und die Ausgabe der Datenträgerverwaltung dokumentiert. (siehe Abbildung 22)

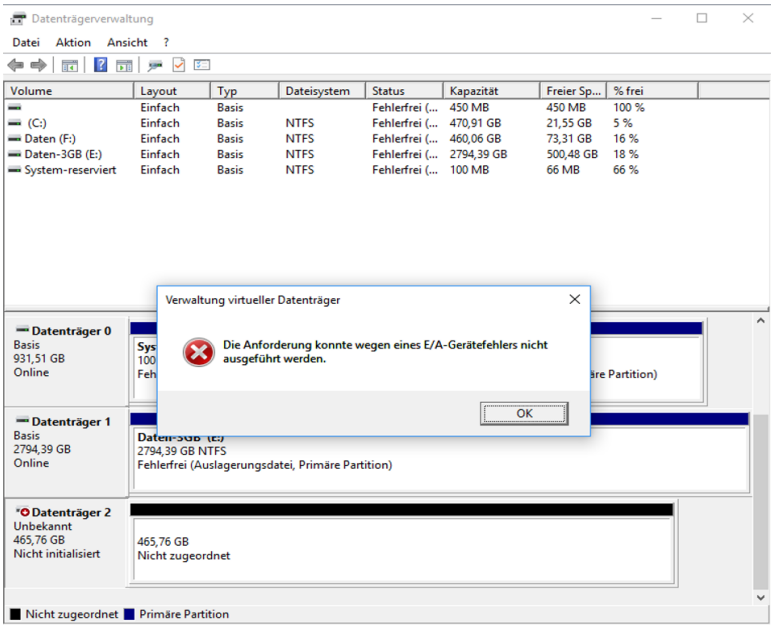


Abbildung 22: Datenträgerverwaltung unter Windows

Windows erkennt die Festplatte bis auf die Kapazität nicht und gibt einen Ein – und Ausgabe-Gerätefehler an. Darüber hinaus wurde die Festplatte an das gleiche System über einen Writeblocker des Herstellers Tableau angeschlossen und die Ausgabe dokumentiert. (siehe Abbildung 23) Der Writeblocker erkennt die Festplatte und ebenso, dass Sicherheitserweiterungen aktiviert sind, gewährt aber dennoch keinen Zugriff auf das Laufwerk.

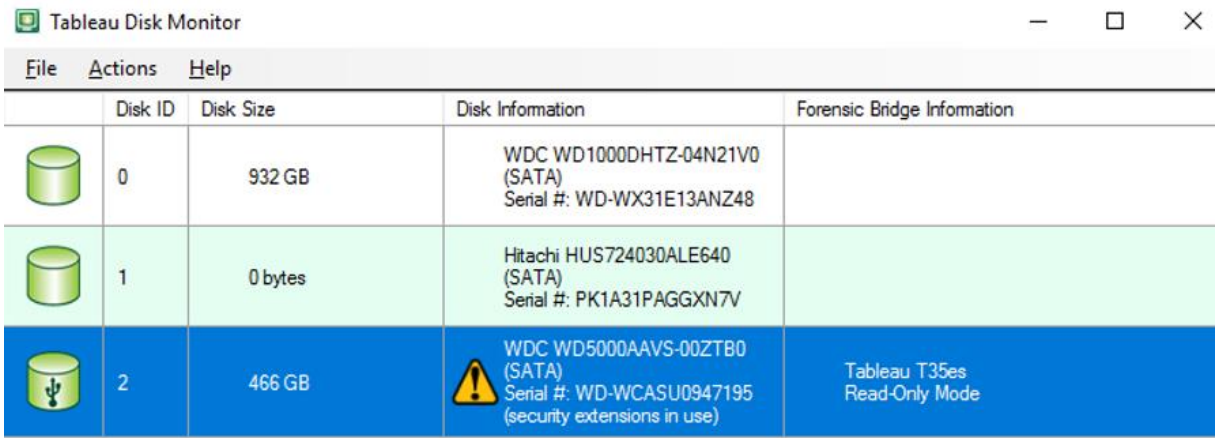


Abbildung 23: Datenträgerübersicht Tableau Disk Monitor

Durch PC-3000 Express wurde die Festplatte über den Startbildschirm auf dem üblichen Weg initialisiert und gestartet. (siehe Abbildung 24 und 25)

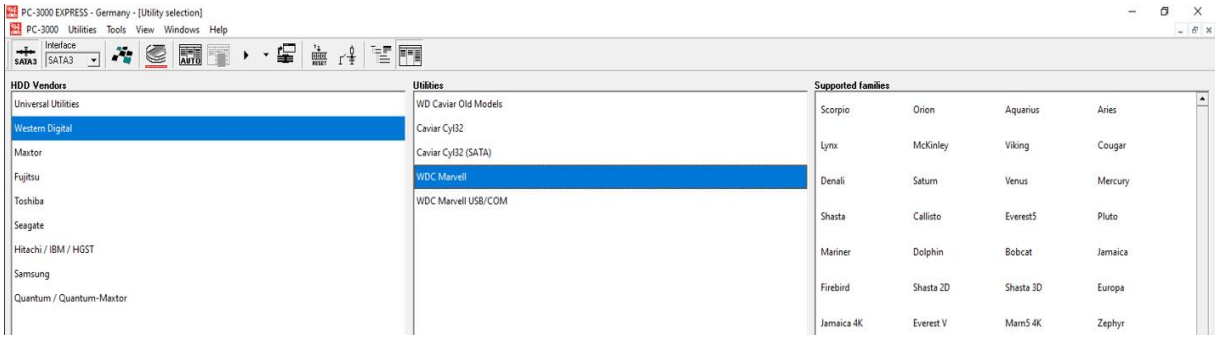


Abbildung 24: Startbildschirm PC-3000 Express (2) [8]

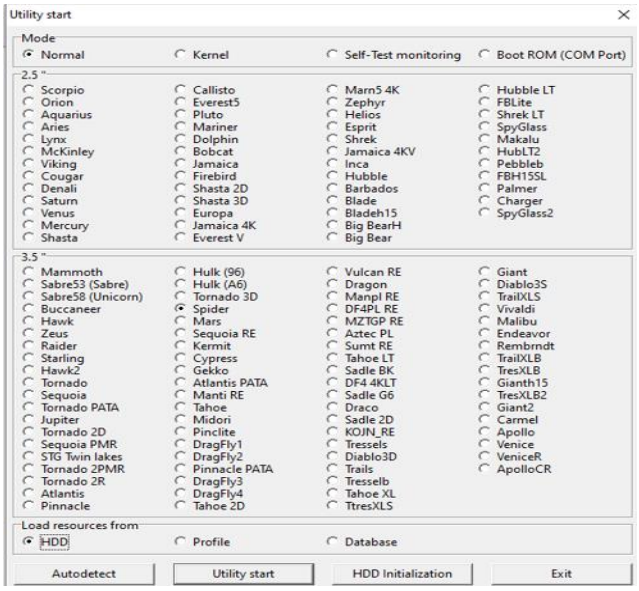


Abbildung 25: Initialisierungsfenster PC-3000 Express (2) [8]

Daraufhin begegnet dem Benutzer folgender Dialog:

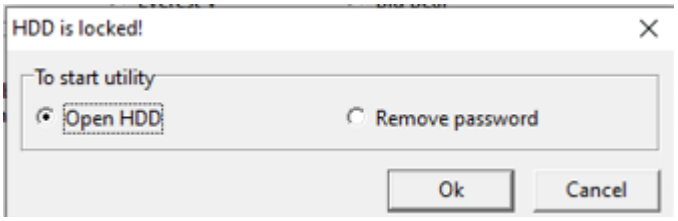


Abbildung 26: Passwortschutz-Statusmeldung PC-3000 Express [8]

PC-3000 Express erkennt die Sicherheitsvorkehrungen der Festplatte und bietet dem Benutzer die Möglichkeit, das Passwort sofort entfernen zu lassen. Darüber hinaus kann die Festplatte mit „Open HDD“ sogar ohne Passwort geöffnet werden, der vollumfängliche Zugriff auf Daten ist gewährleistet und das gesetzte Passwort wird erkannt und dem Benutzer preisgegeben. Außerdem kann den Logdaten des Startprozesses das Default-Masterpasswort von Western Digital entnommen werden. (siehe Abbildung 27 und 28)

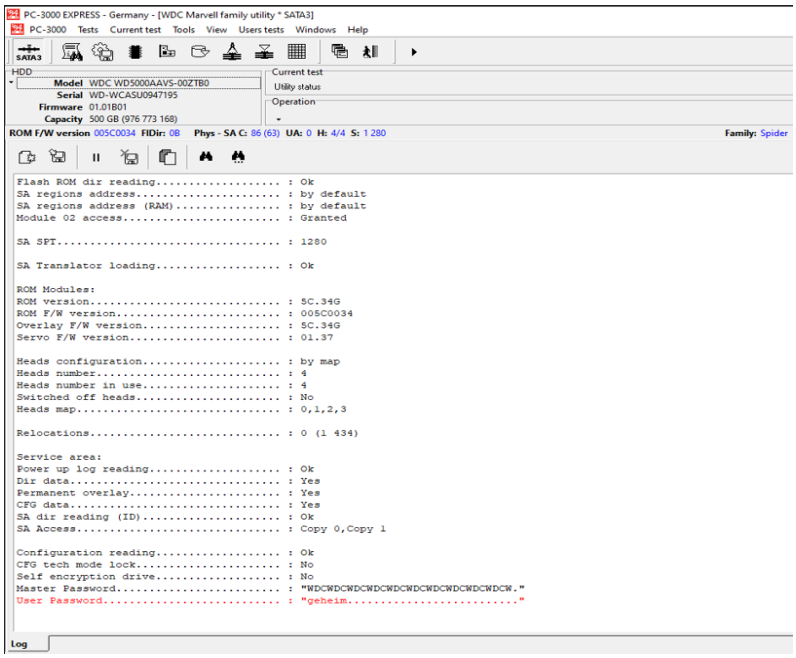


Abbildung 27: Logmeldungen zur Initialisierung (2) [8]

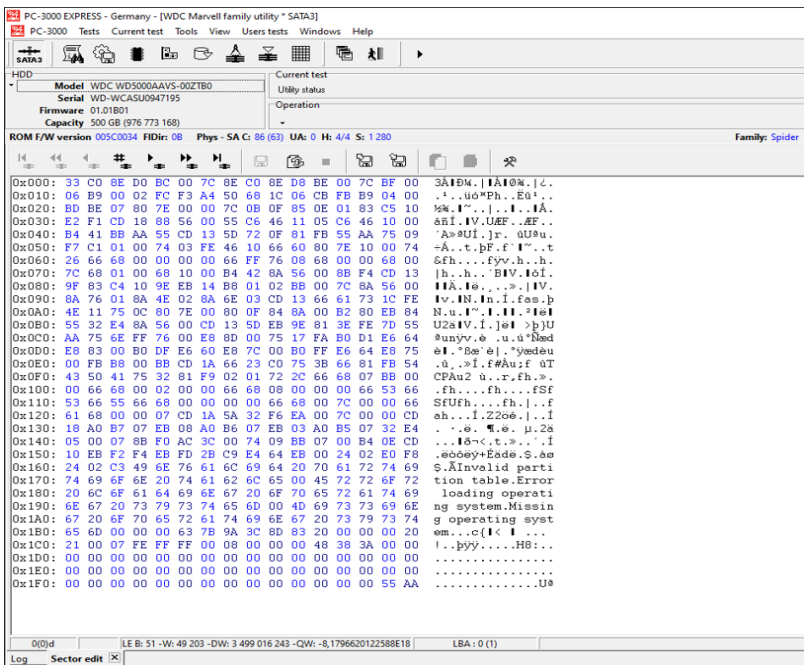


Abbildung 28: Zugriff auf Daten durch Sektoreditor [8]

2.6.3 Herstellerspezifische Kommandos

Bevor eine Festplatte ausgeliefert wird, implementieren die Hersteller systemunabhängige Firmware und eigene Diagnoseprogramme, die je nach Hersteller und Modell über eine eigene Schnittstelle verfügen. Mit Hilfe dieser speziellen Wartungsschnittstelle können herstellerspezifische Befehle ausgeführt, das Terminal entsperrt oder bei manchen Festplatten ausschließlich hierüber der ROM ausgelesen werden. Das PC-3000 System liefert aus diesem Grund für die verschiedenen Hersteller zugeschnittene Adapter mit. Mit Hilfe dieser Adapter und dem freigeschalteten Terminal auf der jeweiligen Festplatte ist es möglich, über PC-3000 Express herstellerspezifische Kommandos auszuführen. Für diesen Zweck stellt Seagate zum Beispiel einen eigenen Adapter bereit, während bei Samsung die Schnittstelle hinter den Jumper-Pins zur Festplattenkonfiguration versteckt ist. Da sich die Schnittstelle aber in jedem Fall am PCB der jeweiligen Festplatte befindet und diese mit deutlich niedrigeren Spannungen auskommt als ein verbundener PC, müssen die Adapter oder gegebenenfalls dazwischen geschaltete Pegelwandler auch dafür sorgen, dass die Signalspannungen umgewandelt werden. Das entsprechende Terminal verfügt zudem über verschiedene Modi, um die Geschwindigkeit der Datenübertragung anzupassen (Baud Rate) und muss der Festplatte entsprechend konfiguriert sein. Immer wenn eine Festplatte startet, erzeugt der Bootprozess Statusmeldungen und danach meldet das Terminal Bereitschaft anhand eines herstellerspezifischen Eingabe-Prompts. [10, 13, 52]

Am Beispiel einer Samsung SP2504C P120S fanden Knauer und Baier [10] durch Reverse Engineering heraus, welche herstellerspezifischen Befehle über das Terminal ausgeführt werden können, um den Passwortschutz dieser Festplatte zu umgehen.

Befehl	Beschreibung
`RM Index`	Lädt das Firmware Module `Index` aus dem Servicebereich in den Speicher der Festplatte.
`MW Offset Word [Word ...]`	Schreibt `Word` an Adresse `Offset` im Speicher der Festplatte.
`WM Index`	Speichert den Inhalt des Speichers als Module `Index` im Servicebereich ab.

Tab. 4: Wichtige Terminalbefehle für Samsungs SP2504C P120S

Abbildung 29: Wichtige Terminalbefehle für Samsungs SP2504C P120S [10]

Bereits bekannt ist, dass die Firmware auf der Festplatte in einzelne Module aufgeteilt ist. Dabei werden die Module über einen Index referenziert, der wie bei den verschiedenen Betriebssystemen einem Master File Table (MFT) oder einem File Allocation Table (FAT)

ähnelt. An den ersten vier Datenwörtern jedes Moduls wird seine Bezeichnung gespeichert. So wurde im Falle der Samsung Festplatte an der zweiten Position im Index ein File Information Table (FIT) lokalisiert, der „ein Inhaltsverzeichnis über alle verwendeten Module; mit Index, Name, Größe und der Cylinder-Head-Sektor Adresse“ beinhaltet. [10, S. 9] Anhand der FIT wurde das Modul 16 als Security-Modul identifiziert. Durch den RM Befehl wird das entsprechende Modul aus dem Servicebereich in den Speicher der Festplatte geladen und auf dem Terminal ausgegeben. (siehe Abbildung 29) Der Inhalt auf dem Terminal wird abgespeichert. Danach kann wie bei Abschnitt 2.6.2 beschrieben, ein Benutzer – sowie Masterpasswort für die Festplatte gesetzt werden und das Security-Modul wird erneut ausgelesen und die Inhalte der Module verglichen. Im Falle des Security Moduls beginnen die ausgegebenen Informationen immer fortlaufend am Adress-Offset W:005B00. An Stelle W:005B08 offenbart sich dann im Klartext das Masterpasswort und an Stelle W:005B18 das Benutzerpasswort. [10]

Die beiden bisher nicht berücksichtigten Befehle aus Abbildung 29 können für das Zurücksetzen von Passwörtern gesperrter Festplatten benutzt werden. Sobald das erste Datenwort an den Stellen des Benutzer – sowie Masterpasswortes mit dem Wert Null überschrieben wird, hat das resultierende Passwort eine Länge von Null und ist somit deaktiviert. Dafür wird jeweils ein „MW 5B08 0000“ und ein „MW 5B18 0000“ im Terminal ausgeführt. Um das Passwort dauerhaft zu deaktivieren, wird mit Hilfe des „WM 16“ Befehls das modifizierte Security-Modul in den Servicebereich zurückgeschrieben. „Diese einfache Manipulation der Daten ist nur möglich, weil die Firmware keine Prüfsummen vorsieht, um die Integrität der Daten zu überprüfen.“ [10, S. 10] Zum aktuellen Zeitpunkt könnten allerdings herstellerseitig Maßnahmen ergriffen worden sein, um solche Manipulationen zu verhindern. [10]

Schlussendlich zeigt die Ausführung von ATA-Befehlen, genauso wie die Ausführung herstellerspezifischer Befehle wunderbar, welche Modi und Möglichkeiten PC-3000 Express auf eine bequemliche Art und Weise über seine Benutzeroberfläche bietet. Dazu gesellt sich ein genauso komplexer, aber auch mächtiger Data Extractor, der mit PC-3000 Express und der dazugehörigen Hardware das PC-3000 Express Professionell System bildet. Mit diesem System und auf der Grundlage eines forensischen Leitfadens, werden in den kommenden Abschnitten zwei Fallbeispiele analysiert. Darüber hinaus verdeutlicht besonders dieser Abschnitt nicht nur die Funktionen und Wirkungsweisen des Reparatur – und Wiederherstellungssystems, sondern auch auf welcher komplexen Grundlage, dem Reverse Engineering, für die verschiedenen Hersteller von Festplatten Lösungen entwickelt werden.

3 Forensischer Leitfaden

Grundsätzlich kann der Begriff Leitfaden in Verbindung mit der IT-Forensik auch als Richtlinie der IT-forensischen Arbeit bezeichnet werden. Im Allgemeinen dient ein Leitfaden dem Zweck, einer großen Zielgruppe von Lesern eine Handlungsvorschrift zu präsentieren. Diese Handlungsvorschrift kann dann zur Orientierung in Fällen benutzt werden, in denen der Leser feststellt, dass ein aufgetretenes Problem mit Hilfe des Leitfadens effektiver und zielorientierter behandelt werden könnte. Der hier vorgestellte forensische Leitfaden zu Spezialverfahren der Datenrettung wird noch einmal in drei unterschiedliche Leitfäden gegliedert. Ziel der Leitfäden ist es, dem Leser mit jeder Unterteilung des forensischen Leitfadens eine Konkretisierung in Bezug auf das Thema von Spezialverfahren der Datenrettung zu präsentieren.

3.1 Leitfaden nach BSI

Dieses Kapitel soll den Prozess der Anwendung von Spezialverfahren der Datenrettung innerhalb des vom BSI formulierten Leitfadens zur IT-Forensik beschreiben. Zuerst soll die Bedeutsamkeit und das Zustandekommen des Prozesses gerechtfertigt werden. Danach wird anhand der festgelegten Bestandteile eines IT-Forensik Prozesses herausgearbeitet, welche Bedeutung die jeweiligen Bestandteile für ein Spezialverfahren der Datenrettung haben.

3.1.1 Rechtfertigung von Spezialverfahren der Datenrettung

Das BSI definiert den Begriff der IT-Forensik folgendermaßen:

„IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“ [18, S. 8]

Mit dieser Definition erweitert das BSI die bisherige Auslegung des Begriffes um die „Betrachtungsweise und Einsatzmöglichkeiten aus der Sichtweise des Anlagenbetreibers.“ [18, S. 8] Eine weitere wesentliche Rolle aus Sicht des BSI spielt die strategische Vorbereitung, die genauso gut als Prävention bezeichnet werden könnte. Dadurch soll noch vor dem

Eintreten eines Vorfalls, „die Ergebnisqualität der forensischen Untersuchung“ maßgeblich verbessert werden.“ [18, S. 8] „Ein Beispiel ist das Aktivieren von Logdiensten, welche geeignet scheinen, die Umstände des Vorfalles mit zu protokollieren.“ [53] Als Konsequenz leitet das BSI ab, „dass IT-Forensik bereits mit der strategischen Vorbereitung beginnt.“ [18, S. 8] Für den Prozess der Datenanalyse zur Aufklärung von Vorfällen wird die Vorfallsbearbeitung eingeschlossen, in der wiederum die Bearbeitung von Supportfällen vorgesehen ist. Supportfälle beziehen sich hier auf „Hardware – und Softwareversagen und Fehlbedienung durch den Nutzer.“ [18, S. 8] Die Kombination der strategischen Vorbereitung und des Einbeziehens von Supportfällen soll dazu führen, dass wertvolle Hinweise geliefert werden, wenn die Ursache eines Vorfalls nachträglich als absichtlich herbeigeführte Betriebsstörung erkannt wird. [18]

Im Rahmen der Benutzung eines PC-3000 Express Professionell Systems bei Behörden ist festzustellen, dass für jede Festplatte entweder:

1. Eine absichtlich herbeigeführte Betriebsstörung zugrunde liegt.

Zum Beispiel bei Durchsuchungen:

- aus dem Fenster geworfen
- durch Gegenstand beschädigt
- Brandspuren
- Wasserschaden

2. Ein Supportfall bezüglich einer Festplatte zugrunde liegt, die relevante Daten enthält.

Zum Beispiel:

- Ausfall der Festplatte eines Sachbearbeiters während einer Untersuchung
- Ausfall einer Festplatte, auf der sich eine Hash-Datenbank befindet (kein Backup vorhanden)
- Herunterfallen einer Festplatte während eines Transportes

Damit rechtfertigen sich Spezialverfahren der Datenrettung vor allem in Bezug auf die erwähnten Supportfälle. Dabei weist jede zu untersuchende Festplatte mindestens ein Hardware – oder Softwareversagen auf oder der Supportfall wurde durch Fehlbedienung herbeigeführt. Auch eine Kombination dieser Fehlerarten ist denkbar.

3.1.2 Einordnung von Spezialverfahren der Datenrettung

„Allgemein lässt sich die IT-Forensik in die Post-mortem-Analyse und in die Live-Forensik bezüglich des Zeitpunktes der Untersuchung einordnen.“ [18, S. 13] Bei der Post-mortem-Analyse (auch bekannt als Offline Forensik) wird der Vorfall nachträglich aufgeklärt. Zur Post-mortem-Analyse zählen auch die Spezialverfahren der Datenrettung. Das grundsätzliche Ziel dabei ist, ein Datenträgerabbild der nichtflüchtigen Spuren auf einer Festplatte zu erstellen. Das BSI gliedert eine forensische Untersuchung im Leitfaden in die Vorfallsbearbeitung bzw. Krisenreaktion ein. Diese ist wiederum Teil des Notfallmanagements. „Das Notfallmanagement schließt neben der Vorfallsbearbeitung auch den „Wiederanlauf“ und die „Wiederherstellung“ ein.“ [18, S. 13] Dementsprechend zählen Spezialverfahren der Datenrettung zur „Wiederherstellung.“

„Die Wiederherstellung (die Restauration) soll den vorherigen Zustand (vor dem Auftreten des Vorfalls) herstellen, alle Auswirkungen des Vorfalls beseitigen, also eine De-Eskalation und damit den Normalbetrieb sicherstellen. Selbst im nachfolgenden Normalbetrieb können IT-forensische Untersuchungen von Nöten sein, um das Gesamtbild des Vorfalls zu vervollständigen.“ [18, S. 14] Die Erfahrung bei behördlichen Untersuchungsprozessen hat gezeigt, dass im „nachfolgenden Normalbetrieb“ immer zusätzliche Untersuchungen durchgeführt werden müssen, da so gut wie nie Backups der zu untersuchenden Datenträger vorliegen. Allerdings nimmt die Komplexität eines Spezialverfahrens/Wiederherstellungsprozesses so viel Zeit in Anspruch, dass die im Normalbetrieb nötige IT-forensische Untersuchung/Analyse aus der Prozesskette ausgegliedert wird. Da sowohl bei Durchsuchungen viele Festplatten anfallen als auch im Allgemeinen/bei Behörden viele Festplatten im Einsatz sind, widmet sich eine zuständige Person ausschließlich den Spezialverfahren der Datenrettung. Daraus ergibt sich, dass für diesen Leitfaden nur die ersten drei Bestandteile des IT-Forensik Prozesses nach BSI in Bezug auf Spezialverfahren der Datenrettung relevant sind.

3.1.3 Bestandteile des IT-Forensik Prozesses nach BSI

„Der Leitfaden des BSI unterteilt die Vorgehensweise einer forensischen Untersuchung in die folgenden sechs Abschnitte:“ [18, S. 24]

„1. Strategische Vorbereitung

2. Operationale Vorbereitung

3. Datensammlung

4. Untersuchung

5. Datenanalyse

6. Dokumentation“ [18, S. 24]

1-6: Das BSI empfiehlt zudem eine fortlaufende Dokumentation während allen Abschnitten. [18]

3.1.4 Strategische Vorbereitung

„Zur strategischen Vorbereitung zählt man alle Maßnahmen des Anlagenbetreibers, die im Voraus, in Erwartung eines Vorfalles vor dem Eintreffen des Vorfalles getroffen werden.“ [53] Zunächst einmal ist das Erstellen von Backups der Daten einer Festplatte die beste Möglichkeit der strategischen Vorbereitung. Sollte eine Festplatte ausfallen, kann eine neue, funktionierende Festplatte die Daten aus dem Backup beziehen und das System läuft wieder. Für Privatpersonen ist das wahrscheinlich die beste Möglichkeit um Datenverlust zu vermeiden. Für den behördlichen Einsatz oder für Unternehmen mit einer Spezialisierung im IT-Bereich ist die Erstellung von Backups genauso wichtig. Jedoch ist in diesen Bereichen die Dichte von verwendeten Datenträgern, insbesondere auch Festplatten, deutlich höher. Bekanntermaßen fallen Festplatten ziemlich häufig durch Firmware Fehler aus. Dabei spielt für die Festplatte keine Rolle, wie viele Laufstunden sie hinter sich hat oder wie neu sie ist. Eine relativ neue Festplatte zu ersetzen oder allgemein Festplatten mit Fehlern oft ersetzen zu müssen, wirft damit auch einen finanziellen Aspekt auf. Mit Hilfe von PC-3000 Express könnten solche Fehler oftmals recht einfach behoben werden, ohne die Festplatte durch eine neue ersetzen zu müssen. Darüber hinaus müssen stets Anwendungsfälle für PC-3000 einbezogen werden, in denen kein Backup vorhanden ist.

Aus diesem Grund gilt es im Rahmen von Spezialverfahren der Datenrettung von Festplatten, Maßnahmen der strategischen Vorbereitung zu treffen, die eine Reparatur von Festplatten (z.B. Firmware Fehler) vereinfachen. Eine sehr nützliche Funktion bietet PC-3000 Express durch eine integrierte Datenbank, in der Kopien der wichtigsten Daten einer Festplatte hinterlegt werden. Zusätzlich besteht die Möglichkeit, Logs und wichtige Daten separat zu speichern. Darunter zählen unter anderem Identifikationsdaten eines Laufwerks; der Inhalt des ROM; der Aufbau und die Struktur des Service Bereichs auf den Festplatten, insbesondere der einzelnen Firmware Module; HDD Informationen in Form von Allokationstabellen, Tabellen für die Verwaltung von fehlerhaften Sektoren und so weiter (Alt List, G-List) und das Speichern von S.M.A.R.T Daten.

Des Weiteren ist es sinnvoll, keine Festplatte aus der Hand zu geben, die noch intakte physische Bestandteile besitzt, um sie als Ersatzteilspender zu benutzen. In diesem Zusammenhang ist es ratsam, eine Übersicht für Ersatzteilspender anzulegen, um für einen konkreten Fall ermitteln zu können, ob ein Austausch mit Ersatzteilen in Frage kommt. Ein letzter wichtiger Punkt für die strategische Vorbereitung bezieht sich auf das Wipen von Festplattendaten. Gerade in einem IT-forensischen Prozess spielt die sogenannte „chain of custody“ oder auch Beweismittelkette eine wichtige Rolle. Neben einer vollständigen Dokumentation über den Verbleib eines Datenträgers über mehrere Stationen hinweg, soll die Beweismittelkette vor allem die Integrität von Daten sicherstellen. Eine Festplatte, deren Daten vorher nicht sicher gelöscht wurden, führt dazu, dass eine verfahrensrelevante Sicherung, die auf dieser Festplatte gespeichert werden soll, eine Vermischung der unterschiedlichen Daten verursacht. Damit wäre eine Einbringung des Datenträgers als Beweismittel vor Gericht schwierig.

3.1.5 Operationale Vorbereitung

„Unter operationaler Vorbereitung sind alle Maßnahmen zu verstehen, die zwar nach dem vermuteten Eintreten des Vorfalles aber vor der eigentlichen Datensammlung erfolgen. Beispiele sind die Identifikation und Enumeration potentieller Datenquellen.“ [54] Das BSI schreibt dazu: „[...] was gesichert werden kann, ist es wichtig, sich der Frage, was gesichert werden soll, anzunehmen.“ [18, S. 88] Der Data Extractor sieht dafür zum Beispiel die Ermittlung relevanter logischer Datenspeicherbereiche vor, um die Datensicherung zu beschleunigen und später die Analyse zu vereinfachen. Dafür durchläuft der Data Extractor automatisch relevante Dateisystemstrukturen und kann auf Abruf in kürzester Zeit den Verzeichnisstrukturbaum abbilden. Über diesen können dann selektiv einzelne Dateien logisch gesichert werden, ohne eine physische Kopie des gesamten Datenträgers erstellen zu

müssen. Für die operationale Vorbereitung spielt auch das Stichwort Ersatzteilspender erneut eine Rolle. Wurden Maßnahmen der strategischen Vorbereitung beachtet, kann im Zuge dessen ein Ersatzteilspender ermittelt und beschafft werden. Hierunter zählt auch die Auswahl entsprechender Tools und Hilfswerkzeuge. In Bezug auf Festplatten wäre das Tool der Wahl das PC-3000 Express Professionell System. Hilfswerkzeuge schließen Werkzeuge zum Öffnen einer Festplatte, aber auch die Bereitstellung eines sogenannten Reinraumes ein.

3.1.6 Datensammlung

Im Abschnitt der Datensammlung beginnt die eigentliche Bestandsaufnahme. „Für die Sammlung der Daten werden Werkzeuge aus einem zuvor festgelegten Katalog ausgewählt und angewendet.“ [55] „Prinzipiell wird im Rahmen dieses Untersuchungsabschnitts die Durchführung einer forensischen Duplikation der betroffenen Massenspeicher erforderlich.“ [18, 89] „Die Erzeugung eines forensischen Datenträgerabbildes bildet als Maßnahme der Datensammlung die Grundlage für die nachfolgenden Abschnitte des forensischen Prozesses, insbesondere der Untersuchung und Analyse.“ [18, S. 235]

„Deshalb ergeben sich die folgenden Anforderungen an eine forensische Duplikation:“ [18, S. 26]

• „Physische Kopie - Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben;“ [18, S. 26]

Der Data Extractor ist speziell darauf ausgelegt, diese Art der physischen oder auch bitweisen Kopie für alle zu untersuchenden Festplatten durchzuführen.

• „Fehlerbehandlung - Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden;“ [18, S. 26]

Der Data Extractor erkennt Lesefehler im Rahmen von bestimmten festgelegten Parametern automatisch. Darüber hinaus ist es mit Hilfe des Fine-Tuning durch die Parametereinstellungen sehr oft möglich, entstandene Lesefehler zu korrigieren und die Anzahl erfolgreich gesicherter und gelesener Sektoren zu erhöhen. Da alle Informationen, insbesondere eine Übersicht für fehlerhafte Sektoren, die das Programm generiert, exportiert werden können, ist die Protokollierung von Fehlern in einer Datei problemlos möglich.

• „Vollständigkeit des Abbildes - Reservierte Bereiche von Massenspeichern (bspw. HPA und DCO) müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;“ [18, S. 26]

Hierfür hält PC-3000 Express tatsächlich keine automatische Funktion bereit. Deshalb muss der Benutzer, wie nach Leitfaden des BSI beschrieben, den betroffenen Bereich erkennen. Dabei unterstützen alle Festplatten den ATA Befehl „Read native max address“, der die maximale Anzahl aller auf dem Datenträger befindlichen Sektoren ermittelt. Über „Tools → Device Configuration Overlay“ kann der Befehl „Restore Device Configuration“ (entspricht „Read native max address“) ausgeführt werden und die Ausgabe kann mit dem aktuellen Zustand der Festplatte verglichen werden, um reservierte und nicht ohne weiteres zugängliche Bereiche ausfindig zu machen.

• „Unveränderthеit - Die Erstellung des Abbildes muss mit der Berechnung einer kryptographischen Checksumme abgeschlossen werden, um die Unveränderthеit (Integrität) des Abbildes nachweisen zu können.“ [18, S. 26]

Der Data Extractor bietet die Möglichkeit, Dateien in ein forensisches Format zu konvertieren, in dem die Erstellung von kryptographischen Checksummen automatisch umgesetzt wird.

3.2 Allgemeiner Leitfaden

Dieser Leitfaden soll als eine Handlungsempfehlung für den allgemeinen Umgang mit Festplattenproblemen dienen. Hierbei können sowohl private Anwender, die selbst Probleme mit einer Festplatte feststellen, als auch Personenkreise, die sich täglich mit Festplatten auseinandersetzen, profitieren.

3.2.1 Erste Maßnahmen bei Festplattenproblemen

Als erste Maßnahme im Zusammenhang mit Festplattenproblemen gilt natürlich, die Festplatte bei Problemen nicht weiter zu betreiben und dadurch zusätzliche Probleme zu provozieren. Wenn noch während des Betriebs ungewöhnliche Geräusche vernommen werden, diese unbedingt so detailliert wie möglich merken oder notieren und dazu bereit sein, die Festplatte sofort abzuschalten. Bei ausreichendem technischen Grundverständnis kann die Festplatte ausgebaut werden. Im Zuge dessen ist es ratsam, Basisinformationen zur Festplatte, falls vorhanden, wie Hersteller, Seriennummer, et cetera zu erfassen. Anschließend könnte man die Festplatte augenscheinlich auf Schäden untersuchen und eventuell

das PCB abschrauben und analysieren. Das PCB verbindet viele Einzel – und Kleinteile miteinander. Manche Schäden können deshalb nur mit Hilfe einer Lupe eindeutig erkannt werden, wie zum Beispiel kleine Risse der Chips. Ein Blick auf die SATA/PATA-Anschlüsse (oder ähnliches), genauso wie die Kontrolle der sogenannten Jumper Pins kann Hinweise liefern. Ebenso könnten Bestandteile durch Korrosion in Mitleidenschaft gezogen worden sein. Das gilt vor allem häufig für die Verbindung des PCB´s zur Kopfteilbaugruppe. Darüber hinaus können auch ein verbrannter Geruch und/oder vernommene Geräusche aus dem Inneren der Festplatte wertvolle Hinweise liefern. Sollte ein Ausbau der Festplatte nicht möglich sein, ist vor allem wichtig, die Reaktion des Computersystems zu beobachten und gegebenenfalls Notizen zu erstellen. Beispielhaft für das weit verbreitete Betriebssystem Windows, aber auch alle anderen Betriebssysteme wäre relevant: [56]

- Hat das System vor oder während des aufgetretenen Problems sehr langsam reagiert oder sich aufgehangen? Dann könnte man bereits vermuten, dass sich die Fehlerquelle in fehlerhaften Sektoren oder schwachen Köpfen äußert.

- Das Betriebssystem gibt eine Fehlermeldung aus oder reagiert gar nicht mehr; dann kann man davon ausgehen, dass ein schwerwiegenderer Fehler, wie defekte Service-Bereich Module oder defekte Komponenten der Festplatte die Ursache sind.

Sollte eine Person mit einer zu untersuchenden Festplatte derartige Erkenntnisse nicht im Vorfeld notiert haben, sollten diese unbedingt im Vorfeld einer Analyse durch den jeweiligen Experten erfragt werden. Dabei ist relevant:

- wann und wie das Problem aufgetreten ist

- was mit der Festplatte passiert ist (Geräusche etc.)

- ob sich die Festplatte noch gedreht hat

- Zugang zu Benutzerdaten noch möglich war

- Identifikationsdaten der Festplatte korrekt erkannt werden

- ob die Festplatte vorher bei anderen Experten war oder selbst Versuche zur Lösung des Problems unternommen wurden

- welche Daten auf der Festplatte besonders relevant für den Besitzer sind

Wenn aus den eben erwähnten Fragen hervorgeht, dass die Festplatte heruntergefallen ist oder in Kontakt mit Wasser kam, gilt allgemein und für Experten ausdrücklich, die Festplatte nicht zu betreiben und zunächst das Innere der Festplatte zu prüfen und ggf. zu reinigen. Auch ohne eindeutige Hinweise eines Besitzers auf diverse schädliche Szenarien für Festplatten, sollte die Festplatte von einem Experten vor dem erneuten Betrieb gründlich untersucht werden. Hier könnte der Experte zum Beispiel bei entsprechenden Hinweisen neben einem Mikroskop auch ein Spannungsmessgerät für das PCB einsetzen, um elektrische Probleme der Komponenten auszuschließen. [56]

3.3 Leitfaden nach ACE Lab

Der Leitfaden nach ACE Lab geht im Gegensatz zum Leitfaden nach BSI auf konkrete Fehlerarten von Festplatten ein. Für jede mögliche Fehlerart, werden Ansätze und Möglichkeiten beschrieben, den Fehler oder eine Kombination aus Fehlern mit Hilfe von PC-3000 Express zu korrigieren.

3.3.1 Allgemeines zu Fehlern

Wenn eine zu untersuchende Festplatte in keiner Hinsicht startet und ihre Platten nicht dreht, sollte grundsätzlich folgendes untersucht werden:

1. Die Köpfe im Inneren des Laufwerks berühren die Platten/stecken fest

2. Das Laufwerk besitzt eine falsche ROM Version oder das PCB ist nicht original

3. Der Spindelmotor ist defekt [57]

3.3.2 Erste Fehlerart

Die Festplatte dreht beim Startvorgang, erzeugt aber mehrere Klick/Tickgeräusche und daraufhin stoppt der Spindelmotor – Die Register DRD, DSC und ABR sind aktiv

Grundsätzlich bedeutet diese Art von Fehler, dass die Köpfe Servoinformationen nicht lesen können. Daraus ergibt sich, dass einer oder mehrere Köpfe defekt sind und wahrscheinlich ausgetauscht werden müssen. Wenn das Laufwerk zwar anfangs Klick/Tickgeräusche verursacht, dann aber doch weiterläuft und Bereitschaft meldet, heißt das, dass einer oder mehrere Köpfe schwach sind, aber zunächst Daten gesichert werden können, ohne die Köpfe zu tauschen. Nichtsdestotrotz müssen nicht immer zwangsweise die Köpfe für den Fehler verantwortlich sein. Darüber hinaus können folgende Fehler zugrunde liegen:

A) Das PCB ist die Schwachstelle und erzeugt den Fehler. Um den Fehler konkret zu ermitteln bzw. auszuschließen, könnte das PCB eines Spenders benutzt werden. Dafür wird der ROM des Patienten auf das Spender PCB übertragen und das Spender PCB in den Patienten gesetzt. Sollte die Festplatte dann immer noch die Geräusche verursachen, liegt der Fehler nicht im PCB.

B) Der ROM ist nicht original. Wenn ein Zugriff auf den Servicebereich möglich ist, kann die ROM Firmware Version mit einem bestimmten Modul aus dem Servicebereich verglichen werden.

C) Die Headmap ist inkorrekt. Normalerweise ist es einer Festplatte selbst nicht möglich, ihre Headmap zu verändern. Aus diesem Grund kann nur in Frage kommen, dass das PCB oder ROM nicht original sind oder ein voriger Benutzer die Headmap der Festplatte manuell geändert hat. [57–59]

3.3.3 Zweite Fehlerart

Schwache oder defekte Köpfe

Die zweite Fehlerart könnte gleichzeitig die erste Fehlerart sein und umgekehrt. Da die Köpfe in einer Festplatte aber das wohl empfindlichste Bauteil darstellen, soll sich die zweite Fehlerart ausschließlich mit einem Fehler der Köpfe beschäftigen. Zudem treten Fehler der Köpfe relativ häufig auf. Hierbei ist vor allem wichtig herauszufinden, welcher Kopf oder Köpfe betroffen sind. Die einfachste Methode, die PC-3000 Express für diesen Fall bereithält, ist der sogenannte „Heads Test." Auswählbar über „Tests ⇒ Service information ⇒ Work with SA (Service Area) ⇒ Heads Test." Dabei versucht das Laufwerk chronologisch für jeden Kopf in einen bestimmten Bereich Testdaten zu schreiben und diese anschließend wieder zu lesen. Wenn diese Methode nicht zur Ermittlung eines schlechten Kopfes führt, gibt es eine zweite Möglichkeit über „Work with RAM ⇒ RAM headmap editing." Über den RAM können temporär bestimmte Köpfe deaktiviert werden, um so mittels Trial and Error Prinzip den schlechten Kopf zu ermitteln. Dabei gilt dann für einen deaktivierten Kopf, dass alle Zugriffe, die über den Kopf laufen würden, über einen der aktiven Köpfe geleitet werden. Eine weitere Möglichkeit zum Prüfen der Köpfe wäre ein manueller Test. Im Service Bereich existieren bestimmte „System-Dateien" mit einer bestimmten ID, die einen „Drive self test head [Nummer des Kopfes]" enthalten und ausgeführt werden können. [57–59]

3.3.4 Dritte Fehlerart

Die Festplatte startet ohne Geräusche, aber die Identifikationsdaten sind fehlerhaft oder nicht vorhanden

Wenn die Modellnummer, die Seriennummer, die Firmware Version oder die Kapazität eines Laufwerks falsch angezeigt werden oder nicht gefunden werden konnten, heißt das, das Laufwerk konnte seine Service Daten nicht lesen. Es könnte aber auch daran liegen, dass die Service Daten gelesen werden konnten, aber das Übersetzermodul fehlerhaft ist. In jedem Fall sollte zunächst geprüft werden, ob Service Daten gelesen werden können. Eine Festplatte wird immer zuerst versuchen, die Firmware Informationen (Module der Service Daten) via ATA zu lesen. Wenn sich die Festplatte während des Leseprozesses aufhängt, können alternative Methoden zum Auslesen angewendet werden. Einerseits gibt es die Möglichkeit, die Module über das Terminal mit Hilfe des Werksmodus auszulesen. Sollte auch diese Möglichkeit nicht durchführbar sein, kann eventuell ein Teil der Firmware über einen speziellen Boot Code Modus ausgelesen werden. Unabhängig von der Methode zum Auslesen und der Familie und Firmware Version des Laufwerks, befinden sich die relevanten Firmware Module in den meisten Fällen an der gleichen Position. Wurde die Festplatte im Rahmen einer strategischen Vorbereitung schon einmal untersucht und ein Backup der Service Daten erstellt, könnte man auch auf diese Weise Zugriff auf die Service Daten erlangen. Dieselbe ROM Firmware Version eines Spenders wäre ebenfalls denkbar. Dabei gilt es zu beachten, dass die Service Daten immer einen sogenannten „DIR“ und „Loader“ voraussetzen. „DIR“ ist theoretisch das erste SA Modul 01 und enthält eine Liste über alle Module, deren Adressen und weitere Parameter. Der „Loader“ ist ein zusätzlicher Teil des Programmcodes, der benötigt wird, um mit den Service Daten zu arbeiten. Sobald Service Daten auf die eine oder andere Weise gelesen werden konnten, gilt es die einzelnen Module zu analysieren. In der Regel markiert PC-3000 Express beschädigte Module entsprechend und so können sie leicht identifiziert werden. Um sie zu erneuern, kann ein einzelnes Modul aus einem Backup neu geschrieben werden. Wenn das Überschreiben eines Moduls misslingt und verschiedene andere Fehler zusätzlich auftreten, kann es sein, dass der Service Bereich zu viele fehlerhafte Sektoren enthält. Dann wird es nötig sein, die Adresse des beschädigten Modules auf einen nicht fehlerhaften Bereich zu mappen. [57–59]

3.3.5 Vierte Fehlerart

Die Festplatte startet sehr langsam, hängt sich im BUSY Status auf und kommt nicht mehr zur Bereitschaft

In den meisten Fällen wird dieser Fehler ausgelöst, weil die Festplatte versucht, ein beschädigtes SA Modul zu lesen. Durch Fehler oder Abnutzung kann es aber auch sein, dass die Schreibfähigkeit eines Kopfes mit der Zeit abnimmt. Daraus folgt, dass die Firmware irgendwann feststellt, dass im Servicebereich viele fehlerhafte Sektoren auftreten. Diese möglicherweise fehlerhaften Sektoren werden in die Tabellen für fehlerhafte Sektoren aufgenommen. Mit der Zeit denkt die Firmware, dass immer mehr Sektoren fehlerhaft sind und fügt sie der Liste hinzu, die sich mit „Fake-Fehlern“ füllt. Bei der nächsten Initialisierung hängt sich die Firmware dann auf und blockiert den Zugriff auf Benutzerdaten. Um diesen Fehler zu lösen, lässt sich mit Hilfe von PC-3000 Express der Zugriff auf den Servicebereich blockieren. Anschließend lädt man einen neuen DIR und Loader über den RAM, sendet einen Software Reset und mit Hilfe von DIR und Loader kann sich die Festplatte mit „Default-Daten“ selbst identifizieren. Danach sichert man die Module nach ihren physischen Adressen und nicht den durch die Fehlertabellen umgemappten Adressen und hebt die Blockierung wieder auf. Nach einem Neustart sollte der Fehler korrigiert sein. [57–59]

3.3.6 Fünfte Fehlerart

Die Festplatte startet normal, liest alle Identifikations-Daten korrekt und alle Module der Servicedaten sind in Ordnung, aber trotz allem kein Zugriff auf Benutzerdaten möglich

Die vielen fehlerhaften Sektoren im Servicebereich aus dem vorangegangen Beispiel könnten genauso im Bereich der Benutzerdaten auftreten und dadurch die Festplatte einfrieren. Des Weiteren müssen alle Köpfe während der Initialisierung einer Festplatte einen „Head Test“ bestehen, wobei ihre Schreib – und Lesefunktionalität geprüft wird. Wenn einer der Köpfe zu schwach ist und Lese – oder Schreibprobleme hat, wird die Festplatte den Zugriff auf Benutzerdaten sperren, obwohl alle anderen Köpfe einwandfrei funktionieren. Manchmal schaffen es die Köpfe auch, die Initialisierung zu meistern und Service Daten zu lesen, sind aber zu schwach, um mit den Benutzerdaten zu arbeiten. Hier kann es wieder nützlich sein, die Köpfe mit Hilfe der „Headmap“ im RAM zu modifizieren und auf Fehler zu testen. [57–59]

4 Vorgehen Beispiel 1

Dieses Kapitel beschreibt die Vorgehensweise bei der Vorbereitung und Durchführung zu Spezialverfahren der Datenrettung für das erste ausgewählte Beispiel.

4.1 Ausgangslage/Symptome

Ein Mitarbeiter der Polizei in Berlin besitzt einen privaten Laptop mit personenbezogenen Daten. Aus diesem Laptop wurde die Festplatte selbstständig ausgebaut und mit Hilfe eines externen Gehäuses als gelegentlicher Datenspeicher benutzt. Im Laufe des Monats August 2021, bei einer Benutzung der Festplatte, wurde dann festgestellt, dass die Festplatte nicht mehr funktioniert. Am 08.09.2021 gelangt die Festplatte über Kontakte innerhalb der Polizei Berlin zur zuständigen Person für Spezialverfahren der Datenrettung. Zuvor hatte die Privatperson bereits ein Datenrettungsunternehmen damit beauftragt, eine erste Fehleranalyse für die Festplatte durchzuführen. Dabei wurde angeblich festgestellt, dass einer oder mehrere Köpfe der Festplatte defekt wären. Der Besitzer der Festplatte wurde darauf verwiesen, dass eine Reparatur ohne eine Garantie auf Rettung der Daten für circa 950 Euro durchgeführt werden könnte.

4.2 Strategische Vorbereitung

Die strategische Vorbereitung im beschriebenen Fall gestaltete sich schwierig, da der eigentliche Besitzer der Festplatte solche Maßnahmen bisher nicht vorgesehen hatte. Trotz alledem wurden zur späteren Verwendung die Basisdaten der Festplatte ermittelt (siehe Tabelle 6 und 7) und im weiteren Verlauf entsprechende Backups der Festplatten erstellt.

4.2.1 Der Patient

Im nachfolgenden Beispiel wird die Festplatte nur noch als „Patient“ bezeichnet.

Bei der Festplatte handelt es sich um eine 2,5 Zoll große Festplatte des Herstellers Seagate. (siehe Abbildung 30)

Tabelle 6: Übersicht Basisdaten Patient

Bezeichnung	Beschreibung
Modell	ST9500325AS
Seriennummer	5VEETRT0
Firmware Version	0006SDM2
Kapazität	500 GB
Herstellungsland	China
Herstellungsdatum	Dienstag, 7. Dezember 2010
Preamp-Nummer	5A-35
Site	WU
Part-Nummer	9HH134-142
Architektur	F3-Architektur
Familie	3C Wyatt
Headmap	4
Umdrehungen	5400

Abbildung 30: Patienten Festplatte Frontalansicht

4.2.2 Der Spender

Im nachfolgenden Beispiel wird die Festplatte nur noch als „Spender“ bezeichnet.

Bei der Festplatte handelt es sich um eine 2,5 Zoll große Festplatte des Herstellers Seagate. (siehe Abbildung 31)

Tabelle 7: Übersicht Basisdaten Spender

Bezeichnung	Beschreibung
Modell	ST9500325AS
Seriennummer	5VELY7AS
Firmware Version	0006SDM2
Kapazität	500 GB
Herstellungsland	China
Herstellungsdatum	Donnerstag, 22. September 2011
Preamp-Nummer	5A 14

Tabelle 7 (Fortsetzung): Übersicht Basisdaten Spender

Site	WU
Part-Nummer	9HH134-142
Architektur	F3-Architektur
Familie	3C Wyatt
Headmap	4
Umdrehungen	5400

Abbildung 31: Spender Festplatte Frontalansicht

4.3 Operationale Vorbereitung

Mit Hilfe der Webseite https://www.donordrives.com [60] wurde „der Spender“ als in Frage kommendes Spenderlaufwerk ermittelt. Dabei gilt es zu beachten, dass ein in Frage kommender Spender nicht automatisch bedeutet, dass die Ersatzteile auch wirklich kompatibel mit dem Patienten sind. Viele Parameter können oftmals bereits auf dem Label des Herstellers, dass sich auf der Festplatte befindet, eingesehen werden. Die Preamp-Nummer lässt sich im Vergleich zu den restlichen Parametern nicht so leicht ermitteln. Dafür wurde

im Beispiel die Festplatte mit PC-3000 Express verbunden. Eine Variante würde vorsehen, den ROM auszulesen. Dieser speichert an einer bestimmten Stelle die Preamp-Nummer. Die andere hier durchgeführte Variante arbeitet mit dem Terminal. Dazu wird das Terminal über STRG Z aktiviert und mit Hilfe von STRG L werden allgemeine Informationen zur Festplatte, wie die Preamp-Nummer, ausgegeben. (siehe Abbildung 32)

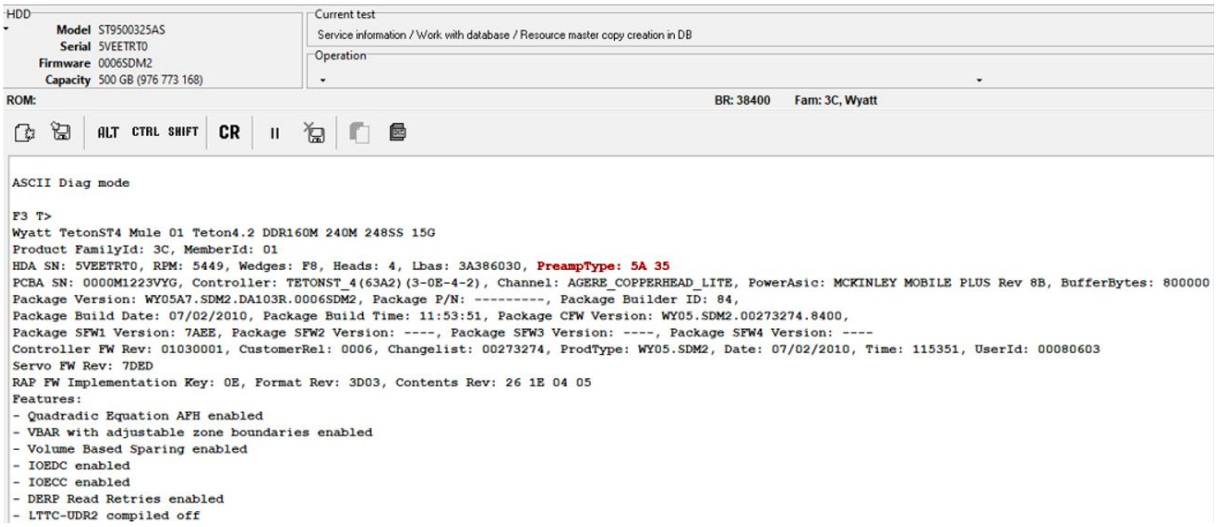


Abbildung 32: Ausgabe des Terminalbefehls STRG L bei Seagate Festplatten [8]

Folgende Parameter wurden bei der Ermittlung des Spenders einbezogen:

- gleiche Modellnummer

- zweites und drittes Zeichen der Seriennummer müssen übereinstimmen

- gleiches Herstellungsland

- Herstellungsdatum sollte möglichst nicht weiter als 3 Monate abweichen, aber ein späteres Herstellungsdatum ist grundsätzlich besser

- Preamp-Nummer: die ersten beiden Zeichen müssen übereinstimmen (Nummer des Chips, der an der Armelektronik sitzt)

- Site = Herstellerfabrik muss gleich sein

- Part-Nummer: die erste Hälfte der Partnummer (vor dem Bindestrich) muss übereinstimmen

- gleiche oder größere Headmap (Anzahl der Köpfe)

4.3.1 Verwendete Software und Hardware

Software:

- PC-3000 Express Professionell System

- PC-3000 Express zur Analyse und Reparatur der Festplatte

- Data Extractor zur Fehlerbehandlung und Datensicherung

- https://www.donordrives.com [60]

- zur Ermittlung eines kompatiblen Ersatzteilspenders

Hardware:

- PC-3000 Express Professionell System

- PC-3000 Express Erweiterungs-Board fest verbaut in einen Untersuchungsrechner

- Terminal Board mit Terminal Adapter für Seagate SATA Festplatten (siehe Abbildung 33)

- Datenübertragungskabel (siehe Abbildung 33)

- Stromzufuhrkabel (siehe Abbildung 33)

- Untersuchungsrechner

- Microsoft Windows 10 Pro, x64-basierter PC

- Intel® Core™ i7-8700 CPU @ 3.20 GHz, 3192 MHz, 6 Kern(e), 12 logische(r) Prozessor(en)

- 64 GB RAM

- 512 GB SSD Systempartition, 2 TB SSD Datenspeicher, 2x 4 TB Festplatten Datenspeicher und 4 interne Festplattenanschlüsse

- *Spender Festplatte mit Ersatzköpfen* (siehe Abbildung 31)

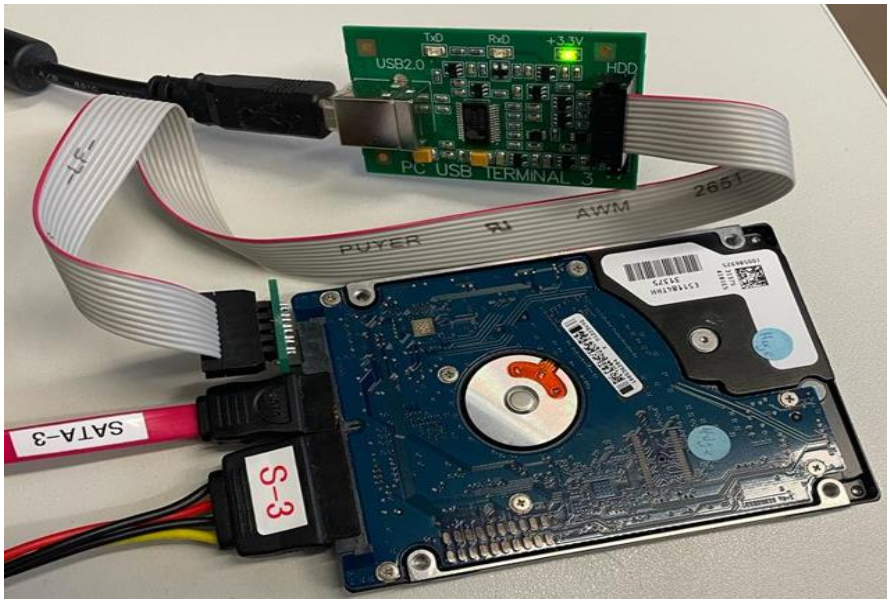


Abbildung 33: Anschlüsse des Patienten an das PC-3000 Express System

4.3.2 Verwendete Werkzeuge

- Handschuhe

- Reinraum-Gerät der Firma Schulz Lufttechnik GMBH

- Schraubenzieher

- Magnetstab (um die Magnete der Festplatte anzuheben)

- Pinzette

- Abstandhalter für die Zwischenräume der Köpfe (beim Wiedereinsetzen)

- Luftpuster (um Staubpartikel von der Oberfläche der Platten zu entfernen)

4.4 Analyse der Fehlerquelle

Nach einer augenscheinlichen Untersuchung der Festplatte wurden keine äußerlich erkennbaren Schäden festgestellt. Auf die gleiche Weise wurde das PCB untersucht und ergab keine Hinweise auf offensichtliche Beschädigungen. Nach dem Verbinden der Festplatte mit PC-3000 Express konnten deutliche Klick/Tickgeräusche wahrgenommen werden und die Festplatte konnte keinerlei Identifikationsdaten ausgeben. Das bedeutet also, dass die Festplatte keinen Zugriff auf ihre Service Daten hat. In Verbindung mit den Klick/Tickgeräuschen, die die Festplatte erzeugt, wurde ein defekter Kopf vermutet. Daraufhin wurden Maßnahmen zur Prüfung der Köpfe eingeleitet, die ergaben, dass Kopf 2 der Festplatte defekt ist.

4.5 Datensammlung

Nachdem anhand des Leitfadens die Fehlerquelle der Festplatte eingegrenzt wurde, können mit Hilfe von PC-3000 Express und dem Data Extractor Schritte zur Lösung des Problems eingeleitet werden. Eine grundlegende Zielstellung sollte immer beinhalten, dass neben der Wiederherstellung von Daten und der Funktionalität der Festplatte, ein Backup der Firmware und anderer relevanter Bestandteile erstellt wird. Zukünftig können damit erneut auftretende Fehler effektiver behoben werden.

4.5.1 Initialisierung und Fehlermeldungen

Zunächst wird die Festplatte wie gewohnt über den Startbildschirm von PC-3000 Express mit Hilfe der „Autodetection“ initialisiert. Dabei wird die F3 Architektur erkannt und die Familie 3C Wyatt zugeordnet.

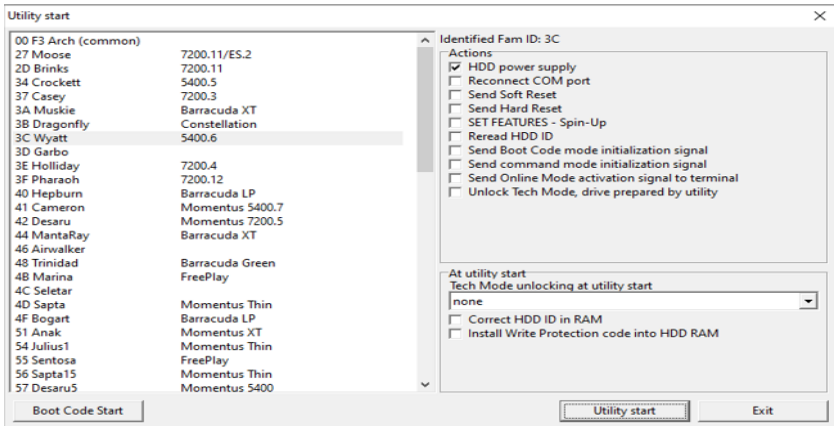


Abbildung 34: Initialisierungsfenster PC-3000 Express (3) [8]

Nach Bestätigung von „Utility start“ erwartet den Benutzer bereits die erste Fehlermeldung:

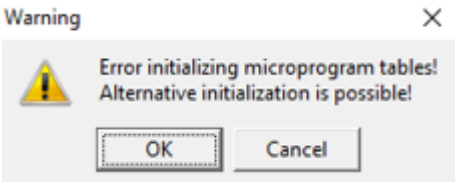


Abbildung 35: Fehlermeldung [8]

Die Festplatte findet demnach nicht genügend Daten um erwartungsgemäß zu starten. Dennoch wird eine alternative Initialisierung angeboten.

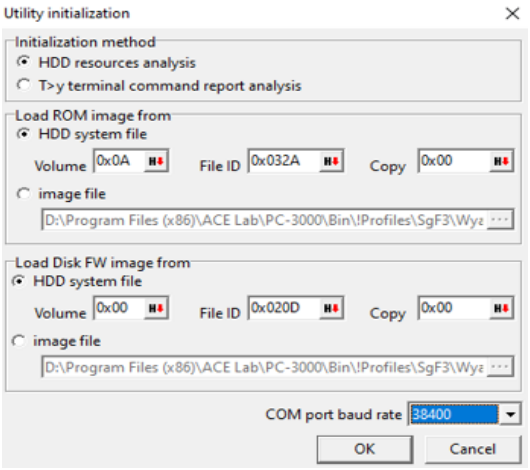


Abbildung 36: Alternative Initialisierung [8]

Diese alternative Initialisierung wird mit Hilfe von „HDD resources analysis“ ermöglicht. (siehe Abbildung 36) ACE Lab sind spezielle „system files“ innerhalb bestimmter Register bekannt, aus denen Teile des „ROM image“ und des „Disk FW image“ geladen werden können. (siehe Abbildung 36) In der Regel ist es dadurch möglich, obwohl kein Zugriff auf den Service Bereich besteht, bestimmte SA Module zu lesen. Mit der alternativen Initialisierung über das Terminal (T>y terminal command report analysis) (siehe Abbildung 36) könnte ausschließlich der ROM ausgelesen werden. Ohne weitere Fehlermeldungen im Startprozess kann der Benutzer jetzt zumindest mit der Festplatte in einem fehlerhaften Zustand arbeiten. Den fehlerhaften Zustand erkennt man neben einigen Fehlermeldungen im Log Tab vor allem an den HDD Identifikationsdaten. Man beachte die unrealistischen 0 MB Kapazität und die unvollständige Firmware Version. (siehe Abbildung 37)

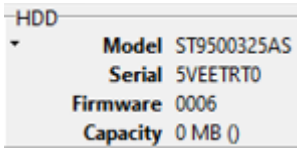


Abbildung 37: Fehlerhafte Identifikationsdaten [8]

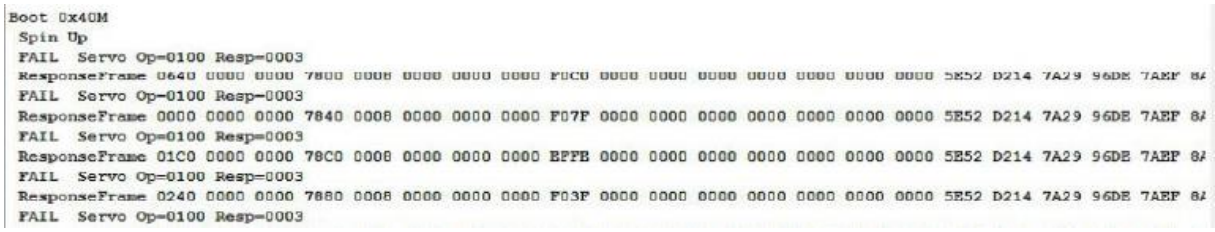


Abbildung 38: Fehlermeldungen (2) [8]

```
LED:000000CC FAddr:00259AD7
LED:000000CC FAddr:00259AD7
Rst 0x08M
RW cmd 002F req = 18 F0 9F E5 18 F0 9F E5 18 F0 9F E5 18 F0 9F E5 18 F0 9F E5 00 00 A0 E1
           opts = 00000000

RW Err = 84150180
```

Abbildung 39: Fehlermeldungen (3) [8]

Wie zu erwarten, erhält der Benutzer eine ganze Reihe von „Servo Fehlern“, „False Address“ Fehlern und „Read/Write-Command-Fehlern“ sowie „Read/Write-Error-Meldungen“. Allesamt weisen den Benutzer darauf hin, dass bestimmte Daten nicht gelesen werden können. (siehe Abbildungen 38 und 39)

Diese Daten beziehen sich vor allem auf die Firmware, die sich im Inneren der Festplatte befindet und verhindern eine Kommunikation über ATA Kommandos. Da in diesem Moment die einzige erreichbare Komponente der Festplatte das PCB darstellt, bietet PC-3000 Express für diese Fälle spezielle ROM Feature. Das heißt zumindest der kleinere Teil der Firmware auf dem PCB, entweder im Flash Chip oder dem Mikrocontroller, kann aus dem ROM gelesen werden. [61] (siehe Abbildung 40)

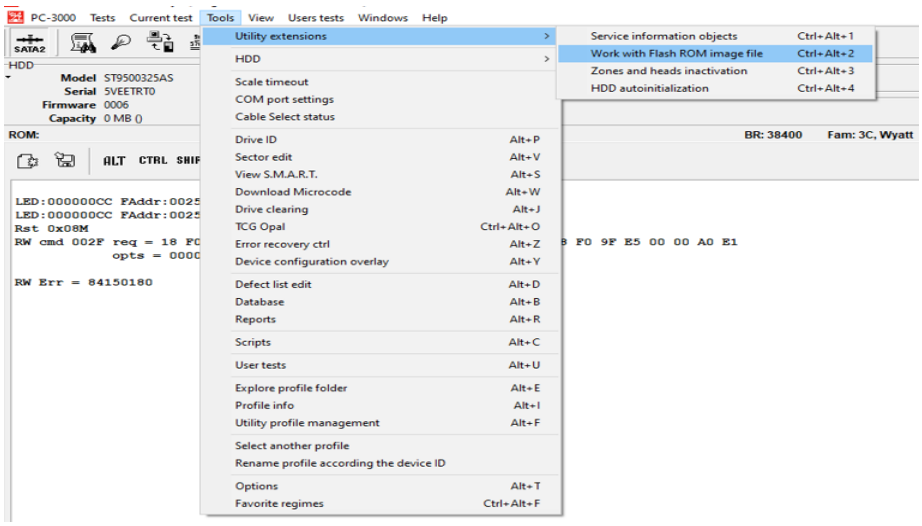


Abbildung 40: Work with Flash ROM image file [8]

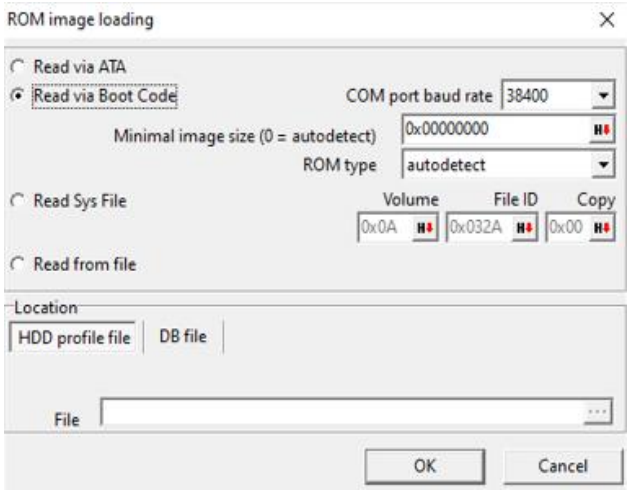


Abbildung 41: ROM image loading [8]

4.5.2 Der Boot Code Modus

Standardmäßig würde die Festplatte das Auslesen des ROM über ATA Kommandos ausführen. Da im vorliegenden Fall aber nicht möglich, soll die Festplatte das „ROM image“ im sogenannten Boot Code Modus lesen. (siehe Abbildung 41) Boot Code ist Teil des ROM und über den Boot Code Modus wird die Festplatte in einen sehr eingeschränkten Betriebszustand versetzt. Boot Code im Allgemeinen kann sehr unterschiedlich ausfallen und ist stark von den verbauten Komponenten in einem System abhängig. Unabhängig davon führt jedoch jeder Boot Code prinzipiell die gleichen Funktionen aus, die im Wesentlichen die Hardware, Busse und den Speicher initialisieren, Interrupts deaktivieren und den Prozessor in einen bestimmten Zustand versetzen. Der erste Hardwareinitialisierungsschritt beinhaltet vor allem das Laden und die Ausführung von Gerätetreibern. Erst nach dieser

Hardwareinitialisierungssequenz wird die verbleibende Software, falls vorhanden, initialisiert. [62] PC-3000 Express liest also im Boot Code Modus den ROM und kann dadurch relevante Informationen filtern. Normalerweise verlangt das Versetzen der Festplatte in den Boot Code Modus einen physischen Eingriff durch den Benutzer. Dafür sollen bestimmte Pins auf dem PCB kurzgeschlossen werden, um den Boot Code Modus zu aktivieren. (siehe Abbildung 42) Die Erfahrung hat allerdings gezeigt, dass oft kein Kurzschluss notwendig ist, um an entsprechende ROM Informationen zu gelangen, wenn die Kommunikationsgeschwindigkeit (Baud rate) des Terminals auf eine Standard Rate von 38400 gesetzt ist. Womöglich führen schnellere „Baud rates“ zu einer Überlastung in der Prozesskette und erzeugen damit Fehler. Gegenüber einem physischen Eingriff auf dem PCB ist diese Variante jedoch deutlich schonender für die Festplatte, wenngleich das Einlesen dann einige Zeit in Anspruch nimmt. [61]

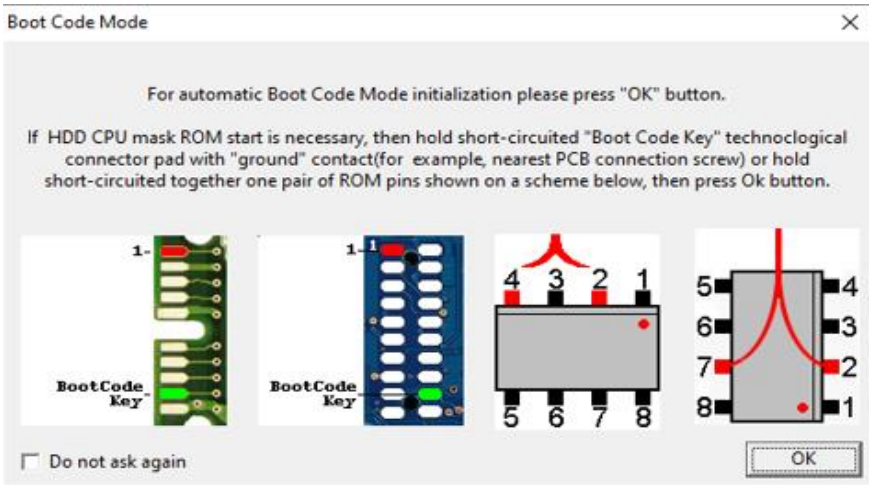


Abbildung 42: Boot Code Modus Initialisierung [8]

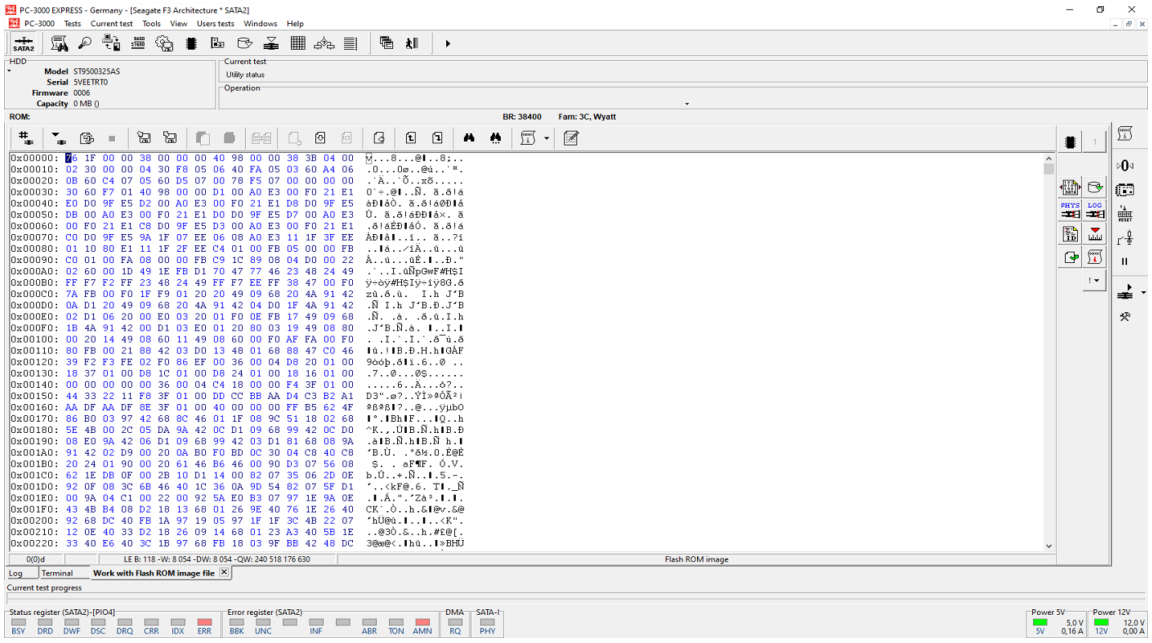


Abbildung 43: Zusätzliche Funktionen im Flash ROM image file Tab [8]

Nachdem der ROM gelesen wurde, sind für den Benutzer auf der rechten Seite zusätzliche Funktionen verfügbar. Vorher wird allerdings der Inhalt des originalen ROM gesichert. [61]

4.5.3 SAP Control Flags und Max Head

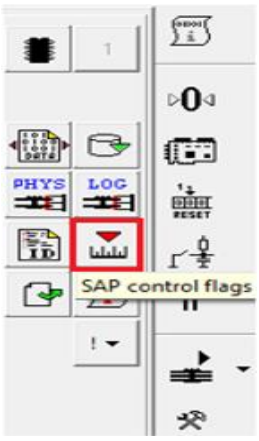
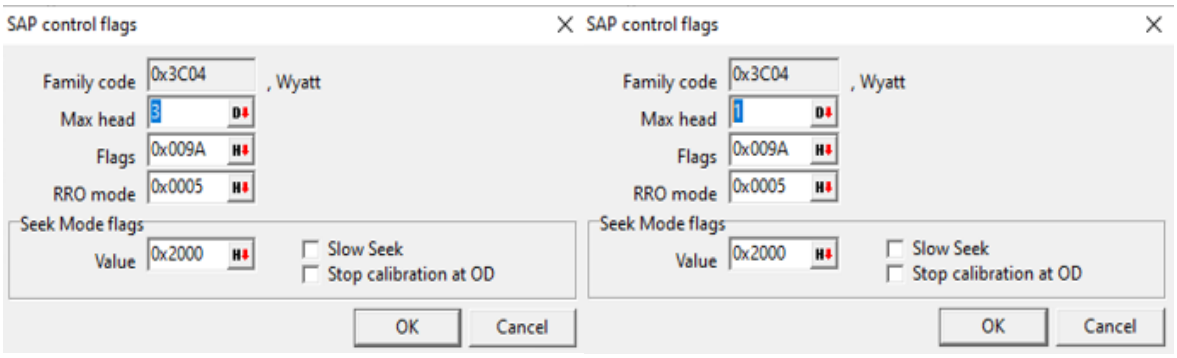


Abbildung 44: SAP control flags [8]

Über die Funktion der SAP (Servo Adaptive Parameters) Control Flags sind nun entscheidende Informationen, wie die maximale Anzahl physikalischer Köpfe der Festplatte, einsehbar. (siehe Abbildungen 45 und 46) Solche Flags sind dazu in der Lage, zur Laufzeit eines Gerätes bestimmte Funktionen zu aktivieren oder zu deaktivieren, ohne die Anwendung oder das Gerät neu starten zu müssen. In diesem Fall werden sie dazu verwendet, die Codebereitstellung innerhalb des Boot Codes zu verändern. Die Vermutung liegt bereits

nahe, dass ein defekter Lesekopf der Festplatte die Fehlerquelle ist. Mit Hilfe der Control Flags ist der Benutzer jetzt dazu in der Lage, nach Belieben bestimmte Köpfe zu aktivieren oder deaktivieren. Konkret heißt das, dass je nach ausgewählter Anzahl maximaler Köpfe, von den vorhandenen vier physikalischen Köpfen, nur noch ein, zwei oder drei aktiv sind. Der Hintergrund lässt sich einfach begründen. Mit Hilfe dieser Funktion wurde nach dem Trial and Error Prinzip Kopf 2 als defekt ermittelt. Dabei wurde der Festplatte zunächst mitgeteilt, dass sie nur noch einen aktiven Kopf (Kopf 0) hat und mit Hilfe des Kommandos „Heads Test“ versucht, Testdaten zu schreiben und zu lesen. Analog wurden dann weitere Köpfe aktiviert und getestet. Grundsätzlich gilt für Seagate Festplatten, dass, sobald ein Fehler im Betriebsprozess auftritt, die Festplatte in einen Zustand übergeht, in dem sie nicht mehr funktionsfähig ist. Einerseits ist diese Art der Fehlerbehandlung gut, denn dadurch können bei sehr sicherheitskritischen Fehlern Folgefehler verhindert werden. Andererseits ist es nachteilig, da die Funktionalität des Laufwerks bei jeglicher Art von Fehler nicht mehr gewährleistet wird und Seagate Festplatten deshalb am Häufigsten eine spezielle Fehleranalyse benötigen. Im konkreten Fall ist außerdem von Vorteil, dass der defekte Kopf 2 keinen Systemkopf darstellt. Systemköpfe sind in der Regel die ersten beiden Köpfe, sprich Kopf 0 primär und Kopf 1 mit einer entsprechenden Kopie sekundär. Diese beiden Köpfe lesen auf ihrer Platte die zur Initialisierung benötigten Service Daten. Wären sie defekt, könnte man selbst mit Hilfe der Flags keine Daten von den Köpfen lesen, sondern müsste direkt versuchen, die Köpfe auszutauschen. Mit dem Wissen über den defekten Kopf 2, werden die entsprechenden Anpassungen vorgenommen. [61]



Abbildungen 45 und 46: Änderung von Max head [8]

Bei „Max head“ wird von standardmäßig 3 (Kopf 0-3 = 4 Köpfe) auf 1 (Kopf 0-1 = 2 Köpfe) umgestellt. (siehe Abbildungen 45 und 46) Anschließend wird die Veränderung im ROM zurückgeschrieben. (siehe Abbildung 47)

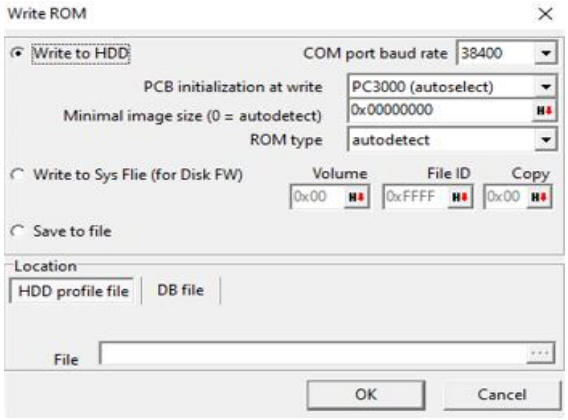
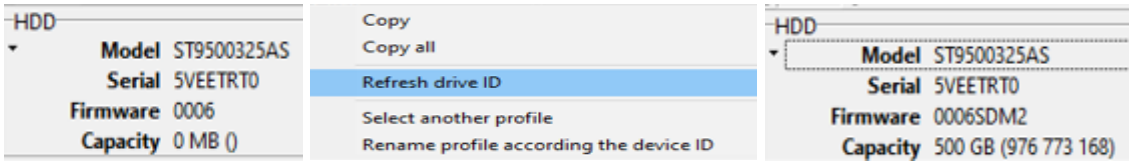


Abbildung 47: Sichern der Max head Veränderung im ROM [8]

Nach einer erneuten Initialisierung der Festplatte wird schnell ersichtlich, dass jetzt keine Fehler mehr auftreten. Die bis zur nächsten Veränderung im ROM aktiven Köpfe 0 und 1 können die Service Daten der Festplatte ordnungsgemäß lesen. Nach einem Rechtsklick auf die Identifikationsdaten und „Refresh Drive ID“ dann endgültig die Erkenntnis: die Festplatte erkennt sich selbst wieder. [61] (siehe Abbildungen 48-50)



Abbildungen 48 und 50: Identifikationsdaten des Laufwerks (Vorher und Nachher) [8]

Abbildung 49: Refresh Drive ID [8]

4.5.4 Backup

Der nächste Schritt ist essentiell wichtig. Der funktionierende Zustand der Festplatte wurde wiederhergestellt, also gilt es so schnell wie möglich ein Backup der Service Daten zu erstellen, um bei weiteren möglichen Fehlern darauf zurückgreifen zu können. Dieses wird in der von PC-3000 Express mitgelieferten Datenbank abgelegt. [61] (siehe Abbildung 51) Für die folgende Sicherung wird eine Veränderung im RAM vorgenommen, um auch Kopf 3 sichern zu können. (mehr dazu im Abschnitt 4.5.6)

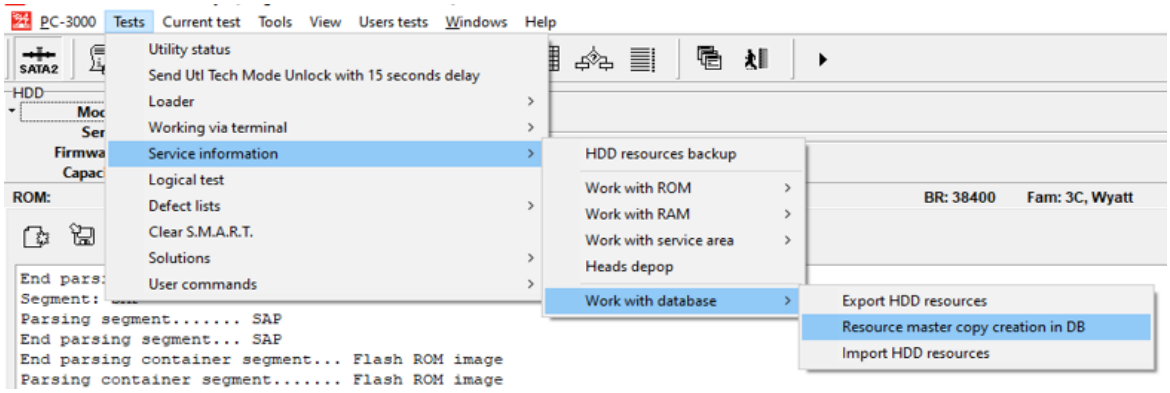


Abbildung 51: Backup Erstellung [8]

Nach dem Wiederherstellen der Funktionalität der Festplatte und einer entsprechenden Sicherung kann der Benutzer zur Arbeit mit dem Data Extractor übergehen.

4.5.5 Einsatz des Data Extractor

Abbildung 52: Building heads map [8]

Über die Funktion auf der rechten Seite wird eine „Heads map“ erstellt, die jedem Kopf seinen zuständigen LBA Bereich zuordnet. (siehe Abbildung 53)

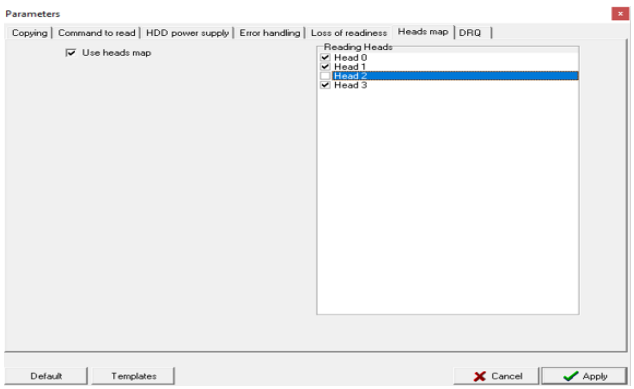


Abbildung 53: Heads map mit Ausschluss von Kopf 2 [8]

Anhand der Tuning Parameter im Abschnitt „Heads map“ wird der defekte Kopf 2 von der nachfolgenden Sicherung ausgeschlossen. Anschließend listet der Data Extractor jeden Sektor für den betrachteten Bereich, der gerade gesichert werden soll und der Sicherungsprozess kann gestartet werden. Durch die Tuning Parameter können wie in Abschnitt 2.5.2.2 beschrieben, weitere Einstellungen zur Behandlung auftretender fehlerhafter Sektoren implementiert werden. Grün markierte Sektoren weisen auf eine erfolgreiche Sicherung hin. (siehe Abbildung 54)

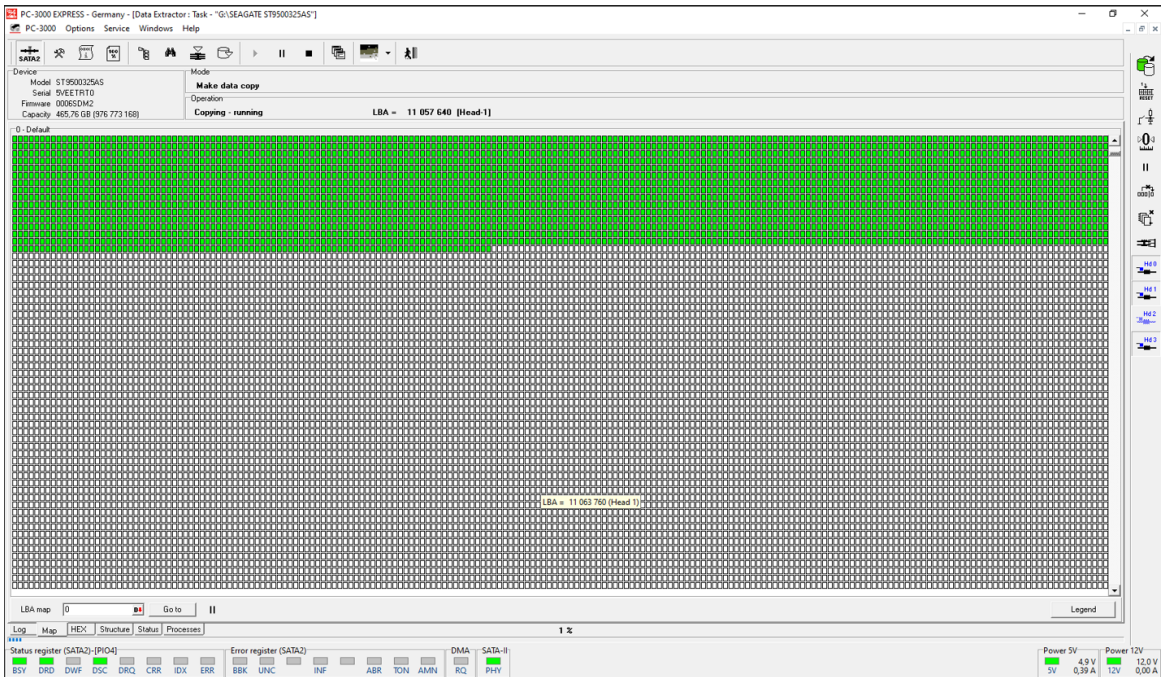


Abbildung 54: Sicherung der Köpfe 0, 1 und 3 [8]

Auf diese Weise sichert der Data Extractor nun erfolgreich die Daten von Kopf 0, 1 und 3. (siehe Abbildung 54)

4.5.6 Die Sicherung von Kopf 2

Um das Maximum an Daten der Festplatte sichern zu können, besteht ein letzter Versuch darin, einen Ersatzteilspender für die „Patienten-Festplatte“ zu finden, die Köpfe auszutauschen und erneut mit Hilfe von PC-3000 Express und dem Data Extractor zu versuchen, die Daten vom defekten Kopf 2 zu sichern.

Nach behutsamem und erfolgreichem Austausch der Köpfe wird die Patienten-Festplatte erneut an das PC-3000 Express System angeschlossen. Hierbei ist zu beachten, dass nach wie vor im ROM Speicher der Festplatte die zuvor getätigte Veränderung über die SAP Control Flags aktiviert ist. Das heißt, die Festplatte denkt nach wie vor, dass ausschließlich

zwei von vier Köpfen aktiv sind. Nun wird sich die Eigenschaft des RAM Speichers zunutze gemacht. Es ist bekannt, dass beim Bootprozess der Festplatte Informationen aus dem langsameren ROM in den schnelleren Zwischenspeicher des RAMs geladen werden, um Zugriffszeiten zu erhöhen. Im Folgenden Schritt soll der Festplatte jetzt mitgeteilt werden, dass alle Köpfe wieder zur Verfügung stehen, um vor allem Kopf 2 sichern zu können. Dazu wird mit Hilfe des Kommandos „Load Adaptives into HDD RAM“ (siehe Abbildung 55) die Anpassung vorgenommen. Zuvor wurde wieder mit dem „Flash ROM image file“ gearbeitet, um Zugriff auf die entsprechenden Funktionen zu erhalten.

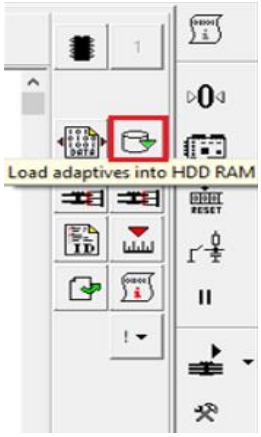


Abbildung 55: Load adaptives into HDD RAM [8]

In den RAM wird der Zustand geladen, in dem sich die Festplatte vor dem Austausch der Köpfe befand, ohne die Veränderungen im ROM. (Original ROM) Hieraus ergibt sich der Vorteil, dass im anschließenden Sicherungsprozess über den Data Extractor keine erneuten Fehler entstehen. Während des Sicherungsprozesses ist nicht klar, ob der Austausch der Köpfe reibungslos funktioniert hat bzw. die Köpfe auch in theoretisch fremder Umgebung reibungslos funktionieren. Wäre ein Kopf defekt oder während des Sicherungsprozesses treten Sektoren auf, die nicht sofort gelesen werden konnten, ist es mit dem Data Extractor möglich, Alternativen für das Lesen defekter Sektoren zu implementieren. So kann eine maximale Anzahl an Wiederholungsversuchen für das Lesen eines Sektors angegeben werden, die Lesegeschwindigkeit via PIO oder UDMA angepasst werden, die Sicherung auf einzelne Bereiche beschränkt werden oder die Festplatte nach einer bestimmten Anzahl fehlgeschlagener Leseversuche mittels eines Soft oder Hard Reset zurückgesetzt werden.

Im Falle eines solchen Hard Resets würden allerdings die zuvor getroffenen Anpassungen im RAM verloren gehen, da dieser die Daten bei Stromverlust nicht dauerhaft speichert. Startet die Festplatte dann neu, würde sie ausgehend von den Informationen im ROM nach

wie vor nur Kopf 0 und 1 ansteuern und damit würde die Sicherung von Kopf 2 an diesem Punkt abbrechen. Wäre wiederum die Einstellung im ROM gleich dem Originalzustand, ohne den RAM einzubeziehen, könnte zwar die Sicherung eventuell weiterlaufen, aber bei einem möglichen Defekt eines Kopfes oder anderen Fehlern, die auftreten können, würde die Festplatte erneut nicht mehr richtig starten. Aus diesem Grund wird eine erneute Fehlerbehebung umgangen, indem die Festplatte voll funktionsfähig von Kopf 0 und 1 aus startet und anschließend über den RAM unkompliziert die Anpassungen vorgenommen, die für die Sicherung von Kopf 2 benötigt werden.

Während des Sicherungsprozesses im schnellen UDMA Modus ist aufgefallen, dass die Festplatte dadurch oft überfordert wurde. Da die ausgetauschten Köpfe nicht exakt die gleichen originalen Köpfe ersetzen, können sie die Informationen nicht schnell genug lesen. Bei einer Umstellung in den PIO Modus, in dem nur acht-neun MB/s gelesen werden, funktioniert die Sicherung dann beständiger und ohne Fehler. Schlussendlich erhält der Benutzer mit dem Austausch der Köpfe auch eine Sicherung der Daten von Kopf 2. Zusammen mit den zuvor gesicherten Daten der anderen Köpfe gelingt damit eine Datensicherung für alle Köpfe der Festplatte. (siehe Abbildung 56)

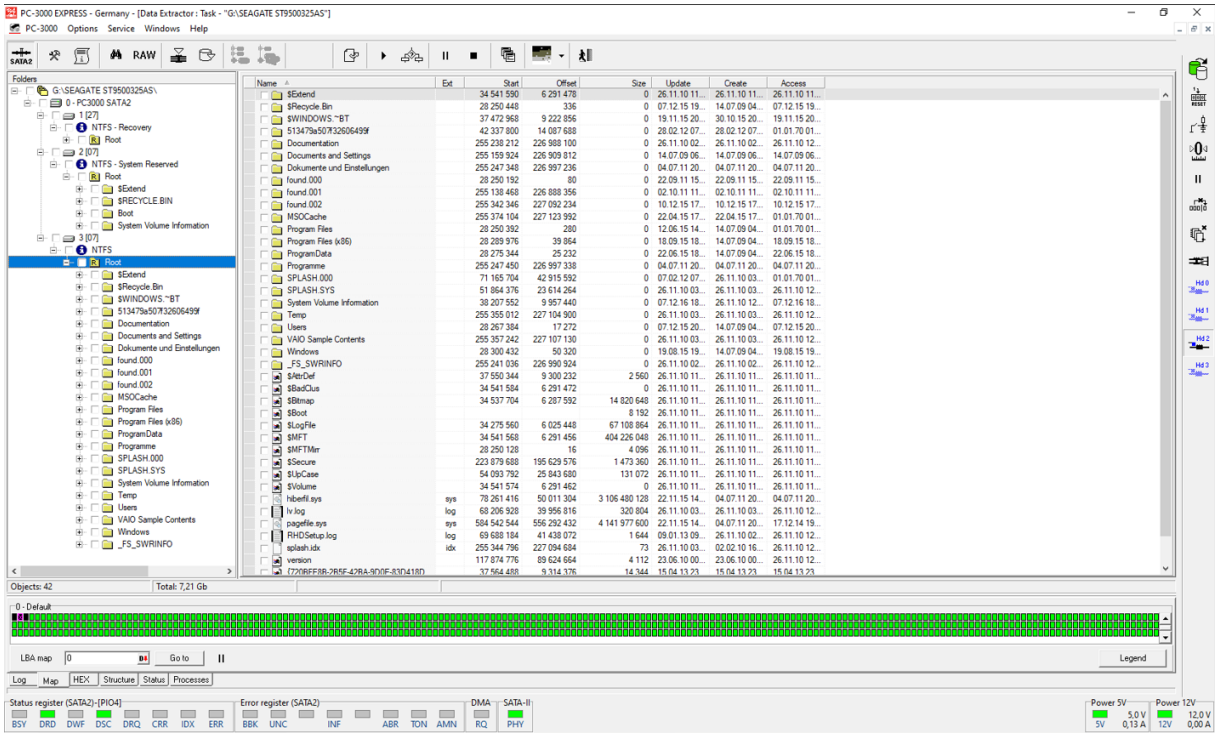


Abbildung 56: Erfolgreich gesicherter Patient mit rekonstruiertem Verzeichnisstrukturbaum [8]

5 Vorgehen Beispiel 2

Dieses Kapitel beschreibt die Vorgehensweise bei der Vorbereitung und Durchführung zu Spezialverfahren der Datenrettung für das zweite ausgewählte Beispiel.

5.1 Was ist eine SSHD?

Eine SSHD vereint die Eigenschaften einer SSD mit denen einer HDD. Aus diesem Grund befindet sich auf dem PCB einer HDD ein zusätzlicher Nicht-Und (NAND)-Flash Chip und macht das System damit zu einer Solid State Hybrid Drive, eben einem Hybrid aus SSD und HDD. Der NAND Chip sorgt für eine beschleunigte Initialisierung der Festplatte und speichert einen Teil der FW. Außerdem benutzt die Festplatte den NAND Chip als schnellen Cache für Benutzerdaten. Allerdings bringen die scheinbar vielen Geschwindigkeitsvorteile der Flash Technologie auch einen Nachteil mit sich. Da der Chip quasi dauerhaft in alle Prozesse der Festplatte eingebunden ist und die Lebenserwartung eines Flash Chips im Schnitt kürzer ist als die der restlichen Bestandteile der Festplatte, wird der Chip damit zur Schwachstelle des Laufwerks. Ist der Chip beschädigt, auch wenn die Festplatte Zugriff auf die Service Daten auf den Platten hat, würde die Festplatte trotzdem nicht korrekt starten. [11]

5.2 Ausgangslage/Symptome

Die betroffene Festplatte liegt bereits seit März 2019 beim Zuständigen für Spezialverfahren der Datenrettung im behördlichen Einsatz vor. Dabei handelt es sich um eine intern benutzte Festplatte, die zu einem Supportfall geworden ist. Anfänglich wurde die Festplatte bereits mit PC-3000 Express analysiert und ein Problem in Verbindung mit dem NAND Chip der Festplatte vermutet. Da zum damaligen Zeitpunkt kein passender Spender auf Lager ist, muss die Reparatur und Wiederherstellung der Daten warten. Erst als im November 2020 ein passender Spender verfügbar wurde, kann die Maßnahme zur Datenrettung durchgeführt werden.

5.3 Strategische Vorbereitung

Die strategische Vorbereitung im beschriebenen Fall gestaltete sich schwierig, da für die Festplatte kein Backup erstellt wurde und das spezifische Modell vorher noch nie im Rahmen einer strategischen Vorbereitung aufgetaucht ist. Trotz alledem wurden zur späteren Verwendung die Basisdaten der Festplatte ermittelt (siehe Tabelle 8 und 9) und im weiteren Verlauf entsprechende Backups der Festplatten erstellt.

5.3.1 Der Patient

Im nachfolgenden Beispiel wird die Festplatte nur noch als „Patient“ bezeichnet.

Bei der Festplatte handelt es sich um eine 3,5 Zoll große SSHD Festplatte des Herstellers Seagate. (siehe Abbildung 57)

Tabelle 8: Übersicht Basisdaten Patient (2)

Bezeichnung	Beschreibung
Modell	ST1000DX001
Seriennummer	Z4YDVWF0
Firmware Version	CC41
Kapazität	1000 GB
Herstellungsland	Thailand
Herstellungsdatum	14. Juli 2016
Site	TK
Part-Nummer	1NS162-300
Architektur	F3-Architektur
Familie	58 Grenada
Headmap	2

Tabelle 8 (Fortsetzung): Übersicht Basisdaten Patient (2)

Umdrehungen	7200
PCB-Nummer	100731495 REV B

Abbildung 57: Patienten Festplatte Frontalansicht (2)

5.3.2 Der Spender

Im nachfolgenden Beispiel wird die Festplatte nur noch als „Spender“ bezeichnet.

Bei der Festplatte handelt es sich um eine 3,5 Zoll große SSHD Festplatte des Herstellers Seagate. (siehe Abbildung 58)

Tabelle 9: Übersicht Basisdaten Spender (2)

Bezeichnung	Beschreibung
Modell	ST1000DX001
Seriennummer	Z4YAVWPD

Tabelle 9 (Fortsetzung): Übersicht Basisdaten Spender (2)

Firmware Version	CC41
Kapazität	1000 GB
Herstellungsland	Thailand
Herstellungsdatum	10. Oktober 2015
Site	TK
Part-Nummer	1NS162-500
Architektur	F3-Architektur
Familie	58 Grenada
Headmap	2
Umdrehungen	7200
PCB-Nummer	100731495 REV B

Abbildung 58: Spender Festplatte Frontalansicht (2)

5.4 Operationale Vorbereitung

Mit Hilfe der Webseite https://www.donordrives.com [60] wurde „der Spender“ als in Frage kommendes Spenderlaufwerk ermittelt. Dabei gilt es zu beachten, dass ein in Frage kommender Spender nicht automatisch bedeutet, dass die Ersatzteile auch wirklich kompatibel mit dem Patienten sind. Viele Parameter können oftmals bereits auf dem Label des Herstellers, dass sich auf der Festplatte befindet, eingesehen werden. Für das zweite Beispiel war vor allem wichtig, dass die PCB-Nummern des Patienten und des Spenders übereinstimmten. (siehe Abbildung 59)

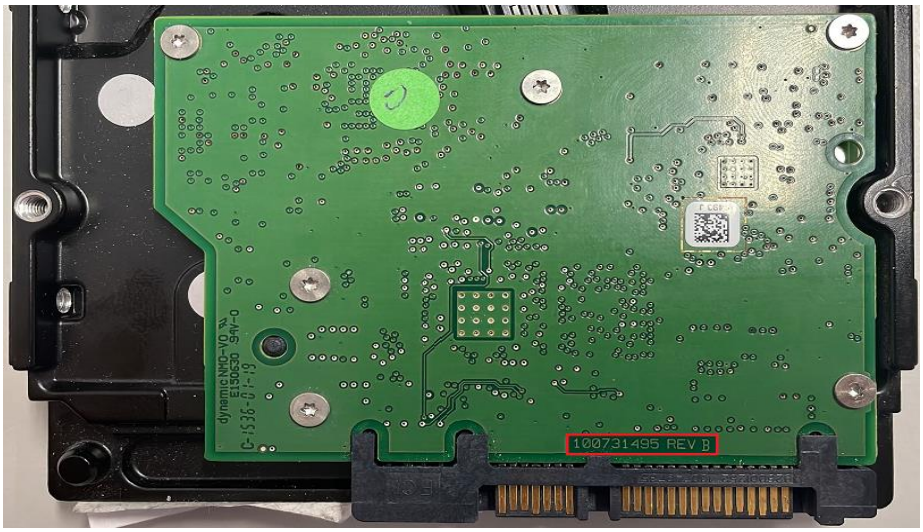


Abbildung 59: PCB mit PCB-Nummer

Folgende Parameter wurden bei der Ermittlung des Spenders einbezogen:

- gleiche Modellnummer

- zweites und drittes Zeichen der Seriennummer müssen übereinstimmen

- gleiches Herstellungsland

- Herstellungsdatum sollte möglichst nicht weiter als 3 Monate abweichen, aber ein späteres Herstellungsdatum ist grundsätzlich besser

- Site = Herstellerfabrik muss gleich sein

- Part-Nummer: die erste Hälfte der Partnummer (vor dem Bindestrich) muss übereinstimmen

- PCB-Nummer muss identisch sein

5.4.1 Verwendete Software und Hardware

Software:

- PC-3000 Express Professionell System

- PC-3000 Express zur Analyse und Reparatur der Festplatte

- Data Extractor zur Fehlerbehandlung und Datensicherung

- https://www.donordrives.com [60]

- zur Ermittlung eines kompatiblen Ersatzteilspenders

Hardware:

- PC-3000 Express Professionell System

- PC-3000 Erweiterungs-Board fest eingebaut in einen Untersuchungsrechner

- Terminal Board mit Terminal Adapter für Seagate SATA Festplatten (siehe Abbildung 60)

- Datenübertragungskabel (siehe Abbildung 60)

- Stromzufuhrkabel (siehe Abbildung 60)

- Untersuchungsrechner

- Microsoft Windows 10 Pro, x64-basierter PC

- Intel® Core™ i7-8700 CPU @ 3.20 GHz, 3192 MHz, 6 Kern(e), 12 logische(r) Prozessor(en)

- 64 GB RAM

- 512 GB SSD Systempartition, 2 TB SSD Datenspeicher, 2x 4 TB Festplatten Datenspeicher und 4 interne Festplattenanschlüsse

- Spender Festplatte mit Spender PCB

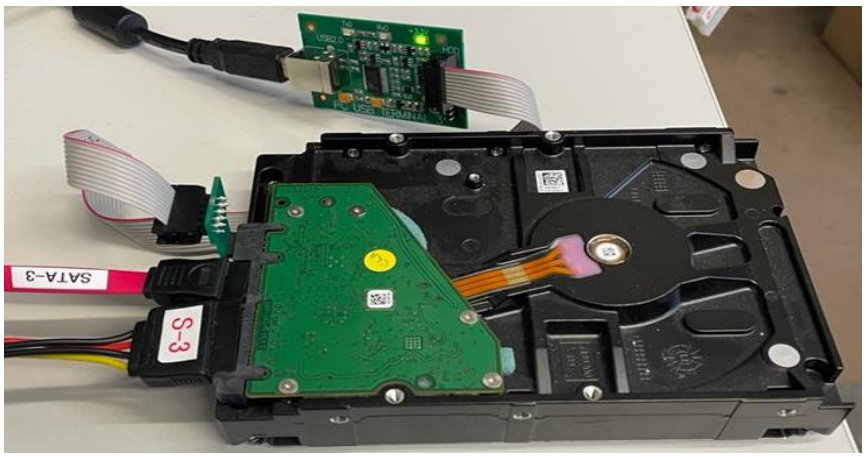


Abbildung 60: Anschlüsse des Patienten an das PC-3000 Express System (2)

5.4.2 Verwendete Werkzeuge

- Schraubenzieher

5.5 Analyse der Fehlerquelle

Nach einer augenscheinlichen Untersuchung der Festplatte wurden keine äußerlich erkennbaren Schäden festgestellt. Auf die gleiche Weise wurde das PCB untersucht und ergab keine Hinweise auf offensichtliche Beschädigungen. Nach dem Verbinden der Festplatte mit PC-3000 Express konnte die Festplatte ihre korrekten Identifikationsdaten ausgeben und meldete anhand der Statusregister mittels DRD und DSC Bereitschaft. Allerdings war kein Zugriff auf Benutzer – oder Servicedaten möglich und die Festplatte drehte ihren Plattenstapel nicht. Obwohl die Festplatte Identifikationsdaten findet, konnte nicht ausgeschlossen werden, dass ein Fehler innerhalb der Service Daten besteht. Außerdem erschien im Log Tab ein solcher Fehler, „LED:0x000000BD FAddr:0x000059D8“, der daraufhin deutet, dass ein Fehler im Service Bereich besteht. Da die Festplatte aber seither ihre Platten nicht ein einziges Mal drehen konnte, musste der Teil der Service Daten betroffen sein, der sich auf dem PCB befindet. Nach dem Ausschlussprinzip für den Initialisierungsprozess einer SSHD, einem scheinbar intakten und sicherbaren ROM sowie originalem PCB der Festplatte und einem vermutlich intaktem Service Bereich im Inneren der Festplatte, konnte höchstwahrscheinlich nur noch ein defekter NAND Chip auf dem PCB als Ursache dienen.

5.6 Datensammlung

Aus den bisherigen Erfahrungen mit der Festplatte ist bekannt, dass der Fehler aus einem defekten NAND Chip der SSHD resultieren kann. Diese Vermutung wird durch die Ausgabe etwaiger Fehler im Log Tab von PC-3000 Express bestätigt. Zudem ist das Terminal nicht erreichbar und die Festplatte dreht ihre Platten nicht.

5.6.1 Patienten ROM

Im momentanen Zustand des Laufwerks hat oberste Priorität, den originalen ROM des Patienten zu sichern. Andere Möglichkeiten sind ohnehin sehr eingeschränkt, da durch den Fehler kaum Funktionen ausgeführt werden können. [11] (siehe Abbildung 61)

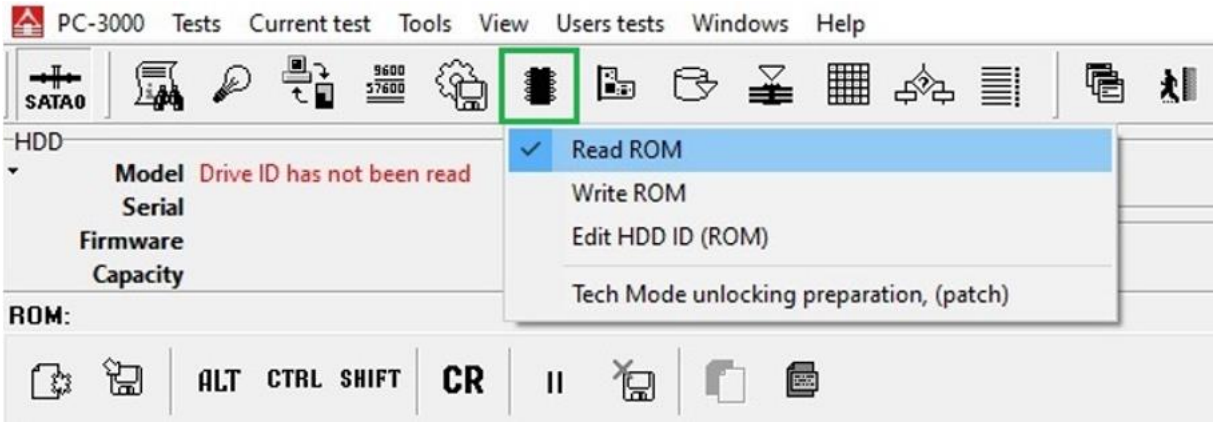


Abbildung 61: Read ROM [11]

5.6.2 Gesperrtes Terminal und ROM Image

Im nächsten Schritt wird der Spender vorbereitet. Diese Festplatte funktioniert soweit fehlerfrei und kann ganz normal initialisiert und gestartet werden. Einziges Manko bis zu diesem Punkt ist, dass der Terminalzugang des Spenders gesperrt ist. Vor allem bei neueren Festplatten ist die Firmware durch die Hersteller so implementiert, dass der Zugang zum Terminal standardmäßig blockiert ist. Hinzu kommt, dass das Terminal manchmal von der Festplatte gesperrt wird, wenn die Köpfe das SA nicht richtig lesen können. [57] In den nächsten Schritten wird es aber nötig sein, Zugang zum Terminal zu erhalten, da über herstellerspezifische Befehle der NAND Chip modifiziert werden muss. Dazu wird wie in Abschnitt 4.5.2 mit Hilfe des Boot Code Modus der ROM des Spenders gelesen und zusätzliche Funktionen freigeschaltet. [11]

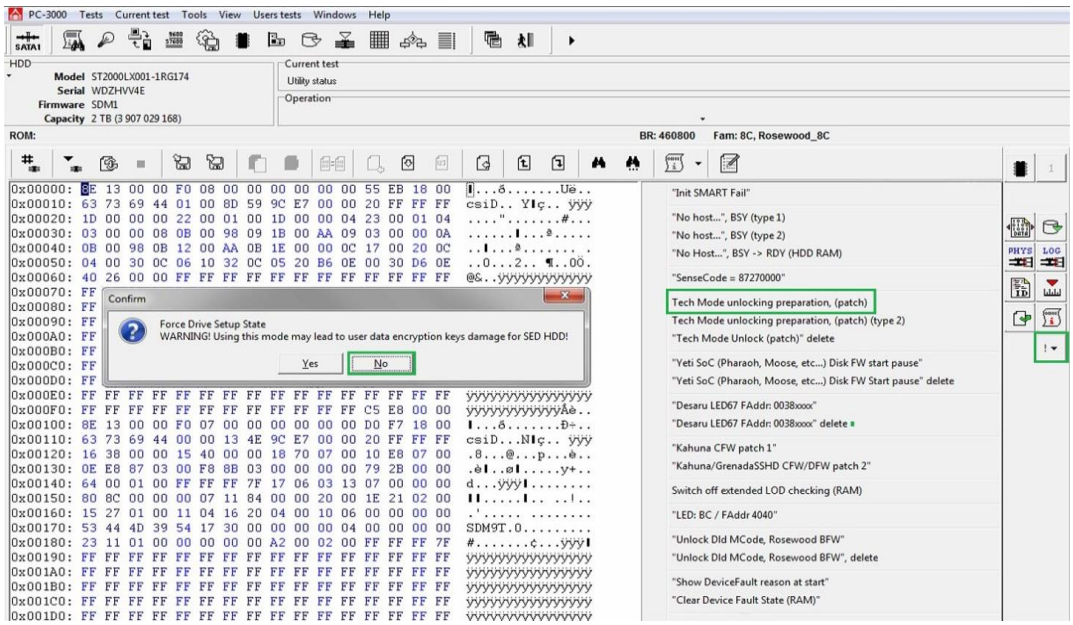


Abbildung 62: Tech mode unlocking preparation (patch) [11]

Über die Funktion „mit dem Ausrufezeichen“ (siehe Abbildung 62) öffnet sich ein Untermenü, in dem der Benutzer dann „Tech Mode unlocking preparation (patch)“ ausführt. Mit diesem Schritt wird das Terminal für die Entsperrung vorbereitet. Die nachfolgende Meldung „Force Drive Setup State“ wird mit „No“ beantwortet, um die Festplatte nicht zu zwingen, vorhandene interne Einstellungen dauerhaft zu verändern. [11]

5.6.3 Freischaltung des Terminals

Nachdem jetzt das „ROM image“ vorliegt und die Entsperrung des Terminals eingeleitet wurde, müssen bestimmte Anpassungen vorgenommen werden. Bekanntermaßen generieren Unternehmen wie ACE Lab ihr Wissen und ihre Software, indem sie durch Reverse Engineering FW (Firmware) Code der Festplattenhersteller dekodieren und übersetzen. Dadurch ist es möglich, Rückschlüsse darüber zu ziehen, an welcher Stelle des Codes eine bestimmte Funktion ausgeführt wird und welche Folgen Veränderungen im Code bewirken. Eine solche Veränderung muss jetzt in Bezug auf den defekten NAND Chip vollzogen werden. Über das „Raute-Symbol“ links oben im ROM Tab öffnet sich eine Liste. (siehe Abbildung 63) Insbesondere bei modernen Festplattenmodellen finden sich im ROM oder Prozessor adaptive Parameter, die wiederum Code zur Initialisierung von Hardwarekomponenten enthalten. In diesem Fall befindet sich der Code zur Initialisierung des NAND Chips innerhalb der IAP – Interface Adaptive Parameters. [11] (siehe Abbildung 63)

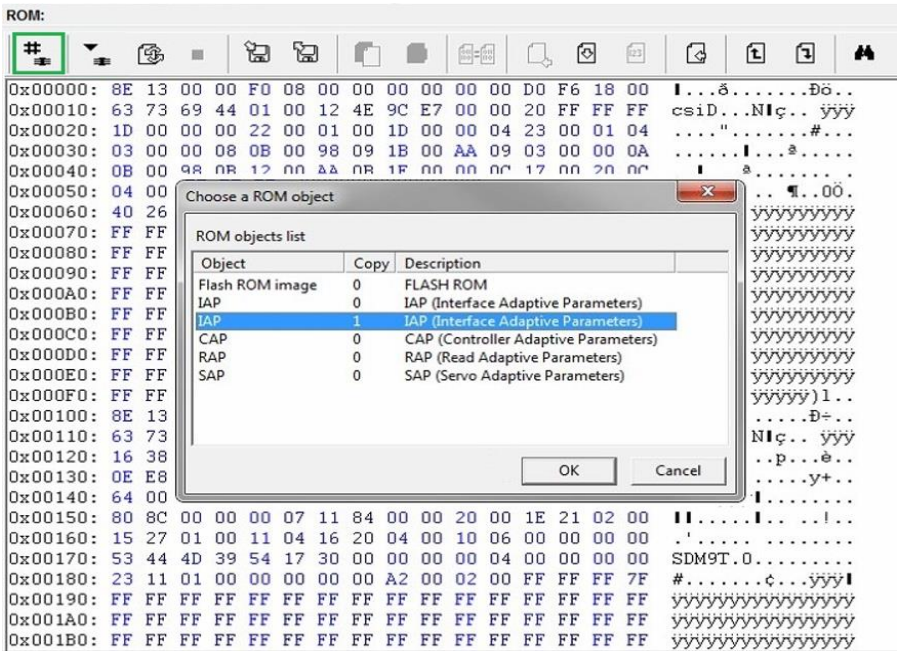


Abbildung 63: IAP (Interface Adaptive Parameters) [11]

Nach der Auswahl der IAP öffnet sich im integrierten Hex-Editor die entsprechende Stelle im ROM, an der die IAP geschrieben sind. Nun muss der Benutzer nach der Sequenz „12 34 56 78“ suchen. Über den Hex-Editor muss jetzt die erste Stelle der Sequenz, also die 1, in eine 8 umgeändert werden. [11] (siehe Abbildung 64)

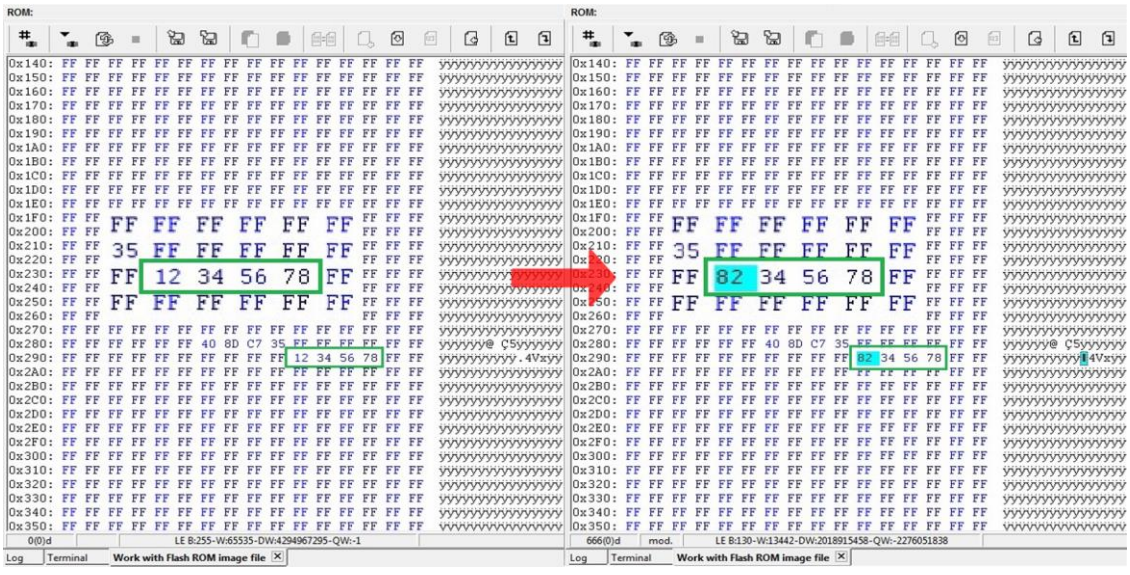


Abbildung 64: Erste IAP Veränderung [11]

Dem Benutzer muss an dieser Stelle bewusst sein, dass er sich im momentanen Schritt immer noch dabei befindet, das Terminal freizuschalten. Die eben veränderte Sequenz beinhaltet den Code zur Initialisierung des NAND Chips. Durch die Veränderung wird die

Startsequenz des NAND Chips blockiert und die Festplatte gezwungen, vom ROM aus zu starten. Die Veränderung wird demzufolge gespeichert und die Festplatte neu gestartet. Da die Festplatte intern immer noch darauf eingestellt ist, mit Hilfe des NAND Chips zu starten und dieser ebenso einen Teil der FW enthält, erzeugt die Festplatte keine Bereitschaft mehr, der NAND Chip ist nach wie vor blockiert. Sinn und Zweck der Veränderung ist einzig und allein, nun die Freischaltung des Terminals über die Veränderung im ROM durchführen zu können. (siehe Abbildung 65)

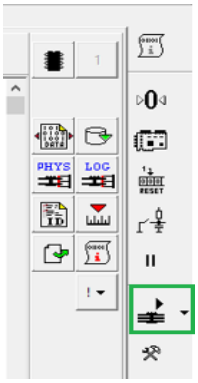


Abbildung 65: Terminal Freischaltung [8]

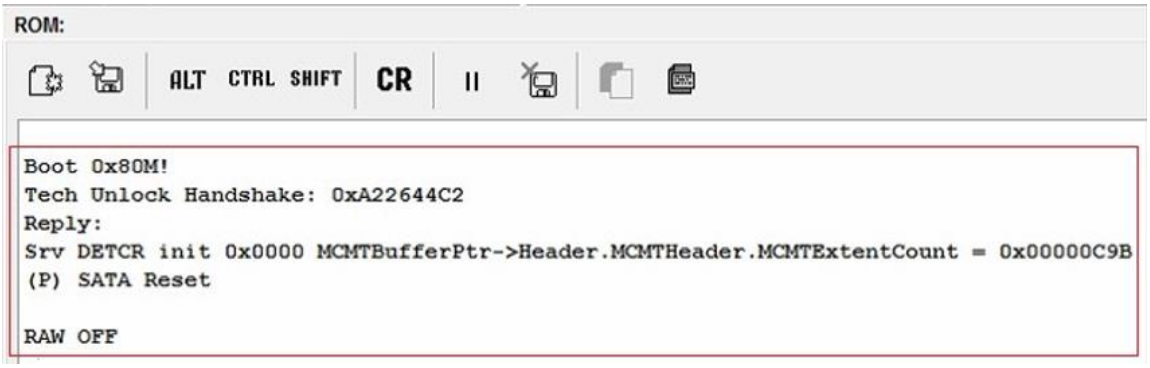


Abbildung 66: ROM Tab Meldung zur Terminal Freischaltung [11]

In der zweiten Zeile des ROM Tab dann die erfolgreiche Rückmeldung: „Tech Unlock Handshake“, die auf den vorigen Befehl (Tech mode unlocking preparation (patch)) zur Vorbereitung der Freischaltung des Terminals im ROM zurückzuführen ist. (siehe Abbildung 66) Jetzt gilt es, die Veränderung in den IAP rückgängig zu machen. Das heißt, die Blockierung des NAND Chips wird wieder aufgehoben. [11] (siehe Abbildung 67)

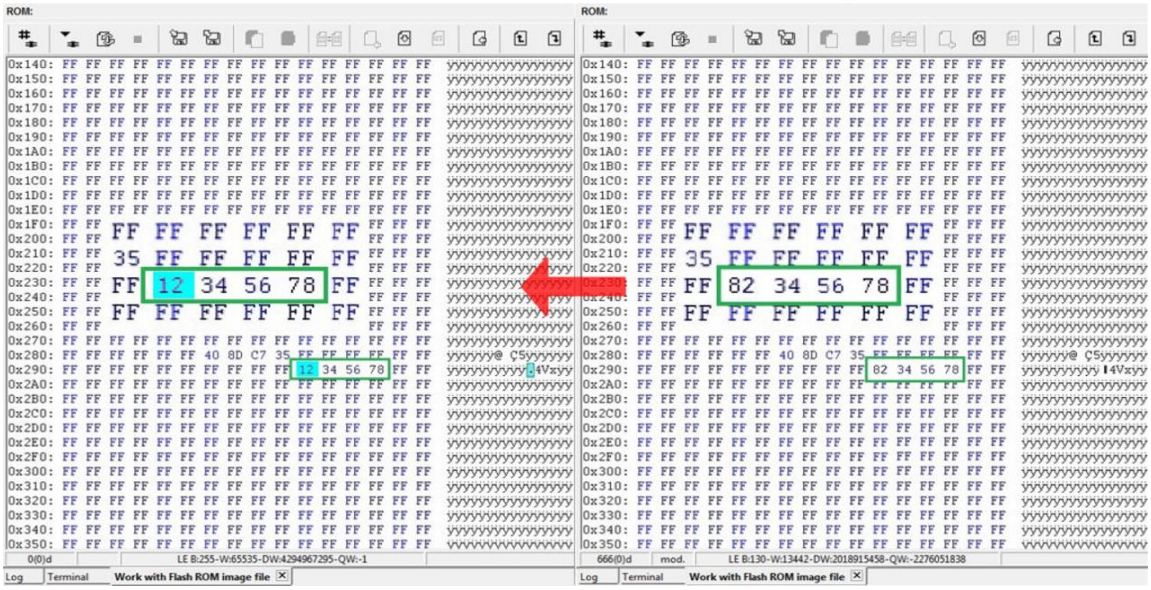


Abbildung 67: Zweite IAP Veränderung

Die Aufhebung der Blockade bewirkt, dass nach dem Zurückschreiben des ROM und einem Neustart der Festplatte die Informationen im ROM, indem jetzt das Terminal freigeschaltet ist, in den NAND Chip geladen werden. Dadurch ist jetzt das Terminal des Spenders nicht mehr gesperrt und die Ausführung von Kommandos über das Terminal möglich. In diesem Zustand, mit Zugang zum Terminal, sollte definitiv ein Backup des ROM durchgeführt werden, wenn die Spender Festplatte zukünftig wieder benutzt werden soll. Da das Terminal nun endlich freigeschaltet ist, kann der Benutzer vom ROM Tab in den Terminal Tab wechseln. Um die Ausführung von Kommandos zu aktivieren, startet man das Terminal durch die Kombination STRG + Z, woraufhin ein Prompt auf Eingaben wartet. [11]

An dieser Stelle soll eine Zusammenfassung der bis zu diesem Zeitpunkt durchgeführten Schritte stattfinden. Ganz zu Beginn wurde ein defekter NAND Chip einer SSHD als Fehlerquelle identifiziert. Daraufhin wurde eine passende Spender Festplatte mit intaktem NAND Chip ermittelt, mit deren Hilfe der defekte NAND Chip auf der Patienten Festplatte ausgetauscht werden soll. Das Risiko eines Chip Off Eingriffs (Ablöten des Chips) bezüglich des NAND Chips wäre sehr groß und zusätzlich stehen andere risikofreiere Methoden zur Verfügung. Aus diesem Grund werden mit Hilfe des Spender PCB und softwareseitig durch PC-3000 Express und dem Data Extractor Schritte zur Lösung eingeleitet. Das Grundprinzip der Lösung sieht zunächst vor, dass der originale Zustand des ROM vom Patienten gesichert wird. Anschließend muss der Inhalt des intakten NAND Chips entfernt werden und der Flash Speicher wird neu initialisiert. Dann wird der originale ROM vom Patienten auf das PCB des Spenders übertragen, indem gerade der NAND Chip neu initialisiert wurde. Wenn der originale ROM erfolgreich übertragen wurde, wird das Spender PCB mit

dem des Patienten ausgetauscht und die Funktionalität sollte wiederhergestellt sein. Die bis zu diesem Zeitpunkt ausgeführten Schritte beschäftigen sich wiederum mit der Problematik, dass sowohl beim Spender als auch nach dem Austausch des PCB beim Patienten der Terminalzugang gesperrt ist. Wenn bis hierhin alle Schritte zur Lösung korrekt ausgeführt wurden, hat der Benutzer beim Spender Zugang zum Terminal erlangt und den Seagate Prompt (F3 T>) vor sich, der auf Eingaben wartet.

5.6.4 Vorbereitung des NAND Chips

Wenn wie in diesem Beispiel ein intakter NAND Chip eines Spenders bzw. das gesamte PCB in ein anderes, unbekanntes Laufwerk eingesetzt werden soll, müssen bestimmte Dinge beachtet werden. Neben den bereits erwähnten Aspekten der Kompatibilität müssen alle Einstellungen und Parameter, die sich vorher auf dem PCB befunden haben, gelöscht oder überschrieben werden. Dazu zählt einerseits das Überschreiben des ROM vom Spender mit dem originalen ROM des Patienten. Damit erhält das eigentlich fremde, umgesetzte PCB sofort alle benötigten Daten, um mit den restlichen Laufwerkskomponenten des Patienten kommunizieren zu können. Andererseits muss der Inhalt des NAND Chips geleert werden. Alle Einstellungen und Parameter, die der NAND Chip vor dem Löschvorgang und der Neuinitialisierung kennt, stammen von denen des Spenders und sind für jede Festplatte individuell. Ohne diesen Vorgang wäre der NAND Chip nicht kompatibel mit dem Patienten, da der Patient versuchen würde, seine eigenen individuellen Einstellungen und Parameter mit dem Chip zu konfigurieren, aber bereits andere, unbekannte Daten des Spenders im Chip hinterlegt sind.

Dementsprechend wird mit dem herstellerspezifischen Seagate Befehl „/OI1“ der Löschvorgang und die Neuinitialisierung für den NAND Chip eingeleitet. (siehe Abbildung 68) Durch die Eingabe des Kommandos „F3 T>/CQ“ erscheint eine Liste aller Kommandos, die für diese SSHD ausgeführt werden können. Seagate teilt seine Befehle in verschiedene Level auf. Durch das voranstellen eines „/“ wechselt der Benutzer das Kommandolevel, in diesem Fall dann in Level „O.“ Für den Parameter „I“ konnte folgendes ermittelt werden: „Level O 'I': Rev 0001.0000, Overlay, CfsInitializeCacheFileSystem, I.“ Für die am Ende des ursprünglichen Kommandos verwendete „1“ wird folgende Funktion vermutet: „1 – Target Address is any VBM.“ Die Funktion der „1“ konnte jedoch nicht bestätigt werden und die Bedeutung des Befehls blieb nach ausgiebiger Recherche unbekannt. Anschließend liefert das Terminal am Ende des Vorgangs die Ausgabe „Flash and Parametric Table was erased and ALF Tables have successfully been initalized.“ Der NAND Chip der Spender Festplatte ist nun für den Einsatz im Patienten vorbereitet. [11] (siehe Abbildung 68)

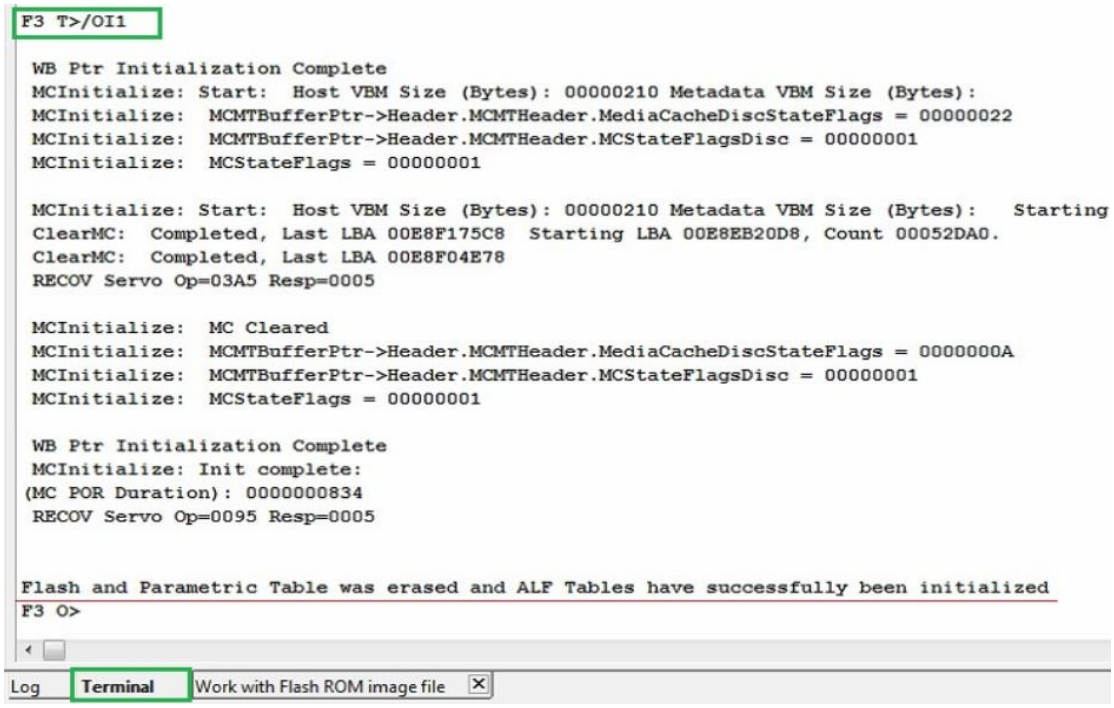


Abbildung 68: Ausgabe des „/OI1“ Befehls [11]

Nun wird der anfänglich gesicherte Zustand des originalen ROM aus dem Patienten auf das eben vorbereitete Spender PCB übertragen und das PCB in den Patienten eingesetzt. Beim Starten des Patienten wird erneut das Terminal gesperrt sein. Deshalb müssen die Schritte zum Entsperren des Terminals wie beim Spender wiederholt werden, ohne die Blockierung des NAND Chips vorher rückgängig gemacht zu haben. Daraufhin wird der Inhalt des NAND Chips erneut gelöscht. Erst jetzt wird die Blockierung des NAND Chips wieder aufgehoben und die Festplatte neu gestartet. Auf diesem Weg bleibt die Entsperrung des Terminals auch für die Initialisierung der Festplatte mit dem NAND Chip standardmäßig erhalten. [11]

5.6.5 Letzte Schritte

Bevor letztendlich die Sicherung beginnt, muss noch ein wichtiger Haken für die Parameter unter „loss of readiness“ gesetzt werden. (siehe Abbildung 69) Sollte die Festplatte während des Sicherungsprozesses die Stromzufuhr, beispielsweise durch einen „Hardware Reset“, verlieren und der Haken wäre nicht gesetzt, wäre auch das Terminal wieder gesperrt. Gerade interne Prozesse zur Neuinitialisierung der Festplatte oder auch während des Sicherungsprozesses benötigen Terminalzugang um bestimmte Befehle im Hintergrund ausführen zu können. Mit der Unterstützung durch das Parameter Tuning läuft der Data Extractor schlussendlich durch und beendet die vollständige Sicherung des Patienten erfolgreich. [11]

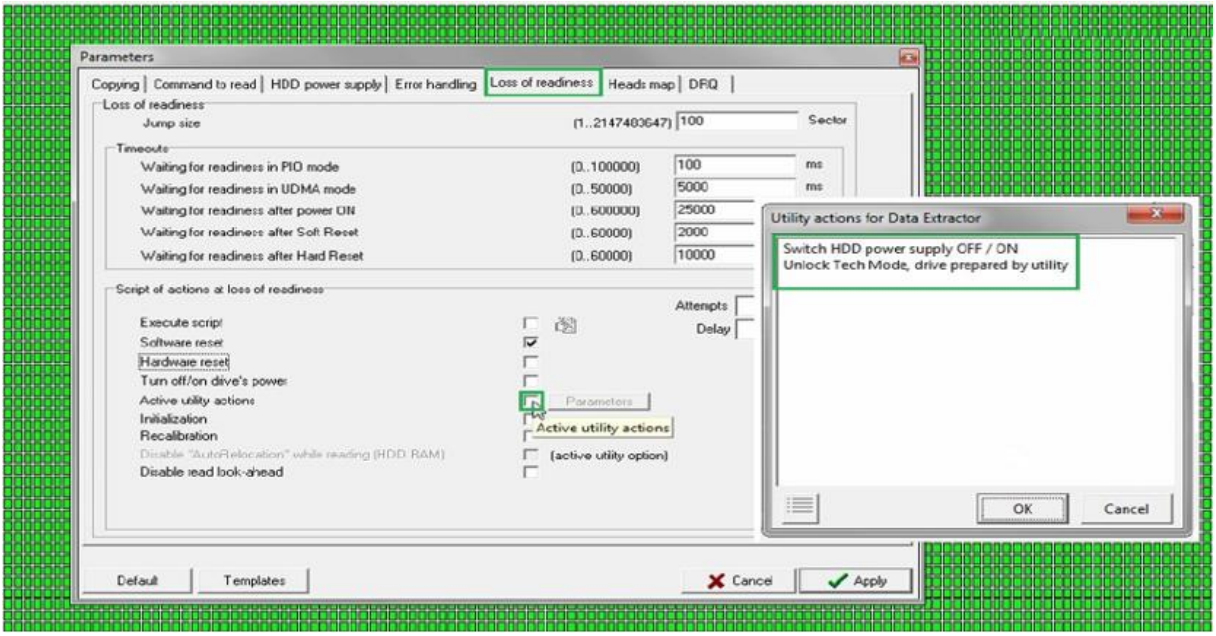


Abbildung 69: Unlock Tech Mode aktivieren [11]

6 Ergebnisse

Dieses Kapitel enthält die Ergebnisse aus den beiden Beispielen zu Spezialverfahren der Datenrettung.

6.1 Beispiel 1

Tabelle 10: Übersicht Ergebnisse Beispiel 1

Bezeichnung	Beschreibung
Sicherung	Die nicht defekten Köpfe 0,1 und 3 des Patienten konnten erfolgreich gesichert werden
Ersatzteile	Der defekte Kopf 2 des Patienten wurde durch kompatible Ersatzteile ausgetauscht
Kopf 2	Die Daten von Kopf 2 des Patienten wurden erfolgreich gesichert
Backup	Für in Zukunft auftretende Fehler (im Rahmen der strategischen Vorbereitung) wurden entsprechende Backups erstellt (ROM, Service Daten, etc.)
Fehlerhafte Sektoren	Die vollständige Sicherung der Festplatte wurde mit der Feststellung von 15 fehlerhaften Sektoren durchgeführt (siehe Abbildung 70)

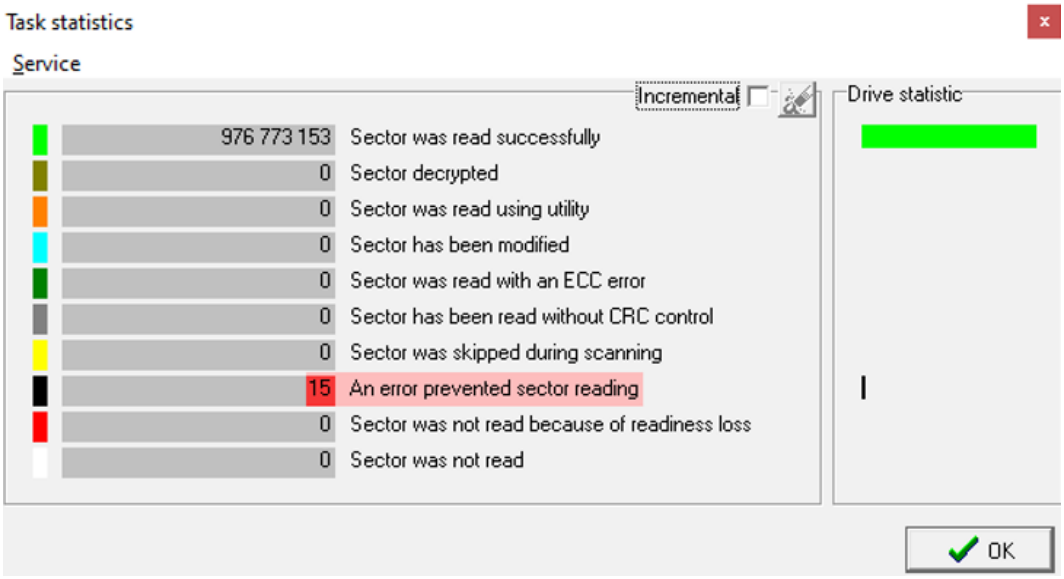


Abbildung 70: Sicherungsstatistik Beispiel 1 [8]

Hinweis: Für die 15 fehlerhaften Sektoren konnte ermittelt werden, dass sich alle im Spare-Bereich der dritten Partition der Festplatte befinden und somit keinen Einfluss auf Benutzerdaten haben. Der durch den Data Extractor generierte Report (siehe Abbildung 71) erkennt jeweils sechs und neun zusammenhängende Sektoren, die als „BAD“ markiert wurden. Die dritte Partition beginnt bei Sektor 34´541´578 und enthält somit alle als „BAD“ erkannten Sektoren. Durch einen Rechtsklick auf die entsprechende Partition und der Auswahl von „Generate report on marked files and folders“ werden alle Dateien der Partition auf Fehler untersucht. Dabei konnten keinerlei Fehler innerhalb der auf Partition 3 befindlichen Dateien festgestellt werden. (siehe Abbildung 72)

```
From = 034541640   To = 034541645 BAD = 6 Sectors
From = 034542727   To = 034542735 BAD = 9 Sectors

Total Bad Sectors Count = 15
```

Abbildung 71: Sicherungsreport Beispiel 1 [8]

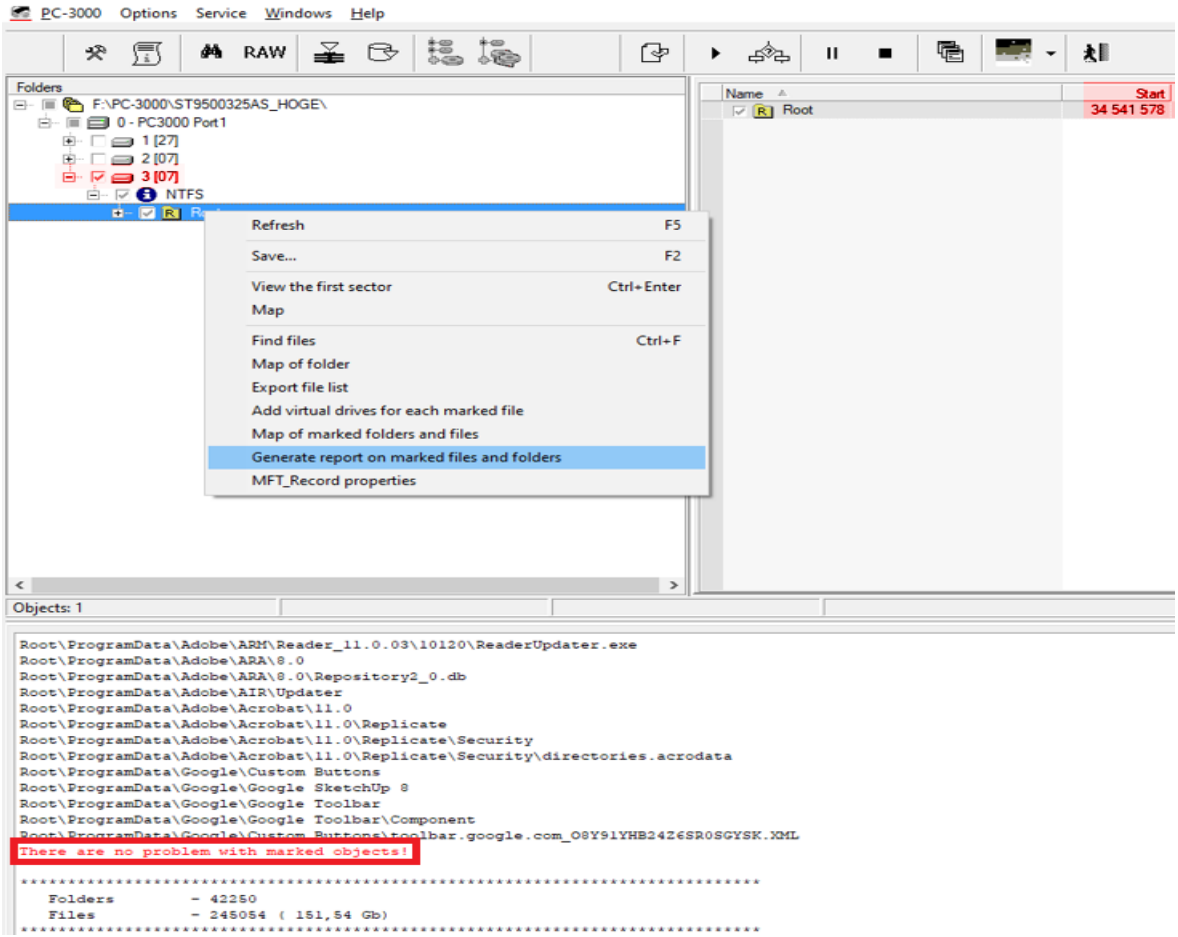


Abbildung 72: Report on marked files and folders [8]

Tabelle 11: Übersicht Vorher/Nachher Beispiel 1

Vorher	Nachher
Kein Zugriff auf Benutzer – und Service Daten sowie fehlerhafte Identifikationsdaten des Laufwerks	Der Patient zeigt Bereitschaft an, hat Zugang zu Benutzer – und Service Daten und konnte über den Data Extractor gesichert werden

6.2 Beispiel 2

Tabelle 12: Übersicht Ergebnisse Beispiel 2

Bezeichnung	Beschreibung
Ersatzteile	Der defekte NAND Chip des Patienten und damit auch das gesamte PCB wurde durch einen kompatiblen Ersatzteilspender ausgetauscht
Terminalzugang	Für den Patienten und den Spender wurde sichergestellt, dass zukünftig der Zugang zum Terminal freigeschaltet ist
Backup	Für in Zukunft auftretende Fehler (im Rahmen der strategischen Vorbereitung) wurden entsprechende Backups erstellt (ROM, Service Daten, etc.)
NAND Chip	Der ausgetauschte NAND Chip wurde erfolgreich mit dem Patienten konfiguriert
Sicherung	Die Festplatte konnte vollständig gesichert werden
Fehlerhafte Sektoren	Fehlerhafte Sektoren konnten nicht festgestellt werden

Tabelle 13: Übersicht Vorher/Nachher Beispiel 2

Vorher	Nachher
Kein Zugriff auf Benutzer – und Service Daten und die Festplatte dreht ihre Platten nicht	Der Patient zeigt Bereitschaft an, dreht seine Platten wieder, hat Zugang zu Benutzer – und Service Daten und konnte über den Data Extractor gesichert werden

7 Diskussion

In der Diskussion geht es um die Bewertung der Arbeit mit dem PC-3000 Express System sowie eine Auseinandersetzung mit dem vorgestellten forensischen Leitfaden und die Vereinbarkeit des Systems im Zusammenhang mit forensischer Arbeit.

7.1 Allgemeine Kritik am System

Das PC-3000 Express Professionell System wird seinem Namen tatsächlich gerecht. Die umfassende Hardware-Software-Lösung kann im Mittel gute bis sehr gute Ergebnisse bei der Reparatur und Sicherung von Festplatten erzielen. Der „Express“ Aspekt innerhalb des Namens lässt sich hauptsächlich auf die PCIe Schnittstelle, mit der das System in ein Computersystem integriert wird, zurückführen. Allerdings wird dem System damit auch genau die Geschwindigkeit ermöglicht, die sich ein Benutzer unter „Express“ vorstellt. Alle Prozesse, die über das System laufen, sind stark abhängig vom Zustand der zu untersuchenden Festplatte. (Alter, Beschädigungen usw.) Doch jede übertragene Aufgabe meistert das System im Rahmen aller Möglichkeiten in den meisten Fällen sehr zügig. Dabei sorgt natürlich auch ein entsprechender Untersuchungsrechner für die nötige Ausdauer, aber insgesamt lassen sich innerhalb der Ablaufprozesse des Systems keine Mängel feststellen. Vor allem in Bezug auf kapazitativ große Datensicherungen kann das System mit einem hohen Maß an Zuverlässigkeit und Geschwindigkeit punkten.

Neben diesen grundsätzlichen Erwartungen an ein hoch entwickeltes und modernes System bieten sich dem Benutzer unzählige Funktionen und Möglichkeiten im Umgang mit Festplatten, worin sich vor allem die Professionalität des Systems gut widerspiegelt. Für den Benutzer ist in diesem Zusammenhang jedoch ein gewisses Maß an Vorsicht geboten, denn ohne die nötige Einarbeitung und Grundlagenwissen kann es schnell unübersichtlich und kompliziert werden. PC-3000 ermöglicht Zugang zu Bereichen einer Festplatte, die nicht von unerfahrenen Benutzern gehandhabt werden sollten. So gut die Funktionen eine Festplatte reparieren mögen, so schnell kann die Festplatte auch negativ beeinflusst werden. Darüber hinaus sind die unzähligen Funktionen und Möglichkeiten, teilweise ohne darauf aufmerksam zu machen, manchmal etwas versteckt und können leicht übersehen werden, obwohl sie sehr nützlich sind. Damit einher geht auch, dass manche Funktionen in ihrer Wirkungsweise selbst für den erfahrensten Benutzer unklar sein können.

In Zukunft wünschenswert wäre auch eine konkrete Erweiterung einer Fine-Tuning Einstellung innerhalb der Parameter Einstellungen des Data Extractors. Für den Bereich „Error Handling“ existiert die Funktion „Reading retries.“ Im Vergleich dazu beim „Loss of readiness“ Tab nicht. Deshalb muss immer während oder nach einer Sicherung manuell eine Liste für alle Sektoren generiert werden, bei denen die Festplatte ihre Bereitschaft verloren hat. Dafür können dann zwar explizit verschiedene Lesewiederholungen eingestellt werden, aber der Wert für die Wiederholungen ist standardmäßig auf 1 gestellt. So ist der Benutzer jedes Mal dazu gezwungen, die Bereitschaftsfehler eigenständig durch 5-10-maliges Anklicken der betroffenen Sektoren zu korrigieren.

ACE Lab arbeitet akribisch und aktiv an der Weiterentwicklung ihrer Tools und baut regelmäßig viele neue Funktionen ein, denen es teilweise an den korrekten Übersetzungen mangelt, da die Firma ihren Ursprung in Russland hat. Genauso muss bemängelt werden, dass die Aktualisierung der von ACE Lab herausgegebenen Handbücher längst überfällig ist. Im Gegenzug dazu stellt ACE Lab regelmäßige Softwareupdates zur Verfügung und unterstützt den Benutzer durch hilfsbereite und kompetente Mitarbeiter sowie bei Bedarf auch per Fernzugriff. Auch Internetforen, die allerhand Informationen bieten und zum Austausch anregen sowie ein eigener Blog mit den neusten Entwicklungen und Informationen gehört zum Goldstandard. In diesem Zusammenhang liefert das Unternehmen auch vereinzelt Fallanleitungen für kritische oder häufig auftretende Probleme von Festplatten. Diese führen den Benutzer in der Regel auch zum gewünschten Ergebnis, jedoch sind die Hintergründe der Ausführungen oft unklar und ohne Vorwissen schwer nachvollziehbar. Da das Ziel jedes Unternehmens ist, Gewinn zu erzielen, sollte dieser Punkt nicht allzu kritisch betrachtet werden, da hierbei auch Betriebsgeheimnisse einbezogen werden müssen. Bei der Erwähnung von Gewinnen, die das Unternehmen erwirtschaftet, sollte auch angesprochen werden, dass die Anschaffung eines PC-3000 Express Systems je nach Ausstattung mindestens 5000 Euro und bis zu 10000 Euro oder mehr kosten kann. Das ist anfänglich eine beachtliche Investition, die für das System getätigt werden muss und demzufolge auch selten ein System, dass sich an einen privaten Benutzer richtet. Mit der Zeit, unter intensiver Nutzung und je nachdem wer das System für welche Zwecke nutzt, dürfte sich die Investition jedoch lohnen. Dabei sei auf den in Abschnitt 3.1.4 erwähnten finanziellen Aspekt verwiesen. Zu guter Letzt ist der Besitz oder zumindest der Zugang für ein großes Ersatzteillager von Festplatten vorteilhaft bei der Arbeit mit dem PC-3000 Express System. Die in dieser Arbeit vorgestellten Beispiele verlassen sich beide darauf, dass entsprechende Ersatzteilspender vorhanden sind. Vor allem im ersten Beispiel wäre ohne Ersatzköpfe die Sicherung der Daten von Kopf 2 nicht möglich gewesen. Ebenfalls garantiert der Einsatz von Spezialwerkzeugen wie PC-3000 Express nicht immer einen Erfolg bei der

Datensicherung. Festplatten Hersteller implementieren immerzu neue Sicherheitsfunktionen, um ihre Firmware und die Bestandteile einer Festplatte vor Eingriffen zu schützen. Außerdem wollen die Hersteller damit auch dem Drang der Konsumenten nach mehr Sicherheit im Allgemeinen gerecht werden. Dabei wird der Benutzer vor allem vor Herausforderungen wie gesperrte Terminals, aber auch Zugangssperren und Verschlüsselung gestellt. In diesem Zusammenhang hätte die Arbeit näher auf die Möglichkeiten aber auch Grenzen von PC-3000 Express eingehen können.

7.2 Analyse und Vergleich der Leitfäden

In dieser Arbeit wurde ein forensischer Leitfaden zu Spezialverfahren der Datenrettung vorgestellt. Dabei wurde der Leitfaden selbst noch einmal in drei Leitfäden gegliedert. Die drei Leitfäden hätten separat betrachtet alle ihre Gültigkeit, aber aufgrund des Themenbezuges sollte ein logischer Zusammenhang zwischen diesen hergestellt werden. Dabei wurde der Leitfaden nach BSI als erste Grundlage für einen forensischen Leitfaden vorgestellt. Dieser beschreibt als offizieller und forensisch anerkannter Leitfaden, neben anderen Leitfäden wie denen nach Casey; Kent, Chevalier, Grance und Dang oder dem des SAP-Modells, einen allgemeinen Leitfaden für den Ablauf einer forensischen Untersuchung. Die vier genannten Leitfäden oder auch Vorgehensmodelle „variieren mit ihrer Abschnittszahl zwischen drei und zwölf Phasen und sind damit schon auf den ersten Blick sehr unterschiedlich in ihrem Detailierungsgrad.“ [63, S. 18] Dabei weist das SAP-Modell gerade einmal drei Phasen auf, wobei das Modell nach Casey zwölf Phasen beinhaltet. Allerdings liefert das SAP-Modell im Vergleich nur wenige Anhaltspunkte für eine forensische Untersuchung, während das Modell nach Casey die meisten Punkte enthält, damit aber auch einen recht starren Ablauf einer Untersuchung vorgibt. [63] Auch wenn sich hinsichtlich der Prozessbestandteile „auf den ersten Blick wenig Gemeinsamkeiten vermuten lassen, so haben die Vorgehensmodelle doch viele Gemeinsamkeiten, nicht zuletzt, weil sie alle den gleichen prinzipiellen Ablauf einer forensischen Untersuchung beschreiben.“ [63, S. 19] Aus diesem Grund wurde sich in dieser Arbeit vor allem auf den Leitfaden nach BSI bezogen, der sich, mit sechs Phasen und einer während der Untersuchung fortlaufenden Dokumentation, genau in der Mitte aller Modelle ansiedelt. Gemeinsam mit Hinweisen und Beispielen aus dem Themengebiet zu Spezialverfahren der Datenrettung wurden die ersten drei Phasen des Modells nach BSI genau analysiert und dienen als Grundlage für die anderen beiden Leitfäden.

Der anschließende allgemeine Leitfaden für Festplatten soll den Übergang zwischen dem allgemeinen Leitfaden nach BSI und dem themenspezifischen Leitfaden nach ACE Lab

bilden. Ziel der Leitfäden ist es, dem Leser mit jeder Unterteilung des forensischen Leitfadens eine Konkretisierung in Bezug auf das Thema von Spezialverfahren der Datenrettung zu präsentieren. Der allgemeine Leitfaden für Festplatten beginnt dabei mit konkreten themenbezogenen Vorgehensmöglichkeiten, ohne dabei Spezialwerkzeuge einzubeziehen. Dabei soll der allgemeine Leitfaden für Festplatten im Rahmen der strategischen und operationalen Vorbereitung nach BSI eine gute Grundlage für die Analyse mit dem PC-3000 Express Professionell System schaffen. Schlussendlich sollte der Leser dann gut auf eine themenspezifische Untersuchung von Festplattenfehlern mit konkreten Entscheidungsmöglichkeiten vorbereitet sein. Dafür werden im Leitfaden nach ACE Lab die häufigsten Ursachen für Fehler von Festplatten aufgegriffen und dem Leser vermittelt, welche Schritte zur Lösung des Problems beitragen können. Im Anschluss daran folgen zwei konkrete Beispiele von Festplatten, die mit Hilfe des PC-3000 Express Professionell Systems erfolgreich gesichert werden konnten.

7.3 Anforderungen an eine forensische Duplikation vs. PC-3000 Express

Im Rahmen von gerichtsverwertbaren Gutachten könnte der Fall eintreten, dass die angewandten Methoden mit PC-3000 Express angezweifelt werden, die Kompetenz des Zuständigen hinterfragt wird oder das die Datensicherung vermeintlich verändert wurde. Auch wenn die Anforderungen an eine forensische Duplikation bereits ausführlich im Abschnitt 3.1.6 erläutert wurden, soll dieser Abschnitt alle Zweifel an eine forensische Duplikation mit PC-3000 Express beseitigen. Wenn Zweifel bei der Fehlerbehandlung aufkommen, kann PC-3000 eine Übersicht für alle Dateien erstellen. Diese Übersicht enthält dann alle Dateien und die genauen Positionen der Sektorfehler innerhalb der Dateien. So kann genau nachvollzogen werden, ob die Fehler tatsächlich Benutzerdaten betreffen. Häufig stellt sich heraus, dass viele Sektorfehler innerhalb von Systemdateien existieren, welche die Benutzerdaten nicht beeinflussen oder im Spare-Bereich einer Platte liegen, die genauso keinen Einfluss haben. Zudem spielen vereinzelte Sektorfehler, sollten sie innerhalb von Benutzerdaten auftreten, kaum eine Rolle, da sie nur zu einem sehr geringen Teil zu einem Verlust der Anzeige und Qualität beitragen.

Wenn Zweifel bei der Erstellung von Prüfsummen aufkommen, kann mit der dynamischen Eigenschaft der Fehlerentstehung bei Festplatten argumentiert werden. Die Erstellung von kryptographischen Checksummen ist grundsätzlich mit dem Data Extractor gegeben. Der Abgleich von Checksummen zur Verifikation der Integrität der Daten wäre allerdings nicht sehr aussagekräftig, da die Anzahl fehlerhafter Sektoren vor allem bei beschädigten

Festplatten dynamisch ist und sich jederzeit ändern kann. Genauso würde jedes Programm, dass dazu in der Lage ist, Sektorfehler zu erfassen, unter Umständen bei jedem Versuch eine andere Anzahl an Lesefehlern feststellen. Darüber hinaus kommt die Feststellung von Sektorfehlern durch bestimmte Programme auch darauf an, wie entwickelt das Tool ist und welche Funktionen zur Ermittlung von Sektorfehlern unterstützt werden.

Wenn Zweifel bei der Reproduzierbarkeit durch Dritte aufkommen, ist grundsätzlich festzustellen, dass PC-3000 mit den gleichen Mitteln und Werkzeugen dieselben Ergebnisse liefert. Auch hier wäre womöglich ein Unterschied in der Anzahl der Sektorfehler feststellbar. Dennoch kann dann ein Abgleich zwischen den tatsächlich gesicherten Benutzerdaten Abhilfe schaffen und ein Dritter könnte somit die Existenz und Echtheit der festgestellten Daten verifizieren. Normalerweise werden grundsätzlich zur Duplikation eines Datenträgers bei Untersuchungen Writeblocker eingesetzt, die alle Schreibzugriffe auf eine Festplatte, wie durch das Betriebssystem, verhindern. Da die PC-3000 Software aber ein geschlossenes System darstellt, kann ein Betriebssystem eine angeschlossene Festplatte nicht erkennen. Nur wenn dies ausdrücklich vom Benutzer gewünscht ist, wird der Zugriff durch das Betriebssystem erlaubt. Dafür sorgen bestimmte Treiber, die genau solche Schreibzugriffe blockieren, die während der Installation von PC-3000 Software mit installiert werden. Zu guter Letzt unterliegen verfahrensrelevante Daten, die von Behörden erhoben und gespeichert werden, bestimmten Gesetzgebungen. Allen voran die „RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016.“ [64, S. 89] Darin heißt es konkret: „Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht.“ [64, S. 90] In Deutschland hat sich grundsätzlich jedes Bundesland an diese Richtlinie zu halten, wenn es um die Speicherung von Daten geht. Allerdings gestaltet jedes Bundesland die Auslegung der Speicherung von Daten jeweils individuell. Die meisten Bundesländer beschränken sich jedoch darauf, die Dauer der Speicherung von Daten auf das erforderliche Maß zu beschränken. (bsp. Sachsen-Anhalt, Thüringen, Bayern oder Nordrhein-Westfalen [65–68]) Dafür gibt es in der Regel bestimmte Fristen wie zum Beispiel nach 2, 5 oder 10 Jahren, an denen die Daten erneut auf ihren Bedarf und ihre Relevanz geprüft werden und ggf. gelöscht werden. (müssen)

8 Fazit & Ausblick

Das PC-3000 Express Professionell System ist eine innovative, vielfältige und sichere Hardware-Software Lösung der Firma ACE Lab, um Daten von Festplatten mit den unterschiedlichsten Mängeln sichern zu können. Das System dient in erster Linie der Reparatur und Sicherung von Festplatten, wird aber auch erfolgreich von Strafverfolgungsbehörden eingesetzt, um fehlerhafte oder bewusst unzugänglich gemachte Daten von Festplatten zu sichern. Im Rahmen von forensischen Untersuchungen werden die Festplatten nach ihrer Sicherung untersucht und analysiert und können in gerichtsverwertbaren Gutachten als Beweismaterial vor Gericht eingebracht werden. Die Herausforderung bei Spezialverfahren der Datenrettung sowie allgemein bei forensischer Arbeit liegt darin, dass jeder Fall individuell ist. Die beste Software und der ausführlichste Leitfaden führen nicht immer zwangsweise dazu, dass am Ende ein erhofftes Ergebnis erreicht wird. Zudem ist es nicht immer nötig und auch nicht ratsam, sich nur auf automatisierte Prozesse einer Software zu verlassen. Gerade in den hier angeführten Beispielen wurde ersichtlich, dass eine Kombination aus Erfahrung beim Umgang mit Festplatten, qualifizierte Hardware-Software Lösungen und nötige Eigeninitiative dazu geführt haben, dass am Ende alle Daten einer vorher nicht funktionsfähigen Festplatte gesichert werden konnten. Ein Benutzer/Sachbearbeiter sollte deshalb stets ein Auge auf durchgeführte Prozesse haben und diese überprüfen und hinterfragen.

Neben Spezialverfahren der Datenrettung zu Festplatten könnten sich zukünftige Arbeiten vor allem mit der immer weiter verbreiteten Flash-Speicher Technologie auseinandersetzen. Dieser Arbeit ging bereits eine Praktikumsarbeit zur NAND Wiederherstellung mit PC-3000 Flash voran, die ein großes Potential für Erweiterungen bietet, sehr aktuell ist und ein in Zukunft beständiges Thema bleiben wird. Im Kern dieser Arbeit wurden vor allem zwei ausgewählte Beispiele angeführt, die mit Hilfe von PC-3000 Express gesichert werden konnten. Aufgrund vieler unterschiedlicher Festplatten Hersteller sowie unterschiedlichster Arten von Festplatten, könnten zukünftige Arbeiten andere Beispiele von Festplattenproblemen beschreiben und Lösungen zur Sicherung der Daten anbieten. Denkbar wären hier Probleme mit den Service Daten, bei denen Firmware Module repariert werden müssen oder auch Translator Probleme, die aufgrund von Datenverschiebungen vorliegen. Ebenfalls denkbar wäre eine nähere Auseinandersetzung mit den Möglichkeiten der Ausführung von ATA Befehlen sowie herstellerspezifischen Befehlen auf Festplatten. Dabei könnten

eigenständig Versuche zum Reverse Engineering unternommen werden, um das Verhalten von Festplatten zu analysieren. Genauso wurde in dieser Arbeit zwar die Benutzeroberfläche des Data Extractor näher vorgestellt und vereinzelte Funktionen erläutert, aber das Potential dieser Software konnte nicht vollumfänglich vermittelt werden. Gerade die Korrektur von fehlerhaften Sektoren durch den Data Extractor wäre ein weiterer interessanter Ansatz.

Abschließend lässt sich festhalten, dass das PC-3000 Express Professionell System ein ausgereiftes System ist, dass sich auf viel Forschung im Bereich der Festplattentechnik stützt und mit seiner Benutzeroberfläche die Möglichkeit bietet, die Reparatur und Sicherung von Festplatten teilweise automatisiert umzusetzen. Wer mit dem System und Festplatten im Allgemeinen gut vertraut ist, kann in fast jeder Situation Daten auf einer Festplatte erfolgreich sichern.

9 Literatur

[1] J. Kwan, *Western Digital Red Pro WD141KFGX 14TB Review.* [Online]. Verfügbar unter: https://aphnetworks.com/reviews/western-digital-red-pro-wd141kfgx-14tb/2 (Zugriff am: 18. Dezember 2021).

[2] A. Rubtsov, *HDD from Inside: Hard Drive Main Parts.* [Online]. Verfügbar unter: https://hddscan.com/doc/HDD_from_inside.html (Zugriff am: 18. Dezember 2021).

[3] D. Roschkowski, *Aufbau einer Festplatte - Was ist in einer Festplatte drin?* [Online]. Verfügbar unter: https://www.port29.net/blog/aufbau-einer-festplatte.html (Zugriff am: 18. Dezember 2021).

[4] M. Schneider, „Der logische Aufbau einer Festplatte“, 2004. [Online]. Verfügbar unter: https://80686.net/downloads/04-05-19-aufbau-einer-festplatte.pdf

[5] DataLab247, *How Hard Drive works: Firmware on Disk Platter and PCB.* [Online]. Verfügbar unter: https://www.datalab247.com/articles/article6.html (Zugriff am: 18. Dezember 2021).

[6] V. Ottmann, *Schnittstellen: SATA, PATA und USB.* [Online]. Verfügbar unter: https://www.pcwelt.de/produkte/Schnittstellen-SATA-PATA-und-USB-Grosser-Vergleichstest-478147.html (Zugriff am: 4. Januar 2022).

[7] ACELab, *PC-3000 Express.* [Online]. Verfügbar unter: https://www.acelaboratory.com/pc3000.Express.php (Zugriff am: 19. Dezember 2021).

[8] ACE Laboratory Ltd, *ACE Lab PC-3000 Data Recovery Equipment.* [Online]. Verfügbar unter: https://www.acelaboratory.com/ (Zugriff am: 3. Januar 2021).

[9] ACE Laboratory Ltd Russia, „SEAGATE F3 architecture“ in *PC-3000 EXPRESS / UDMA / PORTABLE*, 9-16; 50-57.

[10] J. Knauer und H. Baier, „Zur Sicherheit von ATA-Festplattenpasswörtern“, S. 1–12. [Online]. Verfügbar unter: https://www.dasec.h-da.de/wp-content/uploads/2012/02/2012_09_Knauer_Baier_DACH.pdf

[11] ACELab team, *PC-3000 Portable III/Express/UDMA. How to Fix a Rosewood SSHD with a Damaged NAND Chip.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/how-to-fix-a-rosewood-sshd-with-a-damaged-nand-chip.html (Zugriff am: 31. Dezember 2021).

[12] www.bvg-group.ru, *HDD Repair Tool: Basic Documentation.* [Online]. Verfügbar unter: http://www.hddoracle.com/viewtopic.php?f=166&t=1158 (Zugriff am: 29. Dezember 2021).

[13] ACE Laboratory Ltd Russia, „PC-3000 TOOLS“, S. 20–23. [Online]. Verfügbar unter: https://blog.acelaboratory.com/

[14] D. Mikkelson, *Does This Photo Show Computer Storage in 1956?: Imagine a disk drive that weighed over a ton but stored only 5MB of data.* [Online]. Verfügbar unter: https://www.snopes.com/fact-check/computer-storage-1956/ (Zugriff am: 18. Dezember 2021).

[15] D. Löbe, *Festplatte – So hat sie sich entwickelt.* [Online]. Verfügbar unter: https://www.dirks-computerecke.de/hardware/festplatte.htm (Zugriff am: 18. Dezember 2021).

[16] P. Böret und R. Kern, „Elektronische Beweismittelsicherung auf der Basis von Computer Forensik“ in *Security, E-Learning, E-Services: 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf*, 2003, S. 659–662.

[17] D. Heinson, *IT-Forensik: Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen*. Zugl.: Kassel, Univ., Diss., 2014. Tübingen: Mohr Siebeck, 2015. [Online]. Verfügbar unter: https://kobra.uni-kassel.de/bitstream/handle/123456789/2016110751250/DissertationDennisHeinson.pdf;jsessionid=F85A9ED630A986DA3225F2C9B6680BE1?sequence=1

[18] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden IT-Forensik“, 8; 13-14; 24; 26; 88-89; 235, 2011. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf;jsessionid=B6ADF93B15A7E8894C551BC10E45A440.internet462?__blob=publicationFile&v=1

[19] A. Burton und E. Hennan, *Datenwiederherstellung (Data Recovery).* [Online]. Verfügbar unter: https://www.computerweekly.com/de/definition/Datenwiederherstellung-Data-Recovery (Zugriff am: 3. Januar 2021).

[20] IT-SERVICE24 Datenrettung, *Festplatten Aufbau Grundlagen und Herstellung Definition & Begriffserklärung.* [Online]. Verfügbar unter: https://www.it-service24.com/lexikon/f/festplatten-aufbau/ (Zugriff am: 18. Dezember 2021).

[21] H. Strass, *Grundlagen der Festplattentechnik - Teil 1.* [Online]. Verfügbar unter: https://www.channelpartner.de/a/grundlagen-der-festplattentechnik-teil-1,634228 (Zugriff am: 18. Dezember 2021).

[22] Seagate Technology und J. Larson, *How a Hard Disk Drive Works.* [Online]. Verfügbar unter: https://www.youtube.com/watch?v=NtPc0jI21i0 (Zugriff am: 18. Dezember 2021).

[23] it-surfer.de, *Festplatte / HDD.* [Online]. Verfügbar unter: https://www.it-surfer.de/hardware/grundlagen/festplatte-hdd/ (Zugriff am: 18. Dezember 2021).

[24] PC-HELPSITE.NET Computer, Hardware, Software und Internet, *Hardware-Grundlagen: Festplatte oder auch Hard Disk genannt.* [Online]. Verfügbar unter: https://www.pc-helpsite.net/hardware-grundlagen-festplatte/ (Zugriff am: 18. Dezember 2021).

[25] S. Dipl.-Ing. (FH) Luber und J. Ehneß, *Was ist ein Schreib-/Lesekopf?* [Online]. Verfügbar unter: https://www.storage-insider.de/was-ist-ein-schreib-lesekopf-a-883478/ (Zugriff am: 18. Dezember 2021).

[26] O. Mezger, *Dateisysteme: 1. Festplatte physikalisch bzw. logisch.* [Online]. Verfügbar unter: https://mezdata.de/betriebssystem/020_dateisysteme/ (Zugriff am: 18. Dezember 2021).

[27] S. Hsiung, *Logical organization of hard disk.* [Online]. Verfügbar unter: https://www.datarecoverytools.co.uk/2009/11/27/logical-organization-of-hard-disk/ (Zugriff am: 18. Dezember 2021).

[28] H. Strass, *Grundlagen: Festplattentechnik: Anordnung der Daten.* [Online]. Verfügbar unter: https://www.tecchannel.de/a/grundlagen-festplattentechnik,401602,5 (Zugriff am: 18. Dezember 2021).

[29] SNIA, *Data Structures on Disk Drives.* [Online]. Verfügbar unter: https://www.snia.org/education/storage_networking_primer/stor_devices/data_structure (Zugriff am: 18. Dezember 2021).

[30] W. Fischer, *CHS und LBA Adressierung von Festplatten.* [Online]. Verfügbar unter: https://www.thomas-krenn.com/de/wiki/CHS_und_LBA_Adressierung_von_Festplatten (Zugriff am: 18. Dezember 2021).

[31] S. Dillon, „Hide and Seek: Concealing and Recovering Hard Disk Data: 2.2 Data Access and Transfer“, S. 4, 2006. [Online]. Verfügbar unter: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.9336&rep=rep1&type=pdf

[32] SEAGATE, *Braucht meine Festplatte ein Firmware-Update?: Was ist Firmware?* [Online]. Verfügbar unter: https://www.seagate.com/de/de/support/kb/does-my-drive-need-a-firmware-update-206091en/ (Zugriff am: 18. Dezember 2021).

[33] I. Sutherland, G. Davies und A. Blyth, „Malware and steganography in hard disk firmware“, *J Comput Virol*, Jg. 7, Nr. 3, S. 215–219, 2011, doi: 10.1007/s11416-010-0149-x.

[34] X. He, Z. Wang, J. Zhang und C. Ji, „Research on security of hard disk firmware“ in *2011 International Conference on Computer Science and Network Technology (ICCSNT)*, Harbin, China, 2011, S. 690–693, doi: 10.1109/ICCSNT.2011.6182060.

[35] SECURE DATA RECOVERY, *Firmware Failure.* [Online]. Verfügbar unter: https://www.securedatarecovery.com/services/hard-drive-recovery/firmware-failure (Zugriff am: 18. Dezember 2021).

[36] SERT DATARECOVERY, *What exactly is firmware on a hard drive and where is it located?* [Online]. Verfügbar unter: https://www.sertdatarecovery.com/hard-drive-data-recovery/how-to-fix-corrupted-or-damaged-firmware (Zugriff am: 18. Dezember 2021).

[37] A. Berkman, „Hiding Data in Hard-Drive’s Service Areas“, S. 3, 2013. [Online]. Verfügbar unter: https://dl.packetstormsecurity.net/papers/general/SA-cover.pdf

[38] I. Sutherland, G. Davies, N. Pringle und A. Blyth, „The Impact of Hard Disk Firmware Steganography on Computer Forensics“, *JDFSL*, S. 76–77, 2009, doi: 10.15394/jdfsl.2009.1059.

[39] G. Davies und I. Sutherland, „Hard Disk Storage: Firmware Manipulation and Forensic Impact and Current Best Practice“, *Annual ADFSL Conference on Digital Forensics, Security and Law*, S. 55–62, 2010. [Online]. Verfügbar unter: https://commons.erau.edu/cgi/viewcontent.cgi?article=1111&context=adfsl

[40] V. Damjanovski, *CCTV: Networking and Digital Technology*. Elsevier, 2014. [Online]. Verfügbar unter: https://www.sciencedirect.com/book/9780124045576/cctv#book-info

[41] T. Sterling, *High Performance Computing: Modern Systems and Practices*. Saint Louis: Elsevier Science & Technology, 2018. [Online]. Verfügbar unter: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5754509

[42] MikiWiki, *Advanced Technology Attachment.* [Online]. Verfügbar unter: http://mikiwiki.org/wiki/Advanced_Technology_Attachment (Zugriff am: 18. Dezember 2021).

[43] C. Wu und R. Buyya, *Cloud Data Centers and Cost Modeling: A Complete Guide To Planning, Designing and Building a Cloud Data Center,* 1. Aufl. s.l.: Elsevier Reference Monographs, 2015. [Online]. Verfügbar unter: http://gbv.eblib.com/patron/FullRecord.aspx?p=1980479

[44] ITWissen.info, *ATA-Schnittstelle.* [Online]. Verfügbar unter: https://www.itwissen.info/ATA-advanced-technology-attachment-ATA-Schnittstelle.html (Zugriff am: 18. Dezember 2021).

[45] P. Schnabel, *SATA / Serial-ATA.* [Online]. Verfügbar unter: https://www.elektronik-kompendium.de/sites/com/0808061.htm (Zugriff am: 18. Dezember 2021).

[46] W. Matthes, „Technik der Personalcomputer: 9. IDE/ATA-Schnittstelle“, *Technisches Lehrheft 9*, S. 1–12. [Online]. Verfügbar unter: https://www.controllersandpcs.de/lehrarchiv/pdfs/tdp/tlh4_09.pdf

[47] Technical Committee T13 AT Attachment, *Standards - Published.* [Online]. Verfügbar unter: https://t13.org/standards-published (Zugriff am: 3. Januar 2021).

[48] T13 Technical Editor: Curtis E. Stevens, *Information technology - ATA Command Set - 4 (ACS-4).* [Online]. Verfügbar unter: https://dokumen.tips/documents/ata-command-set-4-acs-4.html.

[49] ACE Laboratory Ltd Russia, „Kernel of PC-3000 for Windows“ in *PC-3000 EXPRESS / UDMA / PORTABLE*, S. 19.

[50] ACE Laboratory Ltd Russia, Hg., *PC-3000 EXPRESS / UDMA / PORTABLE.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/

[51] ACE Laboratory Ltd Russia, „Data Extractor UDMA“, S. 5–35. [Online]. Verfügbar unter: https://blog.acelaboratory.com/

[52] A. Vidström, „Computer Forensics and the ATA Interface“, 2005. [Online]. Verfügbar unter: https://manualzz.com/doc/878632/computer-forensics-and-the-ata-interface.

[53] IT-FORENSIK WIKI Hochschule Wismar, *Strategische Vorbereitung.* [Online]. Verfügbar unter: https://it-forensik.fiw.hs-wismar.de/index.php/Strategische_Vorbereitung (Zugriff am: 29. Dezember 2021).

[54] IT-FORENSIK WIKI Hochschule Wismar, *Operationale Vorbereitung.* [Online]. Verfügbar unter: https://it-forensik.fiw.hs-wismar.de/index.php/Operationale_Vorbereitung (Zugriff am: 29. Dezember 2021).

[55] IT-FORENSIK WIKI Hochschule Wismar, *Datensammlung.* [Online]. Verfügbar unter: https://it-forensik.fiw.hs-wismar.de/index.php/Datensammlung (Zugriff am: 29. Dezember 2021).

[56] ACELab team, *PC-3000 for HDD. Basic HDD diagnostics procedure.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/basic-hdd-diagnostics-procedure.html (Zugriff am: 29. Dezember 2021).

[57] ACELab team, *PC-3000 for HDD. Seagate F3 architecture drives specific diagnostics.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/?s=PC-3000+for+HDD.+Seagate+F3+architecture+drives+specific+diagnostics (Zugriff am: 29. Dezember 2021).

[58] ACELab team, *PC-3000 for HDD. WD Marvell drives specific diagnostics.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/?s=PC-3000+for+HDD.+WD+Marvell+drives+specific+diagnostics. (Zugriff am: 29. Dezember 2021).

[59] ACELab team, *PC-3000 HDD. How to find out the problems in WD Marvell drives.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/pc-3000-hdd-how-to-find-out-the-problems-in-wd-marvell-drives (Zugriff am: 29. Dezember 2021).

[60] DonorDrives Ultimate Storage Device Marketplace, *Head Swap Donor Matching Guide.* [Online]. Verfügbar unter: https://www.donordrives.com/blog/matching-guide (Zugriff am: 29. Dezember 2021).

[61] ACELab team, *PC-3000 for HDD. Seagate F3. Practical cases. How to get the Service Area access if one of non-system heads is damaged.* [Online]. Verfügbar unter: https://blog.acelaboratory.com/?s=PC-3000+for+HDD.+Seagate+F3.+Practical+cases.+How+to+get+the+Service+Area+access+if+one+of+non-system+heads+is+damaged. (Zugriff am: 29. Dezember 2021).

[62] T. Noergaard, *Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers,* 2. Aufl. Burlington: Elsevier Science, 2012. [Online]. Verfügbar unter: http://gbv.eblib.com/patron/FullRecord.aspx?p=1105867

[63] G. Dreo, F. Tietze, P. Hillmann, M. Golling und B. Stelte, *Grundlagen der IT-Forensik.* [Online]. Verfügbar unter: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjj4emcto71AhWQ3oUKHYedDjQQFnoECAIQAQ&url=https%3A%2F%2Fwww.unibw.de%2Ftechnische-informatik%2Fmitarbeiter%2Fprofessoren%2Fdreo%2Fpublikationen%2Fseminararbeiten-forensik-2013.pdf%2F%40%40download%2Ffile%2FSeminararbeiten-Forensik-2013.pdf&usg=AOvVaw30h9_sTBhPBZMjkajvdojY (Zugriff am: 31. Dezember 2021).

[64] Das Europäische Parlament und der Rat der Europäischen Union, *Amtsblatt der Europäischen Union: RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016.* [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680&from=DE (Zugriff am: 31. Dezember 2021).

[65] Freistaat Thüringen - Online-Verwaltung Thüringen, *Thüringer Gesetz zum Schutz der freiheitlichen demokratischen Grundordnung und zur Vorbeugung vor Gefahren für die freiheitliche demokratische Grundordnung (Thüringer Verfassungsschutzgesetz - ThürVerfSchG -) Vom 8. August 2014*: § 13 Speicherung, Veränderung und Nutzung personenbezogener Daten.* [Online]. Verfügbar unter: https://landesrecht.thueringen.de/bsth/document/jlr-VerfSchutzGTH2015pP13 (Zugriff am: 4. Januar 2021).

[66] Bayerische Staatskanzlei, *Art. 53 Allgemeine Regeln der Datenspeicherung und sonstigen Datenverarbeitung.* [Online]. Verfügbar unter: https://www.gesetze-bayern.de/Content/Document/BayPAG-53 (Zugriff am: 4. Januar 2021).

[67] Ministerium des Inneren des Landes Nordrhein-Westfalen, *Geltende Gesetze und Verordnungen (SGV. NRW.) mit Stand vom 1.1.2022: Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW); Bekanntmachung der Neufassung vom 25.07.2003.* [Online]. Verfügbar unter: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=5173&anw_nr=2&aufgehoben=N&det_id=469934 (Zugriff am: 4. Januar 2021).

[68] Sachsen-Anhalt - Landesrecht Sachsen-Anhalt, *Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt (VerfSchG-LSA) in der Fassung der Bekanntmachung vom 6. April 2006: § 9 Speicherung, Veränderung und Nutzung personenbezogener Daten.* [Online]. Verfügbar unter: https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-VerfSchutzGST2006V3P9 (Zugriff am: 4. Januar 2021).

Eidesstattliche Erklärung

Versicherung an Eides statt

Ich, Marius Julian Walter Zimmer, Matrikel 49740,

versichere an Eides statt durch meine Unterschrift, dass ich die vorstehende Arbeit selbständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe, mich auch keiner anderen als der angegebenen Literatur oder sonstiger Hilfsmittel bedient habe.

Ich versichere an Eides statt, dass ich die vorgenannten Angaben nach bestem Wissen und Gewissen gemacht habe und dass die Angaben der Wahrheit entsprechen und ich nichts verschwiegen habe. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Leipzig, 14.01.2022 

Ort, Datum Unterschrift