Fakultät für Ingenieurswissenschaften

Projektarbeit

IT-Forensik Projekt II

Write-Blocking: ein Überblick und vergleichende Gegenüberstellung von Write-Blockern mit dem Schwerpunkt auf Open-Source und Software-Lösungen

Studiengang IT-Forensik

Sommersemester 2022

eingereicht von: Christian Peter

Yannick Schmitz

Christopher Bublies

Erstgutachter: Prof. Antje Raab-Düsterhöft

Hamburg, den 19.06.2022

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
4Deck	Forensics module for The Deck
AFF	Advanced Forensic Format
BSI	Bundesamts für Sicherheit in der Informationstechnik
CC	Creative Commons
CFTT	Computer Forensics Tool Testing Program
DC3DD	Department of Defense Cyber Crime Center DD
DCFLDD	Department of Defense Computer Forensics Lab DD
DD	disk dump, duplicate data, ursprgl. copy and convert
DIN	Deutsche Institut für Normung e. V.
EN	Europäische Norm
FAT	File Allocation Table
FTDI	Future Technology Devices International Ltd
EWF	Expert Witness Format
IDE	Integrated Drive Electronics
iSCSI	internet Small Computer System Interface
ISO	International Organization for Standardization
MD5	Message-Digest Algorithm 5
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
PATA	Parallel Advanced Technology Attachment
SATA	Serial Advanced Technology Attachment
SAS	Serial Attached SCSI
SHA1	Secure Hash Algorithm 1
UDeck	USB Deck
UDMA	Ultra-Direct Memory Access

1 Einleitung / Motivation

Die zunehmende Bedeutung IT-forensischer Prozesse wird insbesondere für Strafverfolgungsbehörden in der jährlich vom Bundeskriminalamt (BKA) veröffentlichen polizeilichen Kriminialitätsstatistik deutlich. Fallzahlen von Cybercrime-Delikte verzeichnen seit Jahren einen permanenten Anstieg. Vermehrt bewegen sich zudem Deliktsfelder in den digitalen Raum. Straftaten wie Betrug, Sexualstraftaten oder Beleidigungen werden immer häufiger über das Internet oder auf Social-Media-Plattformen ausgeübt. Diese Gruppe von Straftaten, die sowohl mit als auch ohne Zunahme des Internets verübt werden können, werden unter „Cybercrime im weiteren Sinne“ subsummiert. Entsprechend groß ist die Bandbreite von Straftaten, die mit technischen Geräten wie PCs, Mobiltelefonen oder Festplattenspeichern begangen werden können. 294.665 Straftaten mit dem Tatmittel Internet wurden 2019 polizeilich erfasst. Die Tendenz ist weiter steigend (1). Dies stellt Strafverfolgungsbehörden vor die Herausforderung, Beweismittel mit dem Hintergrund einer späteren Gerichtsverwertbarkeit sichern zu müssen. Im Zuge dessen haben sich verschiedene Herangehensweisen herauskristallisiert, die übereinstimmend eine forensische Duplikation des Datenträgers als Grundlage voraussetzen.

Im Leitfaden IT-Forensik des Bundesamts für Sicherheit in der Informationstechnik (BSI) (2) wird das Anfertigen einer forensischen Duplikation beim Vorgehen einer forensischen Untersuchung nach der strategischen und operationalen Vorbereitung im Abschnitt „Datensammlung“ verortet. Das BSI führt aus, dass die Unveränderthеit des Dateninhalt eine absolute Notwendigkeit sei, wenn der Datenträger Beweisstück eines juristischen Prozesses ist. Realisiert wird dies im IT-forensischen Sicherungsprozess mit dem Einsatz von sogenannten Writeblockern, die einen schreibenden Zugriff auf Datenträger unterbinden, sowie Hashfunktionen zur Wahrung und des Nachweises der Integrität des erstellten Abbilds.

Diese Arbeit stellt die unterschiedlichen Funktionsweisen von Writeblockern bei der Sicherung von Speichergeräten vergleichend gegenüber. Insbesondere werden auf die Unterschiede zwischen Hardware-Writeblockern sowie softwarebasierten Writeblockern im Sicherungsprozess eingegangen. Die Arbeit beschränkt sich ausschließlich auf die Sicherung von Festplatten sowie USB-Sticks und lässt flüchtige Speicher wie Arbeitsspeicher außen vor. Ebenfalls wird nicht auf Mobilgeräte eingegangen, da die Sicherung im Normalfall nur Veränderung am Dateninhalt wie zum Beispiel durch die Aktivierung des USB-Debugging-Modus bei Android-Geräten möglich ist. Grundsätzlich gilt: Jedwede Änderungen müssen detailliert protokolliert und begründet werden, um in einem späteren Gerichtsprozess als Beweismittel von allen Verfahrensbeteiligten anerkannt zu werden.

2 Vorüberlegungen

2.1 Grundlagen

Schreibschutz oder Writeblocker dienen zum Schutz vor Schreibzugriffen bei angeschlossenen Speichermedien. Sie verhindern sowohl das Erstellen von Dateien als auch Prüfungen des Betriebssystems auf Partitionsfehler oder das Reorganisieren von Daten. Besonders für die Gerichtsverwertbarkeit und der „chain of custody" von Beweisen also konfiszierten Speichermedien wie Festplatten, USB-Sticks oder sonstigen Datenspeichern ist der Schreibschutz von großer Bedeutung.

Writeblocker können dabei auf zwei Arten funktionieren. Einmal als Software-Writeblocker und auf der anderen Seite Hardware-Writeblocker. Je nach Einsatzgebiet haben beide Varianten ihre Vor- und Nachteile, die in dieser Arbeit untersucht werden.

2.1.1 Hardware-Writeblocker

Hardware-Writeblocker sind spezielle, nur diesen einen Zweck bestimmte Geräte, die von Herstellern wie Tableau oder Wiebetech entwickelt und vertrieben werden. Zumeist sind sie auf eine Anzahl von Anschlusstypen festgelegt und können hingegen nicht erweitert werden. Somit muss bei Erwerb geprüft werden, welche Anschlüsse wie USB oder SATA und IDE unterstützt werden. Des Weiteren muss geprüft werden, welche Version oder Spezifikation der Übertragungsstandards möglich sind. Je älter die USB-Version bspw. 2.0, desto langsamer und unsicherer funktioniert eine Übertragung eines USB 3.1 Sticks. Hieraus ergibt sich oftmals ein Nachteil der Hardware-Writeblocker, da die Anschaffung eines extra Gerätes mit nur einem Verwendungszweck und hohen Kosten verbunden ist.

Der große Vorteil gegenüber Software-Writeblockern liegt in der einfachen Bedienbarkeit. Zumeist gibt es eine Stromversorgung und zwei Anschlüsse. Einmal gibt es den Anschluss für das Hostsystem auf der einen Seite und auf der anderen Seite der Anschluss für die Quelle (mindestens ein Anschluss wie USB, aber auch SATA etc.) für das zu sichernde Medium. Durch einfaches Plug'n'Play können zu untersuchende Medien angeschlossen werden und über LEDs oder Anzeigen bedienerfreundlich den jeweiligen Status anzeigen. Meistens bedeuten grüne LEDs einen aktiven Schreibschutz.

Ein weiterer Vorteil liegt in der Geschwindigkeit und somit in der Bandbreite der zu übertragenden Daten, die direkt am Hostsystem zur Verfügung stehen und keine Ressourcen vom Hostsystem benutzt werden.

Die Funktionsweise von Hardware-Writeblockern liegt entweder darin alle gesendeten Befehle zu prüfen und keine Schreibbefehle an das Gerät weiterzusenden oder die Variante alle Befehle an das Medium zu unterbinden.

Einfachere und veraltete Hardware-Writeblocker lassen sich durch Jumper oder Pins an den Mainboards setzen, um der Firmware zu signalisieren, keine Schreibbefehle zu erlauben. Heute noch gängig und bekannt ist der Lock-Schalter an SD-Karten.

Trotz des einfachen Aufbaus von Hardware-Writeblockern gibt es immer mehr Möglichkeiten diese mit bedienerfreundlichen Oberflächen und neuen Features auszustatten. Dies führte allerdings dazu, dass auch Hardware-Writeblocker Sicherheitslücken aufweisen und nach Ausnutzung dieser einen Schreibschutz nicht sicherstellen können. (3)

2.1.2 Software-Writeblocker

Software-Writeblocker beschreiben Software, die über verschiedene Methoden auf unterschiedlichen Betriebssystemen Schreibzugriffe auf Medien verhindern. Dabei gibt es nicht die eine klassische Software, sondern eine Auswahl an verschiedener proprietärer Software oder Open-Source-Projekten. Diese Entwicklung entsteht durch die große Bandbreite und Anpassbarkeit von Betriebssystemen.

Zur Funktionsweise muss hierbei zwischen den einzelnen Betriebssystemen unterschieden werden. Linux-Distributionen ermöglichen direkt ein Einhängen und Einlesen eines Mediums als readonly. Bei Windows lassen sich oftmals über Registryeinstellungen oder angepasste Treiber die Schreibefehle filtern und blockieren. Ebenso ist bei MacOS möglich, die Einstellungen anzupassen, um Befehle an das Medium zu blockieren. Da viele Betriebssysteme direkt beim Anschließen Checks des Datenträgers durchführen, besteht hier die Gefahr, dass Daten verändert werden, bevor der Schreibschutz der Software greift.

Dem entgegen können ein Livesystem oder BIOS-Einstellungen angepasst werden, um auf der darunterliegenden Ebene Schreibzugriffe zu verbieten. Dazu gehört bspw. die Methode den Interrupt 0x13 zu setzen.

Zusammengefasst ist das Vorhandensein eines Hostsystemes eine Voraussetzung für Software-Writeblocker. Dieses System muss bestimmten Anforderungen genügen, um es für ein Projekt einsetzbar zu machen. Die Hardware muss leistungsfähig sein, da das Betriebssystem während der Sicherung des angeschlossenen Mediums Ressourcen für sich beansprucht. Um Medien anzuschließen, müssen dafür passende Anschlüsse vorhanden sein, können aber ferner durch Hubs erweitert werden. Vom forensischen Hintergrund ausgehend wären die Hostsysteme vornehmlich Laptops, um Medien vor Ort zu sichern. Nativ ohne Adapter lassen sich oftmals USB-Geräte und SD-Karten auslesen. Für alle anderen Festplattenanschlüsse wie SATA, IDE und M2 müssen Adapter genutzt werden. Bei Workstations lassen sich mehrere Anschlüsse direkt

nutzen sowie die Erweiterbarkeit um zusätzliche Module für neue Anschlüsse ist gegeben, aber man verliert die Portabilität.

Das Hostbetriebssystem stellt ebenfalls einen wichtigen Faktor zur Verwendung von Software-Writeblockern da. Aufgrund von Updates oder anderer Softwareinstallationen können Einstellungen und besonders bei Windows gesetzte Registrywerte überschrieben oder verändert werden. Durch Upgrades können sich Befehle oder Befehlsketten ändern, sodass die Blockierung nicht mehr die aktuellen Befehle verhindert. Eine Schicht tiefer gibt es ebenso Anpassungen und Updates der Firmware und Treiber für angeschlossene Datenträger.

Besonders die letzten Argumente führen dazu, dass allgemein Software-Writeblocker als weniger sicher angesehen werden und die Empfehlung oder allgemein herrschende Meinung zugunsten von Hardware Writeblockern gegeben wird.

2.1.3 Imaging Prozess

Um forensisch Datenträger und darauf befindliche Daten zu sichern, werden diese typischerweise nicht direkt verwendet, sondern über Imager gesichert. Es wird ein Image oder auch eine bitweise Kopie vom Ausgangsmaterial erstellt. Diese Kopie kann in diversen Formaten mit verschiedenen Eigenschaften vorliegen. Beginnend vom RAW Format, welches eine direkte bitweise Kopie ist, bis hin zu speziellen forensischen Formaten wie SMART und AFF, die weitere aufbereitete Zusatzinformationen mitspeichern.

Für die in dieser Arbeit folgende Durchführung wurde das EWF Format (.E01) ausgewählt, da es stark verbreitet ist und auch im Studium schon Anwendung gefunden hat. Zur Erstellung der Images wird die Software FTK Imager benutzt. FTK steht hier für Forensik Toolkit und bezeichnet eine größere Suite zur forensischen Analyse von Datenträgern.

Da der Fokus hier auf den Writeblockern liegt, findet nur der FTK Imager Verwendung. Der FTK Imager ist eine eigenständige Software zum Sichern, Verifizieren und Auslesen von Datenträgern. Dabei unterstützt der FTK Imager viele Dateisysteme wie gängige NTFS, FAT32, ext4 Systeme. Allerdings können auch APFS, HFS und Reiser gelesen werden.

Zum Download stehen aktuell die Version 3.1.1 als Kommandozeilenversion ohne GUI sowie 4.7.1.2 als grafische Oberfläche zur Verfügung. Der Download ist von der Webseite ohne Registrierung und Kosten möglich. Die Softwareversion wird nur in Englisch angeboten und kommt von der Firma AccessData bzw. exterro.

Ein wichtiger Hinweis aus der Dokumentation zum FTK Imager ist die Warnung, unbedingt einen Writeblocker zwischen Host und dem zu sichernden Medium zu verwenden (4).

2.2 Testaufbau

In Vorbereitung auf das Projekt wurden Datenträger beschafft, die im späteren Testaufbau gesichert werden sollen. Um für jedes Mitglied der Projektgruppe identische Voraussetzungen zu schaffen, wurden je drei Datenträger derselben Marke und desselben Typs bereitgestellt.

Es handelt sich im Einzelnen um je drei:

- 3,5"-Festplatten vom Typ: Seagate ST500DM002_1
  (500GB, 7200 U/min, SATA 6Gb/s)
- 2,5"-Festplatten vom Typ: Western Digital WD500BPVT
  (500GB, 5400 U/min, SATA 3Gb/s)
- USB3-Sticks vom Typ: Sandisk Ultra 32GB
- USB2-Sticks vom Typ: Emtec USB 2.0 Stick 8GB
- USB2-Sticks vom Typ: Imation Nano 2GB

Ebenfalls wurden drei Festplatten mit IDE-Anschluss vom Typ Hitachi HDT722516 beschafft. Hier kam es jedoch zu Ausfällen und Lesefehlern im späteren Verlauf der Testvorbereitung, so dass von diesem Typ Datenträger Abstand genommen wurde.

2.3 Vorbereitung der Test-Medien

Die vorhandenen Test Medien wurden in einem ersten Schritt gewiped bzw. genullt. Im forensischen Kontext findet sich hier häufig die Bezeichnung „Sterilisation“. Dazu wurden die Festplatten in das Gerät „Logicube Forensic Dossier“ als „Destination Drive“ eingesetzt ein Wipe-Befehl ausgeführt. So konnten je zwei Festplatten parallel gewiped werden.

Die Sterilisation der USB-Sticks erfolgte über den Linux „dd“-Befehl:

```
[christian-20b7s2qn02 prosch]# dd if=/dev/zero of=/dev/sdc bs=1M
dd: Fehler beim Schreiben von '/dev/sdc': Auf dem Gerät ist kein Spei
cherplatz mehr verfügbar
```

Eine Sammlung von Fülldaten wurde von Digital Corpora heruntergeladen:

https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/

Hierbei handelte es sich um die Archive: doc.zip, docx.zip, files.jpeg.tar, ppt-part1.zip, ppt-part2.zip und txt.zip. Diese Dateien sind lizenzfrei nach CC0 nutzbar.

Je eine der SATA-Festplatten vom Typ Western Digital und Seagate wurden über das Linux Tool GParted mit einer Partitionstabelle vom Typ „msdos“ und einer NTFS Partition mit einer Größe von 476939 MB versehen. Anschließend wurden die

heruntergeladenen Archive mittels des Dateimanagers Krusader auf die Datenträger entpackt. Nach dem Entpacken wiesen die Datenträger einen Füllstand von 171,1GB auf. Nach der Befüllung mit Daten, wurden die Festplatten mittels des Logicube Forensic Dossier auf die jeweils typidentischen Fesplatten geklont.

Bild 1: Forensic Dossier mit Seagate Festplatte als Source Drive

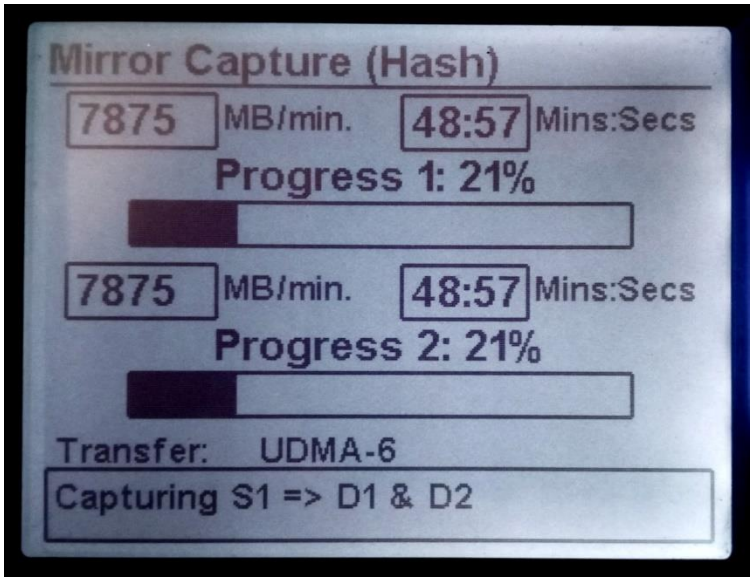

Bild 2: Forensic Dossier – Anzeige bei der Duplikation eines Mediums auf zwei Zieldatenträger

Auch die USB-Sticks wurden über die Software GParted mit einer msdos-Partitionstabelle versehen. Als Dateisystem wurde Fat32 gewählt. Anschließend wurden die Befüllungen entsprechend der vorhandenen Speicherkapazität gewählt:

Die Ordner 000-015 aus dem Archiv doc.zip wurden auf den 2GB Stick (Imation Nano) kopiert und so ein Füllstand von 1,5GB erreicht. Auf den 32GB Stick (Sandisk) wurde das

gesamte Archiv doc.zip entpackt und auf den 8GB Stick (Emtec) die Ordner 000-030 aus dem doc.zip Archiv. Die so bespielten Sticks wurden über den Wiebetech USB3.1 Write Blocker unter Windows 11 mittels der Software Passmark imageUSB gesichert und die jeweils typidentischen USB-Sticks anschließend mit diesen Images beschrieben.

Die erstellten Datenträger wurden zur Verifikation des Klonvorgangs mittels der Software FTK Imager 4.5.0.3 im EWF-Modus unter Verwendung eines entsprechenden Write-Blockers (Wiebetech USB3.1 Write Blocker und Wiebetech Forensic Ultradock v5) gesichert. Es ergaben sich die folgenden Hash-Werte:

Seagate ST500DM002:

MD5 checksum: ca6f055db13bbff662be29a91859538e
SHA1 checksum: 6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Western Digital WD500BPVT:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f
SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

USB 2.0 Stick Emtec 8GB:

MD5 checksum: eba107b6e7f98d667da7b6292b1c4b0e
SHA1 checksum: f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

USB 3.0 Stick SanDisk 32GB:

MD5 checksum: 3a36a973c1470c47dc0d9b34619d36f5
SHA1 checksum: c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

USB 2.0 Stick Imation Nano 2GB:

MD5 checksum: f4bc5f9fa365c3aa076a11c38514c78f
SHA1 checksum: 3ab90273e23ec84b994cbf7973a5e4a6071508f0

Vom Testmedium USB-Stick Imation Nano 2GB konnten nur zwei Geräte mit identischem Hash-Wert erzeugt werden. Dies begründet sich in einer abweichenden Sektorenzahl des dritten Exemplares dieses Mediums. Zwei Sticks weisen 3911680 Sektoren auf, der dritte jedoch 3913728. Eine hashidentische physikalische Sicherung ist so nicht möglich. Eine Sicherung der vorhandenen Partition der Geräte erzeugt hingegen identische Werte. Da sich die Sicherungszeit der USB-Sticks über die genannte Methode nur unwesentlich unterschied und der „größere" Stick sich hierbei im Mittelfeld befand (Zeitspanne: 1 Minute 54 Sekunden bis 1 Minute 57 Sekunden), wurde der abweichende Stick ebenfalls für den Test herangezogen und wird für den Test der Hardware-Write-Blocker verwendet. Die ermittelten Hash Werte lauten:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60
SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

3 Bewertungsschema

3.1 Beurteilung des Schreibschutzes

Im Zuge der Bewertung eines Writeblockers ist es zunächst die Fähigkeit und Effektivität des Schreibschutzes zu bewerten. Diese Fähigkeit wird entsprechend der durchgeführten Tests unterteilt in:

- **den Schutz gegen Dateioperationen**
- **den Schutz gegen Formatierung / Partitionierung**
- **den Schutz gegen Operationen auf Blockebene** (durch Hexedit)

Sofern möglich, wird ein finaler Test mit dem CRU WriteBlocking Validation Utility, das automatisiert Schreibversuche absetzt, durchgeführt.

Je nach Testergebnis, wird ein Testlauf bei erfolgreichem Schreibschutz mit „PASS“ und ein fehlgeschlagener mit „FAIL“ bewertet. Im Falle des CRU Utility Tests kann die Bewertung entfallen, wenn dieser Test bei dem zu testenden WriteBlocker aktuell nicht möglich ist. Insgesamt gilt die Beurteilung des Schreibschutzes als bestanden, wenn alle möglichen Tests mit „PASS“ quittiert wurden. Weiterhin soll festgestellt werden, für welche Schnittstellen der Schreibschutz angeboten wird. Dieser Eintrag dient lediglich der Information und soll keinen weiteren Einfluss auf die Bewertung des WriteBlockers haben.

3.2 Beurteilung der Handhabung (DIN EN ISO 9241)

Als zweites Bewertungskriterium soll die Handhabung des WriteBlockers durch den Nutzer betrachtet werden. Dabei wurde sich an den Vorgaben der DIN EN ISO 9241 (5) orientiert. In dieser Norm werden Kriterien zur „Ergonomie der Mensch-System-Interaktion“ festgelegt. In Teil 110 der Norm werden Interaktionsprinzipien festgelegt. Diese lauten:

- Aufgabenangemessenheit
- Selbstbeschreibungsfähigkeit
- Erlernbarkeit
- Steuerbarkeit
- Robustheit gegen Benutzerfehler
- Benutzerbindung

Im Rahmen der Projektarbeit sollen sowohl Hardware- als auch Software-WriteBlocker beurteilt werden. Um diesen Umstand über ein einheitliches Bewertungssystem zu berücksichtigen, wurden die folgenden Kriterien des Katalogs für die Beurteilung herangezogen:

- **Aufgabenangemessenheit**: Über den WriteBlocker lässt sich ein effektiver Schreibschutz einrichten und das geschützte Medium betrachten. Es ist möglich, das schreibgeschützte Medium physikalisch zu sichern. Unnötige Interaktionen bei der Einrichtung des Schreibschutzes werden vermieden.

- **Selbstbeschreibungsfähigkeit**: Für den Nutzer ist verständlich und erkennbar, welche Handlungen nötig sind um den Schreibschutz zu aktivieren. Der WriteBlocker gibt Rückmeldung, in welchem Zustand er und das angeschlossene Medium sich befinden.

- **Robustheit gegen Benutzerfehler**: Der WriteBlocker weist den Nutzer darauf hin, wenn eine Handlung zu einem möglichen Schreibzugriff auf das Medium führt. Eine fehlerhafte Eingabe / Nutzung lässt sich korrigieren, bevor es zu Schreibzugriffen kommt.

Je nachdem, wie umfänglich diese Kriterien durch den WriteBlocker erfüllt werden, erfolgt eine Zuordnung gemäß den Abstufungen: „voll erfüllt“ (2 Punkte), „teilweise erfüllt“ (1 Punkt) und „nicht erfüllt“ (0 Punkte).

Weiter erfolgt eine Gewichtung der Kriterien. Die Aufgabenangemessenheit wird mit 50% gewichtet, die Selbstbeschreibungsfähigkeit und Robustheit gegen Benutzerfehler mit je 25%. Werden volle zwei Punkte in allen Kriterien erreicht, wird die Handhabung mit 100% beurteilt. Eine Vergabe von einem Punkt führt bei der Aufgabenangemessenheit zu einer Halbierung der möglichen 50% auf 25% und bei den weiteren Kategorien zu einem Beitrag von 13% (gerundet). Die Vergabe von 0 Punkten führt bei allen Kriterien zu einem Beitrag von 0% zur Handhabungs-gesamtbewertung. Die für die einzelnen Writeblocker angefertigten Bewertungen sind dem Anhang zu entnehmen.

3.3 Sicherungszeiten

Aufgrund der unterschiedlichen Testsysteme der Teilnehmer der Projektgruppe lässt sich eine absolute Vergleichbarkeit der Sicherungszeiten nicht erreichen. Auch handelte es sich zwar um typidentische Sicherungsmedien, diese können sich jedoch durch Alterung und Serienstreuung im Datendurchsatz unterscheiden. Die Angabe der Sicherungszeiten lässt dennoch Rückschlüsse auf den Beitrag des WriteBlockers zur Gesamtzeit der Sicherung zu. Einen großen Einfluss hat hierbei die verwendete USB-Version. Es wird ein Ranking der Sicherungszeiten erstellt. Dieses hat jedoch einen rein informativen Charakter und soll erhebliche Abweichungen von erwartbaren Sicherungszeiten aufzeigen.

3.4 Darstellung der Bewertungskriterien

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	PASS	FAIL	
Schutz gegen Formatierung / Partitionierung	PASS	FAIL	
Schutz gegen Operationen auf Blockebene / Hexedit	PASS	FAIL	
Verifikation über CRU CFTT Tool	PASS	FAIL	nicht mgl.
Ergänzende Hinweise zum Schreibschutz	Besonderheiten, die die Art des Schreibschutzes betreffen.		

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit	50%	25%	0%	Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	25%	13%	0%	Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	25%	13%	0%	Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung				
Bewertung Handhabung:	0 - 100%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT		
Seagate ST500DM002_1		
Imation Nano 2GB		
Emtec USB 2.0 Stick 8GB		
Sandisk Ultra 32GB		

4 Durchführung der Testszenarien

Auf Grundlage der zuvor angefertigten Medien und festgelegten Gütekriterien wird im Folgenden Hard- und Software-Wirte-Blocker getestet. Zur Vergleichbarkeit wurde unter den Projektteilnehmern ein einheitlicher Testablauf abbestimmt. Nach der jeweiligen Einrichtung des Write-Blockers wird das präparierte Medium angeschlossen und versucht, schreibend auf das Medium zuzugreifen. Hierfür werden

- Dateioperationen wie Löschen/Verschieben/Bearbeiten,
- das Formatieren der Partition
- sowie das Bearbeiten von Bytes mit einem Hex-Editor ausprobiert.

Anschließend erfolgt die Sicherung des Mediums, dessen Ergebnis im besten Fall mit dem identischen Hashwert zur in Kapitel 2.3 ursprünglich erstellten Version übereinstimmt. Daraus ließe sich ableiten, dass die zuvor ausprobierten Dateizugriffe keinen Erfolg hatten und das Medium unverändert zum Ausgangszustand blieb. Sollte sich der Hashwert nach der Sicherung geändert haben, ist davon auszugehen, dass der jeweils im Test befindliche Write-Blocker einen schreibenden Zugriff nicht unterbunden hatte.

Anhand der auf einer Festplatte während der initialen Sicherung gespeicherten Backup-Images muss im Fall von vollzognenen Schreibzugriffen der Datenträger wieder zurück auf den Ursprungszustand gebracht werden, um für Tests anderer Write-Blocker zu dienen. Exemplarisch wird dieses Szenario für jedes Write-Block-Verfahren an eines der insgesamt fünf vorliegenden Speichermedien angewandt.

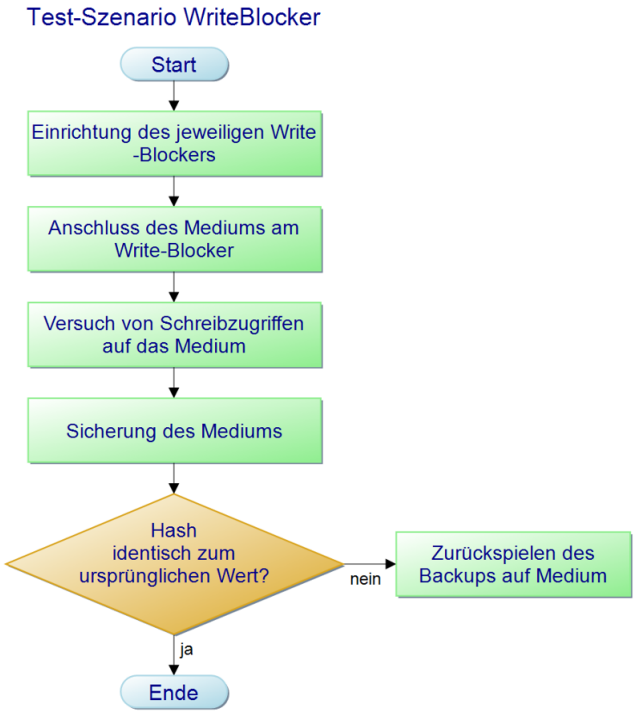

Bild 3: Flowchart zum Testablauf

Zur Bemessung der Performance/Geschwindigkeit und zum Ausschluss von Ausreißern während des Sicherungsprozesses wird ferner jedes Speichermedium dreifach hintereinander gesichert und die Zeitdauer anhand der drei vorgenommenen Sicherungen gemittelt.

Zur abschließenden Bewertung des jeweiligen Write-Blockers wird auf die Erkenntnisse des Computer Forensics Tool Testing Program (CFTT) zurückgegriffen. Das CFTT ist eine Projektgruppe beim National Institute for Standards and Technology (NIST) und beschäftigt sich seit Jahrzehnten mit der Validierung von forensischer Soft- und Hardware (6) durch universell gültige Tests in diesem Bereich. In der Spezifikation von Tools zur Verifikation von Write-Blockern nennt das CFTT folgenden, essentielle Voraussetzungen (7):

- Das Tool darf ein geschütztes Medium nicht erlauben, sich zu verändern
- Das Tool darf das Abrufen von Informationen zu einem Medium (beispielsweise Seriennummer o.ä.) nicht unterbinden
- Das Tool darf keine Operationen unterbinden bei einem Medium, das nicht geschützt ist

Das CFTT veröffentlicht auf seiner Internetpräsenz Test Reports von Write Blockern. Zur Überprüfung von Writeblockern in Windows-Umgebungen nutzt das CFTT das Programm CRU WriteBlocking Validation Utility (8). Das von CRU entwickelte Tool versucht, automatisiert eine Bandbreite von WRITE-Commands auf dem vom Write-Blocker geschützten Speichermedium abzusetzen und vergleicht daraufhin die betroffenen Speicherbereiche. Es testet ferner die zuvor aufgelisteten essentiellen Vorraussetzungen. Als Ergebnis des Tests wird eine PASS/FAIL-Meldung generiert, wodurch die Zuverlässigkeit des zu überprüfenden Write-Blockers bewertet wird. Eine Linux-Version dieses Tools ist noch nicht verfügbar. (9)

4.1 Hardware-Writeblocker

Als Hostsystem wurde hier ein Lenovo Thinkpad T440p mit folgender Ausstattung verwendet:

CPU:	Intel® Core™ i7-4712MQ
RAM:	16GB DDR3
SSD:	Sandisk SDSSDH3 512GB (Manjaro KDE 21.2.6)
	Transcend TS512GMTS430S (Windows 11)
	Samsung SSD 850 EVO 1TB (für durchgeführte Sicherungen)

Das System besitzt insgesamt 4 USB-Schnittstellen. (2x USB 3.0, 2x USB 2.0). Zur Testdurchführung werden die USB 3.0 Schnittstellen verwendet.

Sofern möglich, wird Manjaro KDE 21.2.6 für die Testdurchführung genutzt. Falls erforderlich, kann auf Windows 11 oder ein Live System ausgewichen werden.

Als Ausweichsystem steht ein Thinkpad T440 mit Manjaro XFCE 21.2.6 zur Verfügung.

Es sollen zunächst folgende Open-Source-Ansätze getestet werden:

- DIY USB Writeblocker (Entsprechend einer Anleitung auf instructables.com) (10) auf Basis des FTDI V2DIP1-32 Entwicklerboards
- Firebrick3 (11) auf Basis des ASRock E350M1 Mainboards
- UDeck (12) auf Basis des Einplatinenrechners Beaglebone Black
- 4Deck Magic USB-Hub (13) unter Verwendung eines USB-Hubs und angepasster Udev Regeln

Anschließend werden die folgenden „Low-Cost“ Adapter mit Schreibschutz-Funktion betrachtet:

- Sharkoon DriveLink Combo USB 3.0 V2 (SATA / IDE > USB 3.0 Brücke mit getrennten Schreibschutz-Schaltern für SATA und IDE)
- Delock 62652 SATA / USB Converter mit Schreibschutz-Jumper

Zuletzt sollen marktübliche WriteBlocker mit forensischem Anspruch zum Vergleich herangezogen werden. Es stehen zur Verfügung:

- WiebeTech USB 3.1 WriteBlocker
- Tableau T3iu Forensic SATA Imaging Bay
- WiebeTech Forensic Ultradock V5

4.1.1 Selbstbau USB-Writeblocker

Als kostengünstige Möglichkeit, einen Schreibschutz für Datenträger bereitzustellen, welche über USB angebunden werden, konnte der USB-Writeblocker nach Dr. Philip Polstra, Professor an der Bloomsburg University of Pennsylvania auf dessen Github-Repository vorgefunden werden. (14)

Bild 4: Selbstbau Writeblocker

Dieses Gerät basiert auf dem V2DIP1-32 Entwicklerboard von FTDI und dem von Dr. Postra bereitgestellten Quellcode. Für eine alltagstaugliche Verwendungsmöglichkeit wurde zudem ein Kunststoffgehäuse und eine Zugentlastung für das USB-Slave-Kabel verwendet. Das Beschreiben des Flash-Speichers erfordert zudem das VII-Debugger-Modul, um einen Zugriff über die USB-Schnittstelle zu gewährleisten.

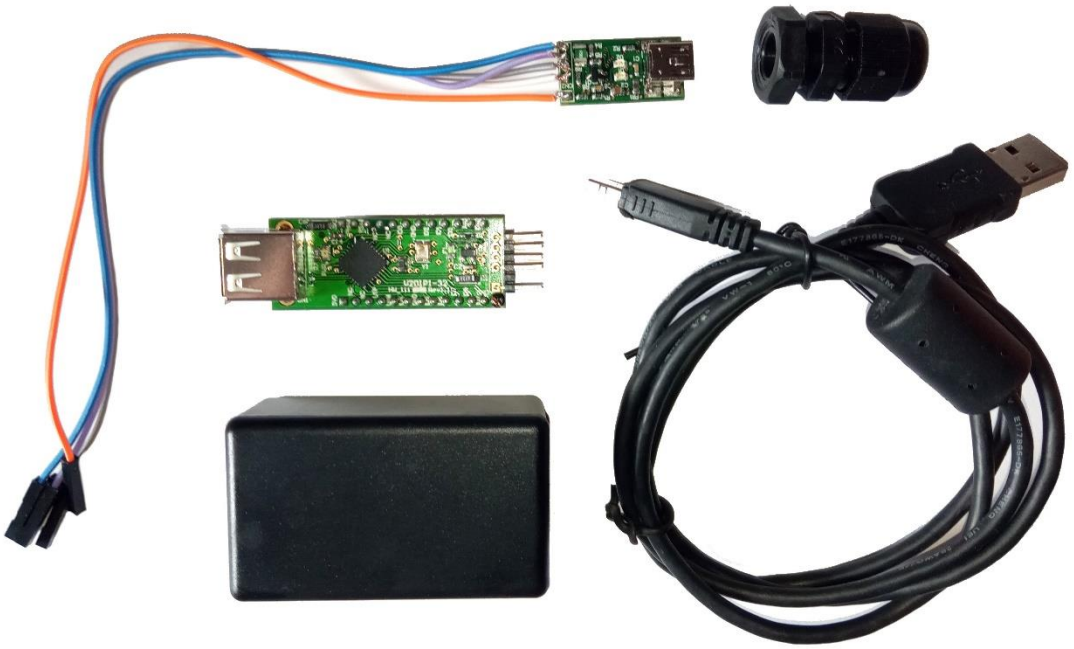

Bild 5: Verwendete Komponenten für den Bau des Writeblockers: Debug-Modul (ergänzt um angelötete Jumperkabel), Zugentlastung, V2DIP1-32, USB-Kabel, Kunststoffgehäuse

Zum Kompilieren des Quellcodes wird die Vinculum II IDE des Herstellers FTDI verwendet. Laut Polstra ist es hierbei von entscheidender Bedeutung die Version 1.4.4 zu verwenden. Mit neueren Versionen entstünden Fehler bei der Kompilierung.

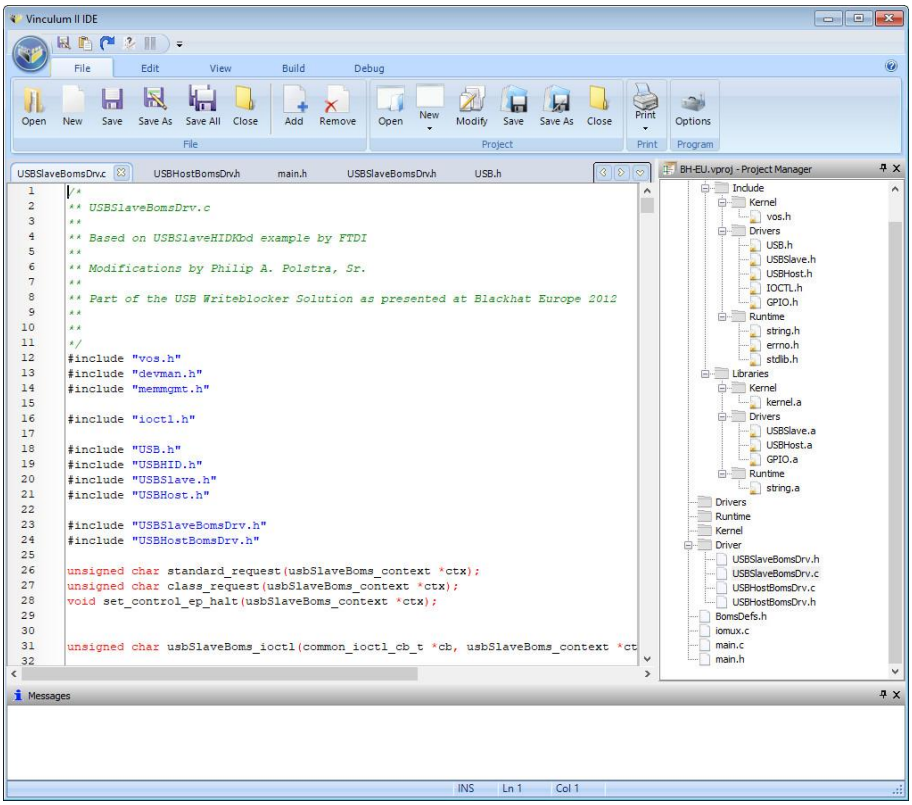

Bild 6: Vinculum II IDE mit geladenem Writeblocker-Projekt

Über die IDE lässt sich der Chip nach der Kompilierung der Rom-Datei auch beschreiben. (Reiter „Debug“). Alternativ kann die Rom-Datei auch über das Tool FTProg (ebenfalls von FTDI) geflasht werden.

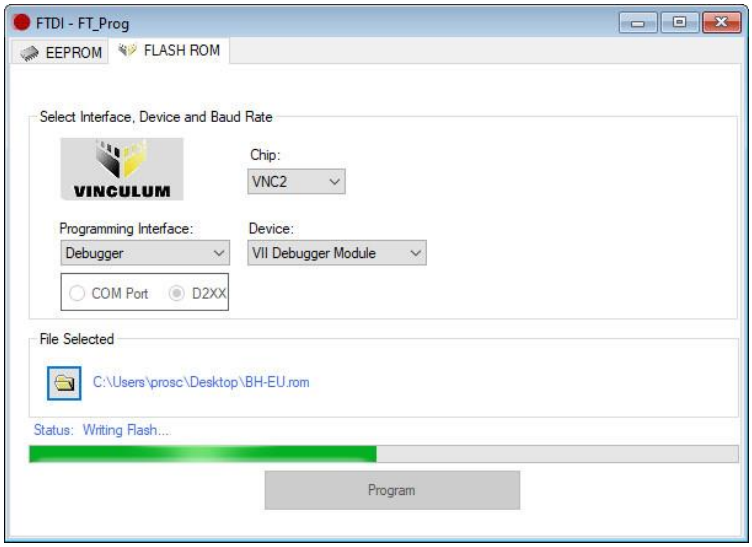

Bild 7: FTProg beim Flashen des Chips

Um einen Zugriff auf das verwendete Debugger Modul zu erhalten, mussten dessen Treiber manuell installiert werden. Dabei genügte es nicht, den Treiber-Installer der FTDI-Website zu verwenden. Unter Windows 10 war es erforderlich, die automatische Treiberinstallation zu deaktivieren und den heruntergeladenen Treiber händisch zu installieren.

Nach dem Flash konnte der USB-Slave-Anschluss angelegt werden. Dazu wurde ein USB-Kabel (eines älteren Kameramodells) aufgetrennt und die einzelnen Adern mit Pin-Verbindern bestückt um einen Anschluss direkt an die Portleiste des V2DIP1-32-Moduls zu ermöglichen.

In seinem Instructables-Beitrag (10) zu dem Projekt erläutert Polstra auch die Pinbelegung für den Anschluss des aufgetrennten USB-Kabels: **rot = 5V+, grün = USB-D+, weiß = USB-D-, schwarz = GND**. Auf die entsprechenden Pins des FTDI-Boards werden diese Adern aufgelegt. Abweichend von Polstra wurden für dieses Projekt die Adern nicht am Board verlötet, sondern angelötete Pinverbinder mit den entsprechenden GPIO-Pins des Boards verbunden.

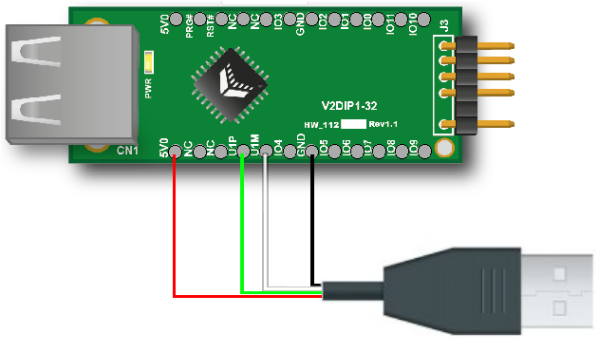

Bild 8: Auflegeplan der USB-Slave-Verbindung (© des Originalbildes der Platine: FTDI, © USB-Stecker: Reichelt-Elektonik)

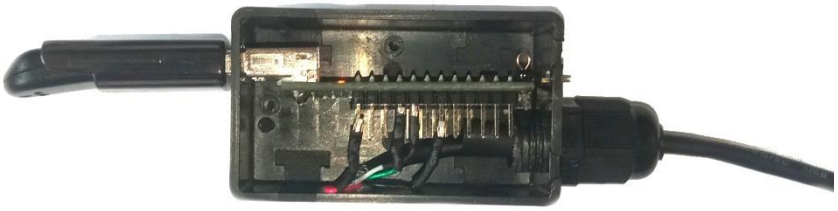

Bild 9: Board mit installierter USB-Verbindung, Gehäuse und Zugentlastung

Nach der Fertigung der erforderlichen Öffnungen am Gehäuse, der Verkabelung der Platine und der Anbringung der Zugentlastung, wurde die Platine selbst mittels Heißkleber im Gehäuse fixiert. Die Pin-Verbinder für das Debugging-Modul sind über eine Öffnung weiter erreichbar.

Bild 10: Einsatz des Writeblockers im Versuchsaufbau

Um die Funktionalität des Writeblockers zu testen, wurde ein USB-Stick zunächst direkt an das System angeschlossen. Dabei zeigte er die folgenden Eigenschaften:

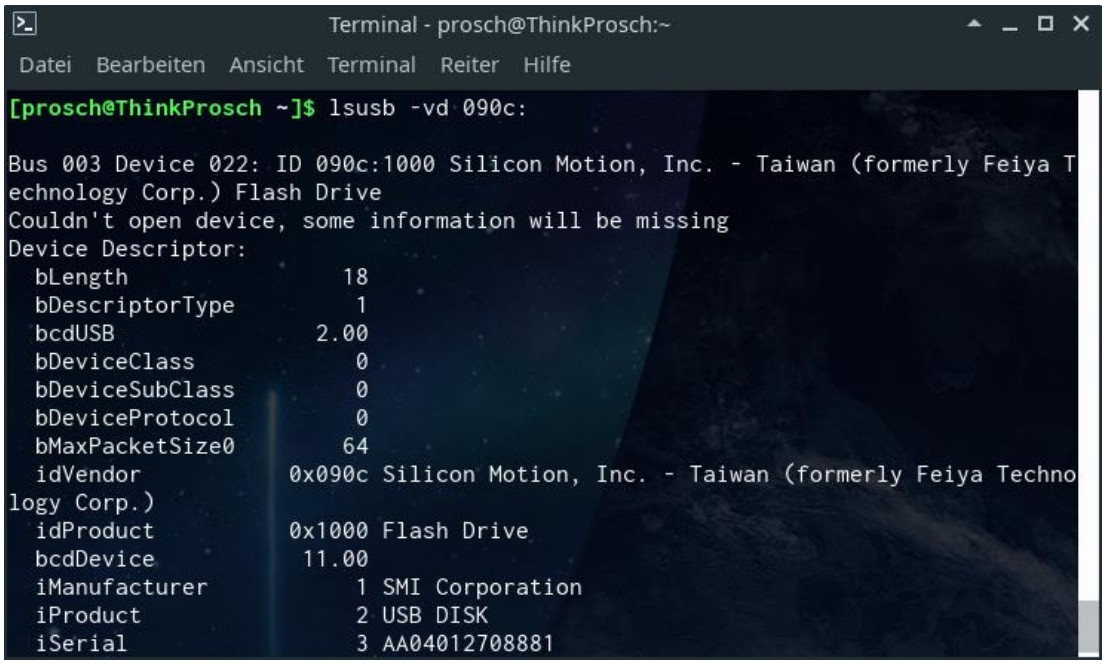

Bild 11: Ausgabe mit Informationen zum verwendeten USB-Stick

An den Writeblocker angeschlossen, wird dieser Stick unter der genannten VID/PID nicht mehr angezeigt. Stattdessen wird die VID/PID des Writeblockers angezeigt, wie sie auch im Quellcode festgelegt wurde:

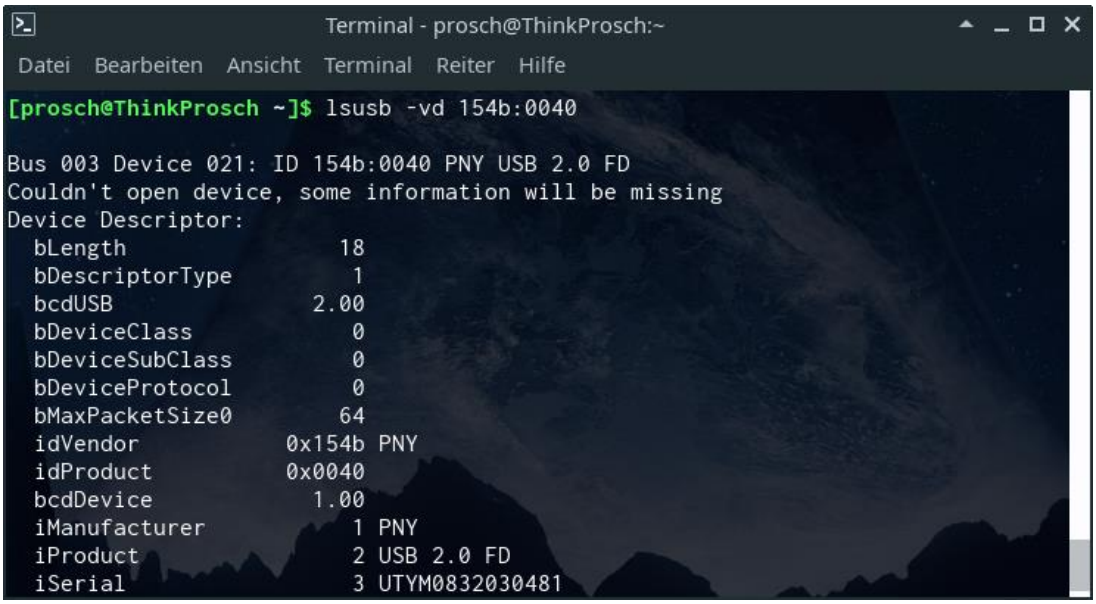

Bild 12: Ausgabe bei Anschluss über den Writeblocker

Es ist ersichtlich, dass bei Verwendung des Writeblockers USB-Geräte an das System angeschlossen werden können, ohne dass deren VID/PID und Seriennummer an das System übermittelt werden. In beiden Fällen wurde aber die UUID korrekt ausgegeben:

Bild 13: Ausgabe der UUID und PARTUUID unabhängig von der Verwendung des Writeblockers

4.1.1.1 Testablauf

Der Test wurde unter Manjaro Linux KDE 21.2.6 durchgeführt. Das Testmedium Imation USB-Stick (USB 2.0) wurde zunächst an den Write-Blocker angeschlossen. Erst mit gestecktem Medium wurde der Write-Blocker selbst per USB mit dem Host-System verbunden.

Eine Verbindung konnte zunächst nicht beobachtet werden. Erst nach vier Versuchen und einer Wartezeit von ca. 40 Sekunden wurde der USB-Stick im System ausgewiesen. Die Darstellung der Verzeichnisstruktur im Dateimanager Dolphin erfolgte ebenfalls erst nach einer Wartezeit von ca. 40 Sekunden.

4.1.1.2 Dateioperationen:

Es wurde versucht, eine Datei (docx.zip) auf den Datenträger zu kopieren und einen Ordner vom Datenträger zu löschen (Ordner 015).

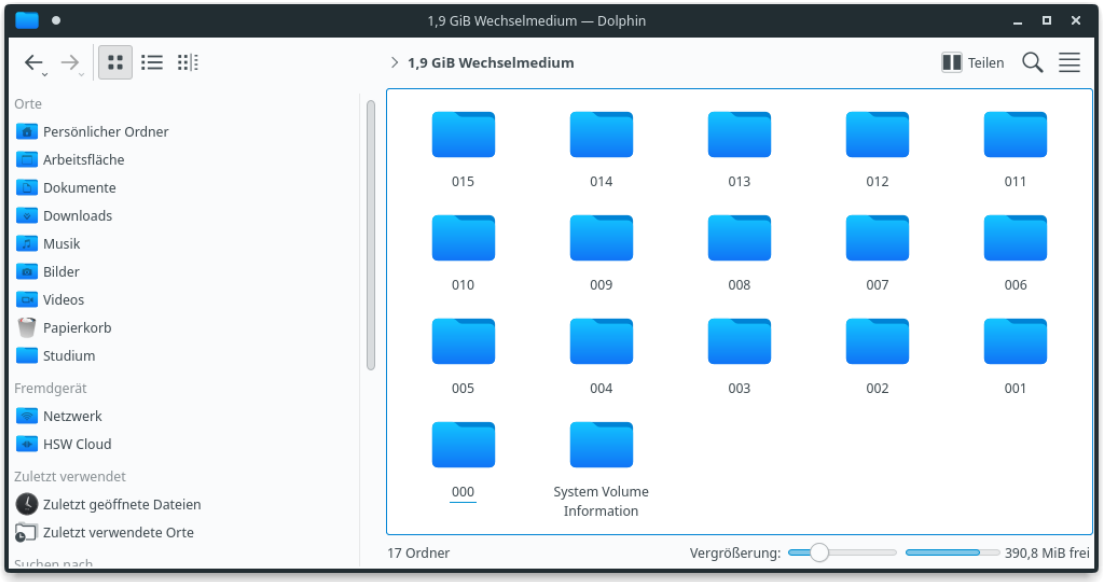

Bild 14: Ordneransicht vor der Durchführung der Dateioperationen

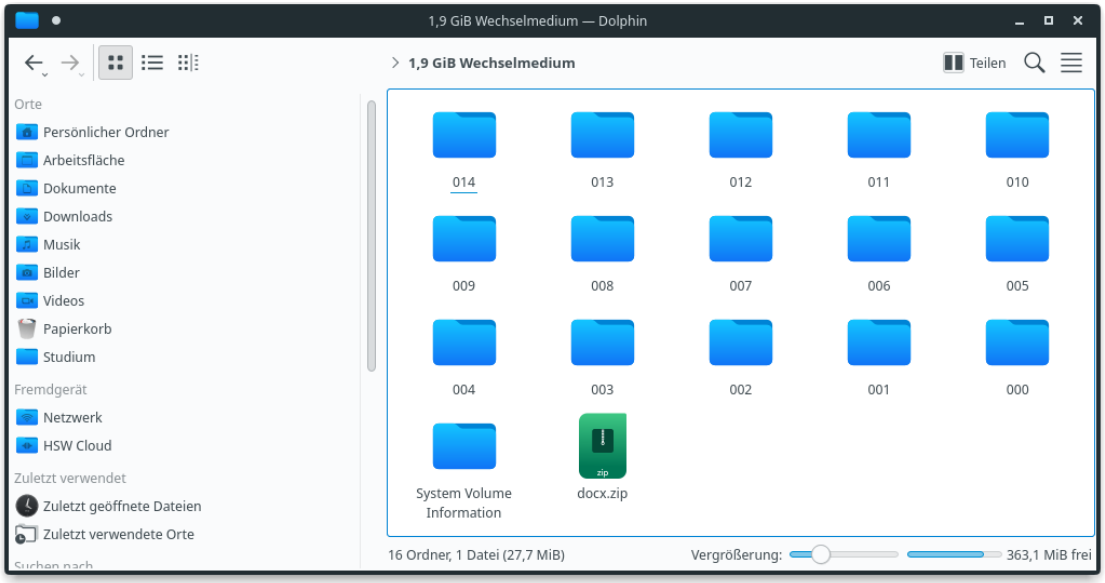

Bild 15: Ordneransicht vor nach Durchführung der Dateioperationen

Augenscheinlich wurden beide Dateioperationen ausgeführt. Anschließend wurde über den FTKImager eine Sicherung des Datenträgers auf Blockebene erstellt:

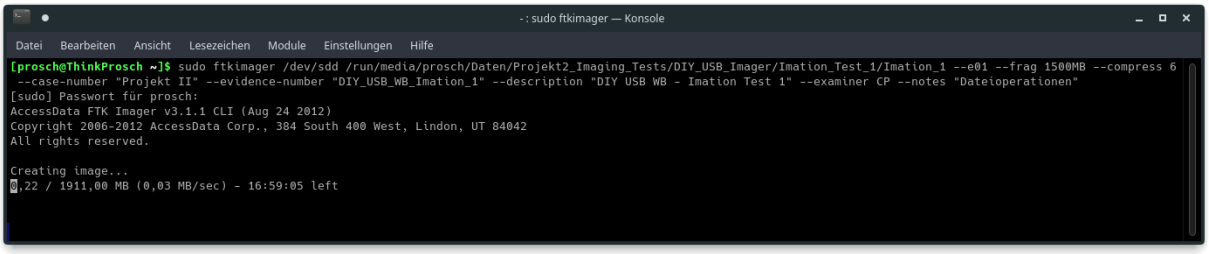

Bild 16: Sicherung des Datenträgers über den DIY USB Write-Blocker

Diese Sicherung war nach 11 Stunden 54 Minuten und 28 Sekunden abgeschlossen und wies folgende Hash-Werte auf:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

Es ist erkennbar, dass trotz der vermeintlich erfolgreichen Dateioperationen keine Veränderung am Medium stattgefunden hat.

4.1.1.3 Formatierung / Partitionierung:

Über die Software GParted wurde eine Neuformatierung des Datenträgers mit dem Dateisystem FAT32 angestoßen:

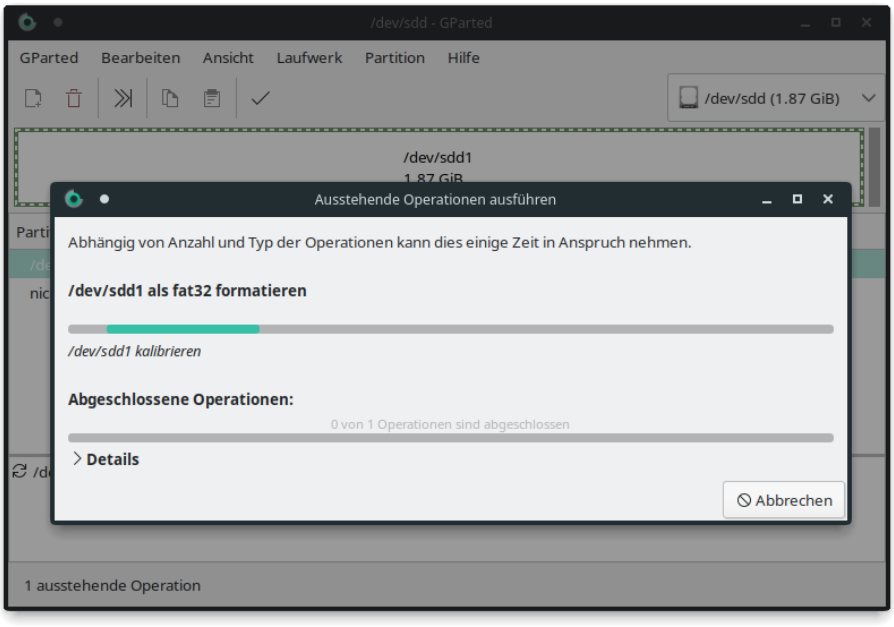

Bild 17: Durchführung der Formatierung ohne Fehlermeldung

Auch die Formatierung wurde augenscheinlich erfolgreich durchgeführt. Nach dem erneuten Einlesen des Datenträgers wies Gparted jedoch wieder den vorherigen Füllstand der Partition aus.

Eine weitere Sicherung des Datenträgers war nach 11 Stunden 46 Minuten und 17 Sekunden abgeschlossen und wies folgende Hash-Werte auf:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

Erneut wurden keine Veränderungen am Datenträger verursacht.

4.1.1.4 Operationen auf Blockebene / Hexedit:

Über die Software Hexedit (http://rigaux.org/hexedit.html) wurde am Datenträger ein Bit von 0 auf 1 gesetzt (00 zu 10) und die Veränderung gespeichert.

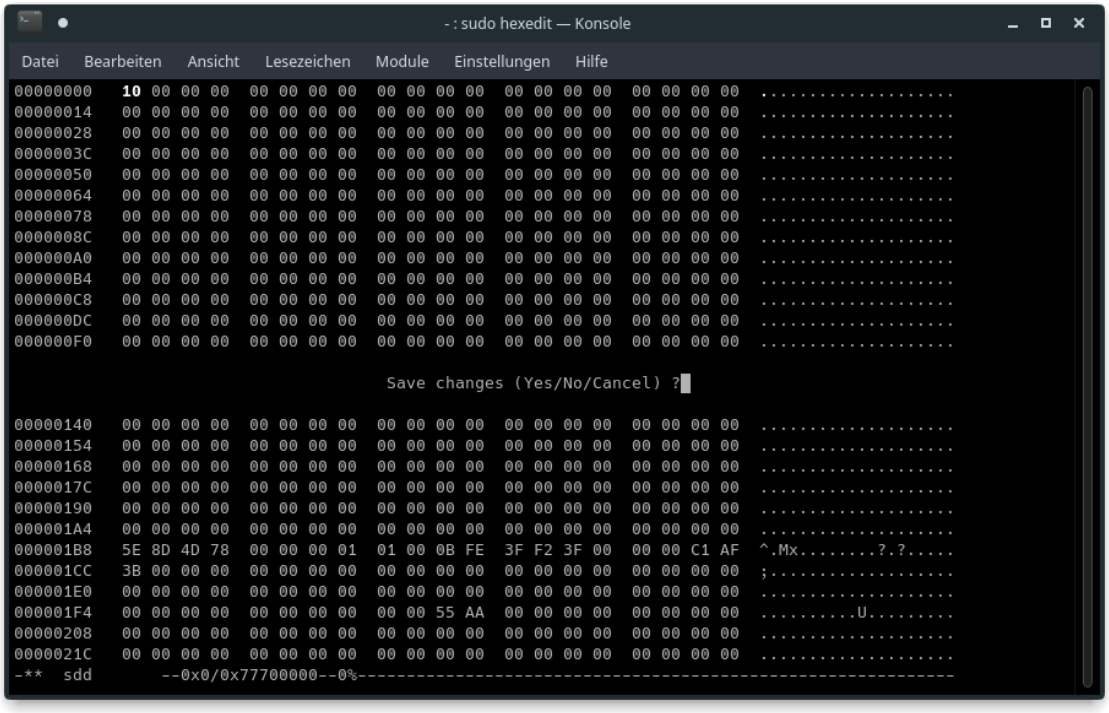

Bild 18: Hexedit – Speicherung der Veränderungen ohne Fehlermeldung

Auch bei der Speicherung der Änderungen wurde keine Fehlermeldung ausgegeben. Ein erneuter Aufruf des Hexeditors zeigte jedoch wieder den ursprünglichen Zustand

(00). Die abschließende Sicherung des Mediums war nach 11 Stunden 46 Minuten und 43 Sekunden abgeschlossen und wies die folgenden Hash-Werte auf:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

Eine Veränderung des Datenträgers fand in keinem der durchgeführten Tests statt.

4.1.1.5 Sicherung weiterer Medien / Ergebnisse

Es wurde versucht, auch die weiteren Testmedien über den Selbstbau-Writeblocker zu sichern. Jedoch konnte im Weiteren nur zu dem Datenträger USB 2.0 Stick Emtec 8GB eine Verbindung über das Gerät hergestellt werden.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Imation Nano 2GB	Sicherung 1:	11:54:28
	Sicherung 2:	11:46:17
	Sicherung 3:	11:46:43
	Durchschnitt:	11:49:09
Emtec USB 2.0 Stick 8GB	Sicherung 1:	44:22:16
	Sicherung 2:	44:10:51
	Sicherung 3:	43:52:40
	Durchschnitt:	44:08:36
Sandisk Ultra 32GB	Sicherung 1:	keine Verbindung
Western Digital WD500BPVT	Sicherung 1:	keine Verbindung
Seagate ST500DM002_1	Sicherung 1:	keine Verbindung

Eine Abschließende Überprüfung des Write Blockers mit der Write Blocking Validation Utility von CRU unter Windows 11 brachte keine verwertbaren Ergebnisse, da die Zeitlimits der jeweiligen Tests überschritten wurden.

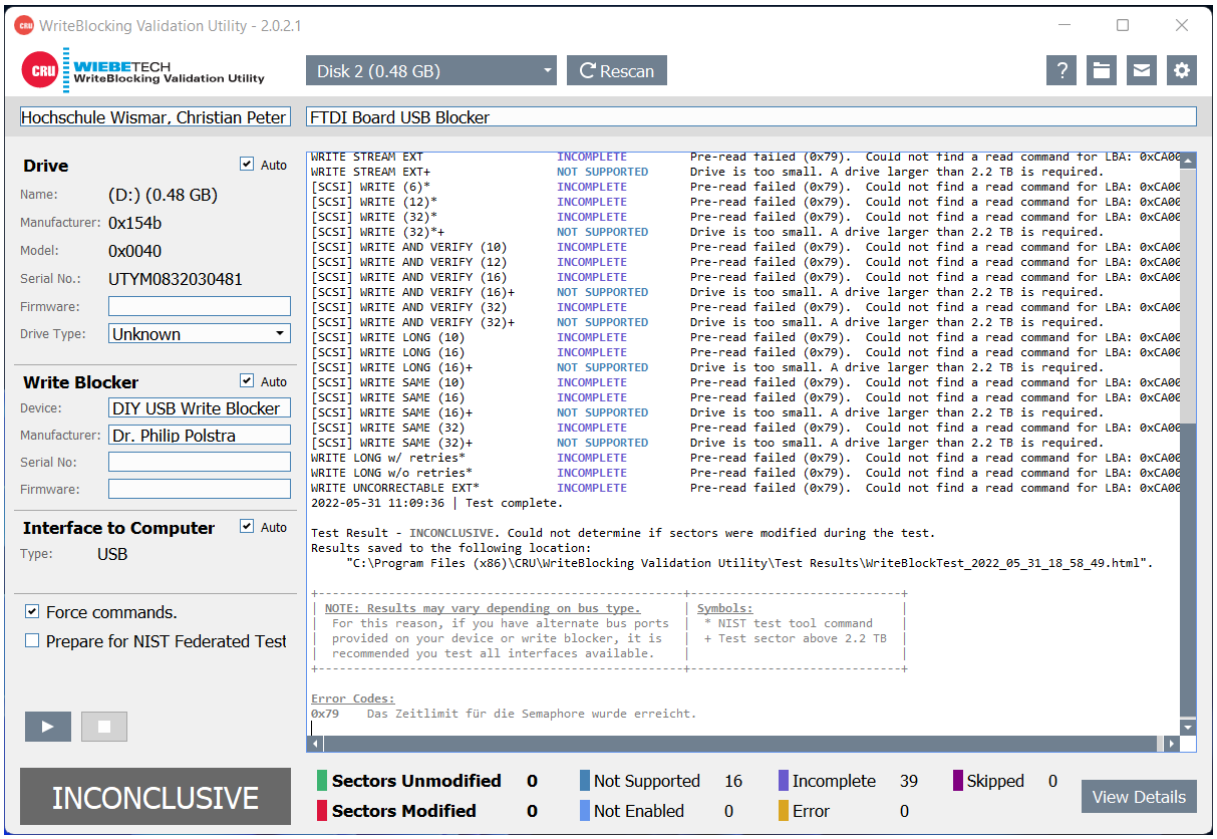

Bild 19: DIY WriteBlocker – Ausgabe des CRU NIST Test Tools

4.1.2 Firebrick3

Der Firebrickk3 Write-Blocker für SATA-Festplatten basiert auf dem MiniITX-Mainboard ASRock E350M1 und einem darauf abgestimmten Mini-Linux.

Bild 20: Firebrick3 im Einsatz

Entwickler Lee Tobin stellte im Jahr 2013 seine erste Version des Firebrick vor. Diese Version des Geräts konnte über eine angeschlossene Tastatur und ein verbautes LCD2USB-Display bedient werden und verstand sich als Imaging Device. Eine Write-Block Funktionalität wurde über Firewire bereitgestellt. Auf diesem Wege wurden auch Images, welche über das Gerät erzeugt wurden vom Gerätespeicher geladen.

Die Firewire-Schnittstelle hat in den vergangenen Jahren stark an Bedeutung verloren und findet sich kaum mehr an neu verkauften PCs und Laptops.

Um eine alternative Form des Datenaustauschs zwischen Firebrick und Host-PC zu etablieren, erstellte Tobin das Projekt Firebrick3, das die RJ45 Netzwerkbuchse des Mainboards für den Datenaustausch verwendet.

Der Codes des Projektes konnte über Github bezogen werden: https://github.com/leetobin/firebrick3. Im Gegensatz zum „Legacy"-Projekt, wie der ursprüngliche Firebrick nun genannt wird, existiert auf dem Repository aktuell kein vorkompiliertes bzimage. Es findet sich jedoch im Wiki des Projekts eine Anleitung zur Kompilierung.

Versuche, das bzimage unter Manjaro Linux 21.1 zu kompilieren, schlugen fehl. Daher wurde über Virtualbox Ubuntu 16.04 als VM installiert, das Repository per git-Befehl geklont und das Make-Script (start.sh) fehlerfrei ausgeführt. Das so erstellte bzimage-File konnte über einen geteilten Ordner auf das Host-System übertragen werden.

Im Anschluss konnte ein bootfähiger USB-Stick über Syslinux erstellt werden.

```
[prosch@christian-20b7s2qn02 ~]$ syslinux --mbr --active --directory / --install /dev/sdc1
```

Das erzeugte bzimage-File wurde im Stammverzeichnis des USB-Sticks abgelegt. Außerdem wurde eine SYSLINUX.CFG mit dem folgenden Inhalt erstellt:

SYSLINUX.CFG:

```
default firebrick
label firebrick
      linux /bzImage
```

Neben dem ASRock E350M1 Mainboard, wurden für den Bau des Firebricks weiterhin benötigt: ein passendes MiniITX-Gehäuse samt Netzteil, SATA-Daten- und Power-Kabel, ein DDR3-Desktop RAM-Riegel (hier 2GB Kingston HyperX DDR3-1600)

Bild 21: ASRock E350M1

Im Wiki des Legacy-Firebricks wird auf eine detaillierte Aufbauanleitung des Firebricks verwiesen: http://digitalfire.ucd.ie/?page_id=1011. In dieser Anleitung wird der Anschluss des Quellmediums über den dritten SATA-Port beschrieben. Über diesen Port wurde zunächst jedoch keine Verbindung zum Quellmedium hergestellt. Ein Anschluss über den ersten SATA-Port ermöglichte hingegen den schreibgeschützten Zugriff auf eine angeschlossene Festplatte. Es ist anzunehmen, dass diesbezügliche Änderungen im Aufbau des Projekts bisher nicht dokumentiert wurden.

Nach dem Zusammenbau des Firebrick wurde über dessen BIOS die Boot-Priorität für den USB-Boot festgelegt. So wird bei gestecktem USB-Stick direkt das erstellte FirebrickOS geladen. Es wurde weiterhin der Versuch unternommen, entsprechend der Anleitung im Legacy-Firebrick Projekt ein Coreboot-Image zu erzeugen und dieses mittels eines CH341A-Programmers direkt auf den BIOS-Chip des Mainboards zu schreiben, jedoch war das Gerät nach dem Start nicht ansprechbar. Daher wurde für den Versuchsaufbau der USB-Boot-Stick verwendet.

Eine Verbindung zum Firebrick vom Host-System aus konnte über ein RJ45-Ethernetkabel aufgebaut werden. Dabei erhält das Hostsystem vom Firebrick via DHCP eine Netzwerkadresse. Das Webinterface des Firebrick ist anschließend über die Adresse: 192.168.0.1 abrufbar.

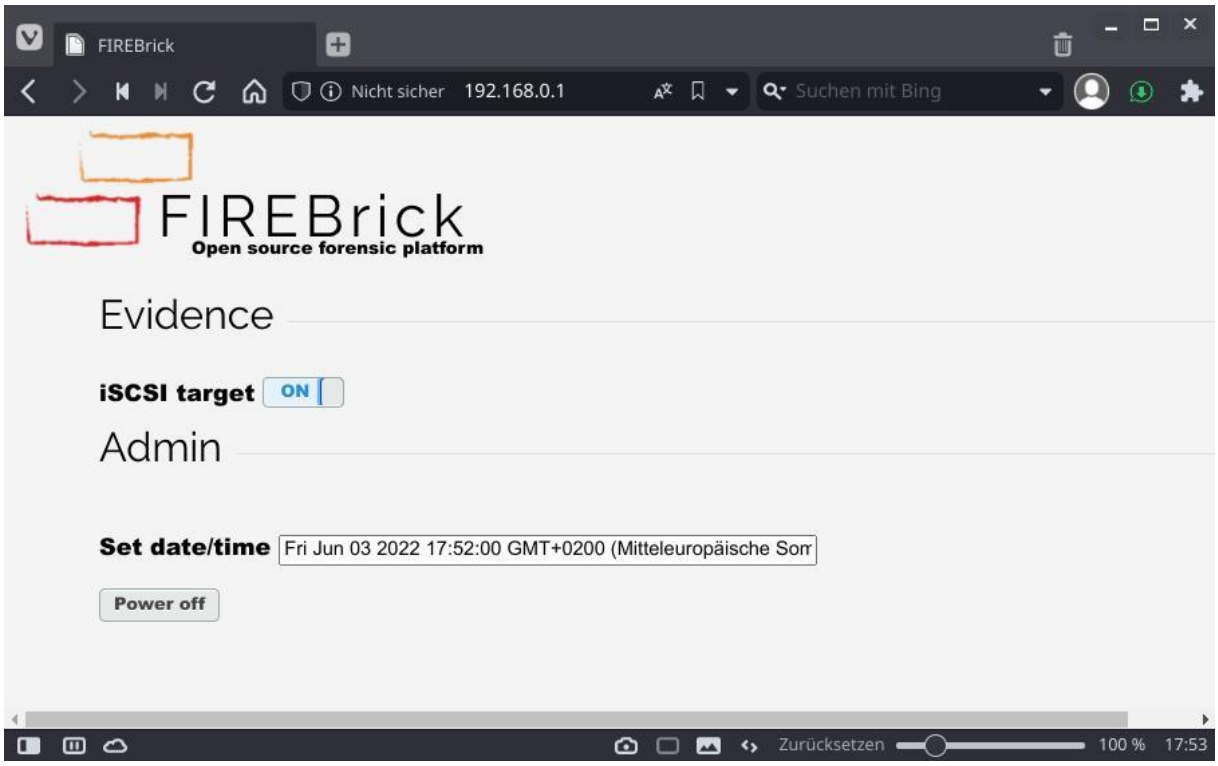

Bild 22: Webinterface des Firebrick3

Über den Button „iSCSI target“ wird der Beweisdatenträger als iSCSI Gerät zur Verfügung gestellt.

Eine Verbindung des Systems mit der am Firebrick angeschlossenen Festplatte konnte unter Linux über Open-ISCSI hergestellt werden.

Bild 23: Zugriff auf den iSCSI Speicher des Firebrick3

4.1.2.1 Testablauf

Das Testmedium Western Digital WD500BPVT wurde an den Firebrick angeschlossen und zusammen gestartet. Nach erfolgter Verbindung zum iSCSI Device über die

Hostmaschine (Manjaro XFCE 21.2.6), konnten die Dateien auf der Festplatte über den Dateimanager Dolphin betrachtet werden.

4.1.2.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen, wurden mit einer Fehlermeldung quittiert:

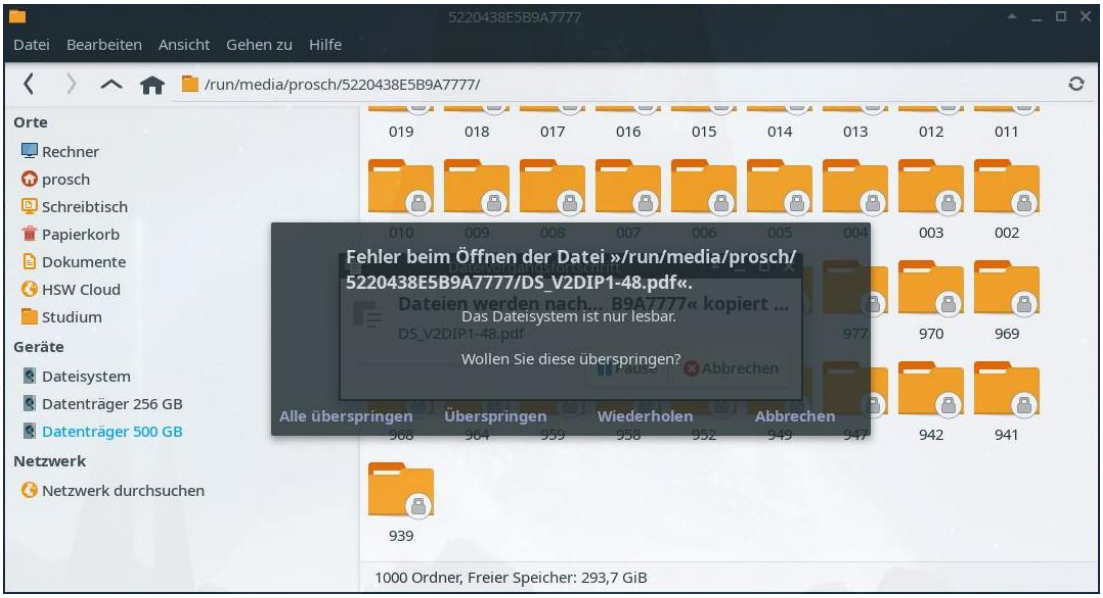

Bild 24: Firebrick3 - Ausgabe eines Fehlers beim Versuch, eine Datei abzulegen

Das Löschen von Dateien wird über den Systemdialog nicht angeboten. Entsprechende Menüpunkte werden dabei ausgegraut. Auch Löschversuche über Tastaturbefehle führen zu keiner Reaktion.

Die erste Sicherung des Datenträgers über den FTKImager ergab dabei nach 1:54:09 Stunden die Hashwerte:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

4.1.2.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im NTFS-Format neu zu formatieren. Dabei wurde eine Fehlermeldung ausgegeben, wonach ein Schreibzugriff auf das Medium nicht möglich sei:

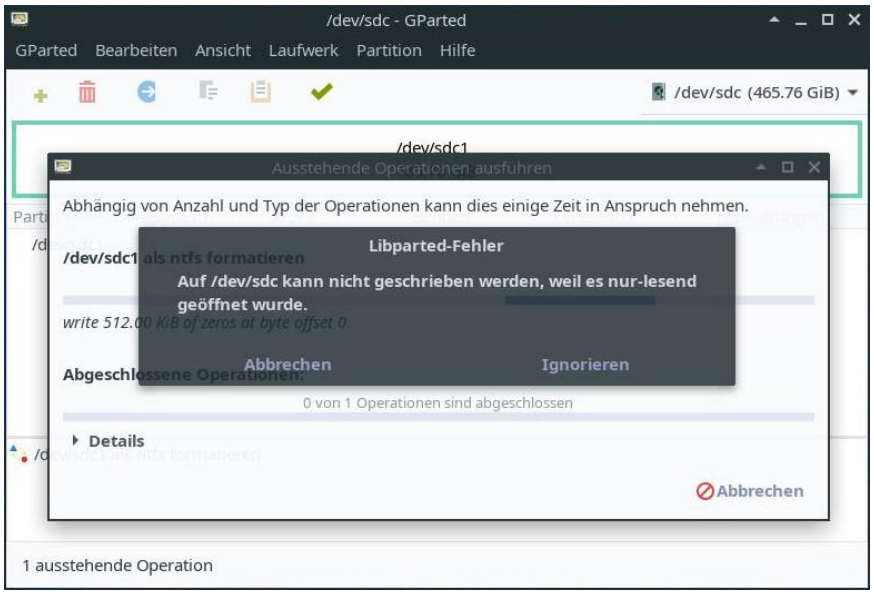

Bild 25: Firebrick3 - Ausgabe eines Fehlers beim Versuch der Formatierung

Die zweite Sicherung des Datenträgers war nach 1:54:00 Stunden abgeschlossen. Es wurden die folgenden Hash-Werte generiert:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

4.1.2.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium durchzuführen, werden mit dem Hinweis blockiert, dass es sich um ein read-only Device handelt:

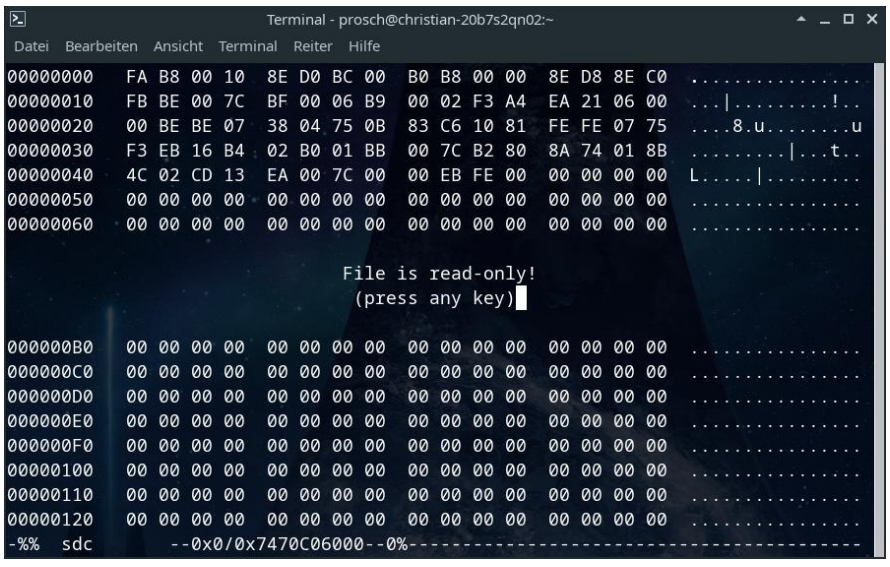

Bild 26: Firebrick3 - Ausgabe eines Fehlers im Hexeditor

Die letzte Sicherung des Mediums ergab dabei die Hash-Werte:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger fand im Rahmen der durchgeführten Tests nicht statt.

4.1.2.5 Sicherung weiterer Medien / Ergebnisse

Da der Schreibschutz des Firebricks nur für die SATA-Schnittstelle bereitgestellt wird, wurden nur die Test-Festplatten gesichert. Eine Anpassung des Systems und eine Erweiterung des Schreibschutzes auf andere Schnittstellen ist jedoch möglich.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Western Digital WD500BPVT	Sicherung 1:	1:54:09
	Sicherung 2:	1:54:00
	Sicherung 3:	1:54:02
	Durchschnitt:	1:54:04
Seagate ST500DM002_1	Sicherung 1:	1:37:55
	Sicherung 2:	1:38:16
	Sicherung 3:	1:37:54
	Durchschnitt:	1:38:02

Eine Überprüfung des Firebrick über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit PASS quittiert:

Summary

PASS No sectors on the drive were modified during the test.

Results

Unmodified Sectors	**34**
Modified Sectors	**0**
Commands Not Supported	19
Commands Not Enabled	0
Incomplete Commands	2
Errors	0
Skipped	0

Options

Force commands	False
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	False

4.1.3 UDeck (Beaglebone Black)

Auf Basis der Beagle Einplatinencomputer erstellte Dr. Polstra eine eigene Forensik-Distribution namens Deck Linux. Als Erweiterung dieses Systems wird auf Github eine Skriptsammlung angeboten, welche unter anderem die Funktion eines Write Blockers bietet. Dabei wird die Fähigkeit des Beaglebone Black genutzt, an einem Hostsystem angeschlossen als Netzwerkkarte und als Massenspeicher zu agieren.

Bild 27: Beaglebone Black als Write Blocker

Die beschriebenen Deck Linux Files werden auf Sourceforge zum Download angeboten. Es konnte zwar eine MicroSD Karte über eine aktuellere Version des Installationsskriptes „setup_sdcard" beschrieben werden, ein Zugriff auf den Beaglebone via SSH war jedoch nicht erfolgreich. Da die Skripte nicht notwendigerweise auf Deck Linux angewiesen sind, wurden aktuelle Ubuntu und Debian Images über die Software balenaEtcher auf eine MicroSD-Karte geschrieben und der Beaglebone mit gesteckter MicroSD-Karte gestartet. Ein Zugriff via SSH war hierbei möglich, die Ausführung des Skripts „mount-usb.sh" führte jedoch nicht zur Bereitstellung eines angeschlossenen USB-Sticks am Host-Gerät. Nach mehreren Versuchen mit verschiedenen Images konnte die gewünschte Funktion auf dem Image „bone-debian-7.11-lxde-4gb-armhf-2016-06-15-4gb.bin" beobachtet werden.

Ein SSH-Zugriff auf das Gerät ist über die IP: 192.168.7.2 möglich. Als Nutzer wird gemäß der Voreinstellung „debian" verwendet mit dem Passwort „temppwd". Die benötigten Skripte konnten via Git von der Udeck-Githubseite bezogen werden:

```
git clone https://github.com/ppolstra/UDeck
```

Die Ausführung des Skripts mit Rootberechtigung:

```
sudo mount-usb.sh
```

führt nun zu einer Trennung der Netzwerkverbindung zum Beaglebone und zur schreibgeschützten Bereitstellung des angeschlossenen USB-Sticks am Host-Gerät.

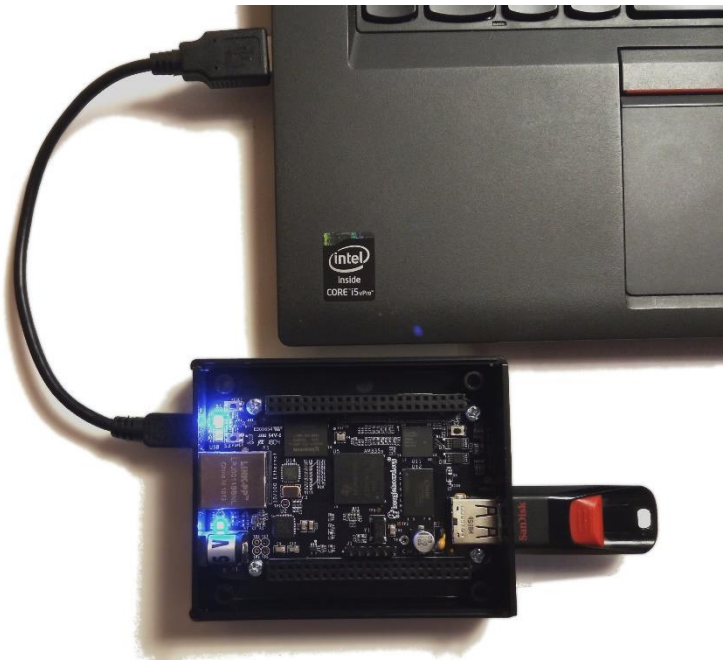

Bild 28: Einsatz des Beaglebone im Versuchsaufbau

4.1.3.1 Testablauf

Zunächst wurde der Beaglebone über dessen Mini-USB-Port mit dem Host -System (Manjaro KDE 21.2.6) verbunden. Im Anschluss wurde das Test-Medium am USB-A Port des Beaglebone eingesteckt. Nach erfolgter SSH-Verbindung und Ausführung des Skripts „mount-usb.sh“ konnte der Inhalt des Datenträgers im Dateimanager Dolphin betrachtet werden.

4.1.3.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen, wurden mit einer Fehlermeldung quittiert:

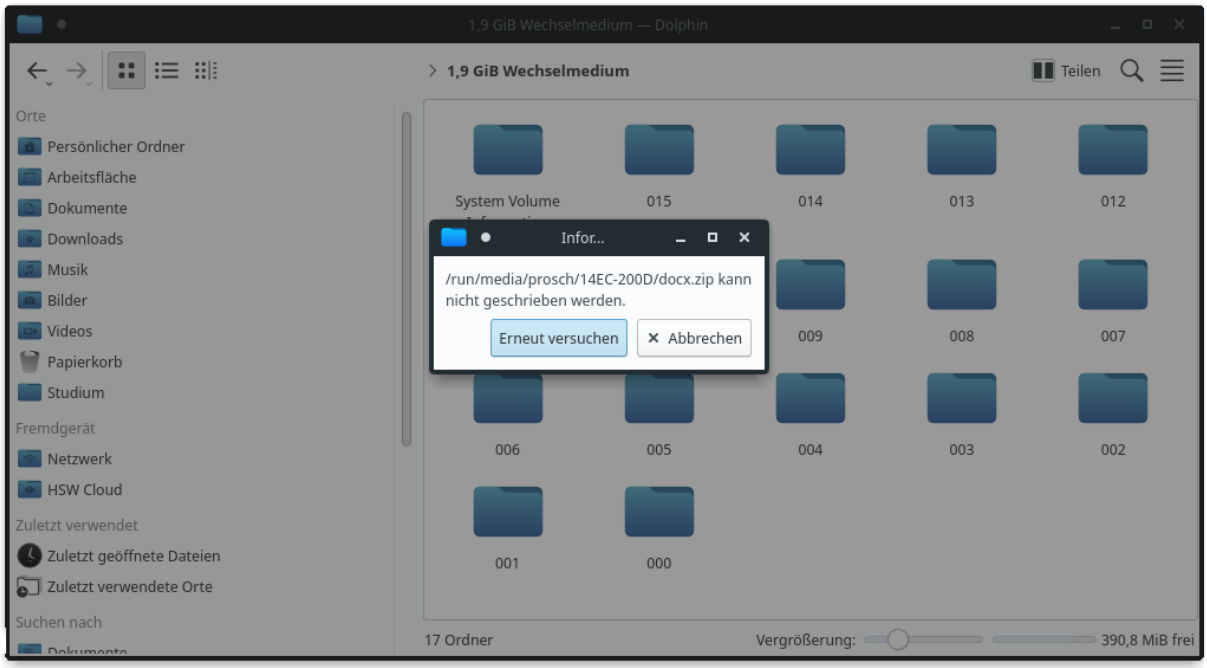

Bild 29: Udeck - Ausgabe eines Fehlers beim Versuch, eine Datei abzulegen

Im Rahmen der ersten Sicherung wurde anschließend folgender Hash berechnet:

MD5 checksum: 2c57db203873a6b4fa4e8b1c786259bf

SHA1 checksum: 1ee6da20a827f0a7d6d46a95c506f4c7f78ffff8

FAIL

Es ist erkennbar, dass dieser Hash-Wert vom ursprünglichen Wert (Siehe 1.1 Vorbereitung der Test-Medien) abweicht. Eine Kontrollsicherung über den forensischen Write-Blocker „WiebeTech USB 3.1 WriteBlocker“ ergab jedoch für dasselbe Medium ohne Zurückspielen des Original-Images den korrekten Hash-Wert. Eine Änderung am Datenträger hat entsprechend nicht stattgefunden. Es liegt lediglich eine Verfälschung des Images im Rahmen der Sicherung vor.

4.1.3.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im Fat32-Format neu zu formatieren. Dabei wurde eine Fehlermeldung ausgegeben, wonach ein Schreibzugriff auf das Medium nicht möglich sei:

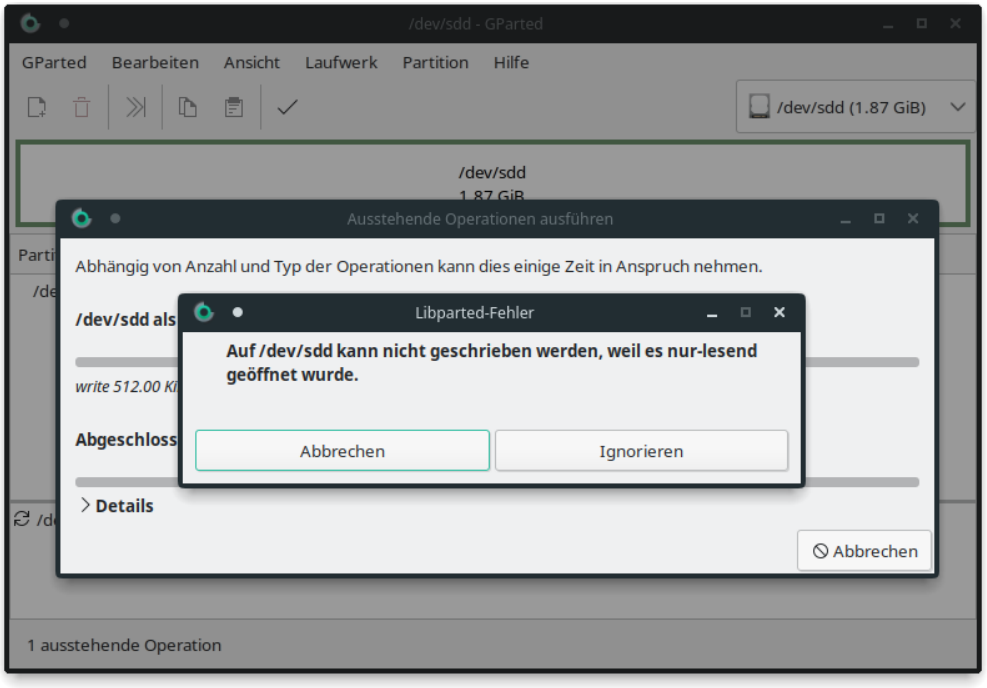

Bild 30: Udeck - Ausgabe eines Fehlers beim Versuch der Formatierung

Im Rahmen der zweiten Sicherung wurde folgender Hash berechnet:

MD5 checksum: 2c57db203873a6b4fa4e8b1c786259bf

SHA1 checksum: 1ee6da20a827f0a7d6d46a95c506f4c7f78ffff8

FAIL

Auch im Rahmen dieser Sicherung wurde der identische verfremdete Hash-Wert ausgegeben.

4.1.3.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium durchzuführen, werden mit dem Hinweis blockiert, dass es sich um ein read-only Device handelt. Bei Betrachtung der einzelnen Blöcke in der Editor-Ansicht fällt auf, dass sich die Werte von denen unterscheiden, welche mit anderen Write-Blockern bei diesem Medium eingesehen werden konnten (Siehe 2.2.1.1 Selbstbau USB-Writeblocker). Aus dem Eintrag der Ersten Zeile: „.X.MSWIN4.1.“ geht hervor, dass hier der Beginn der Partition dargestellt wird. Einträge, welche sich vor dem Beginn der Partition befinden werden über den Beaglebone nicht an das Host-System weitergereicht. So erklärt sich auch ein veränderter Hash-Wert bei der Sicherung der Medien.

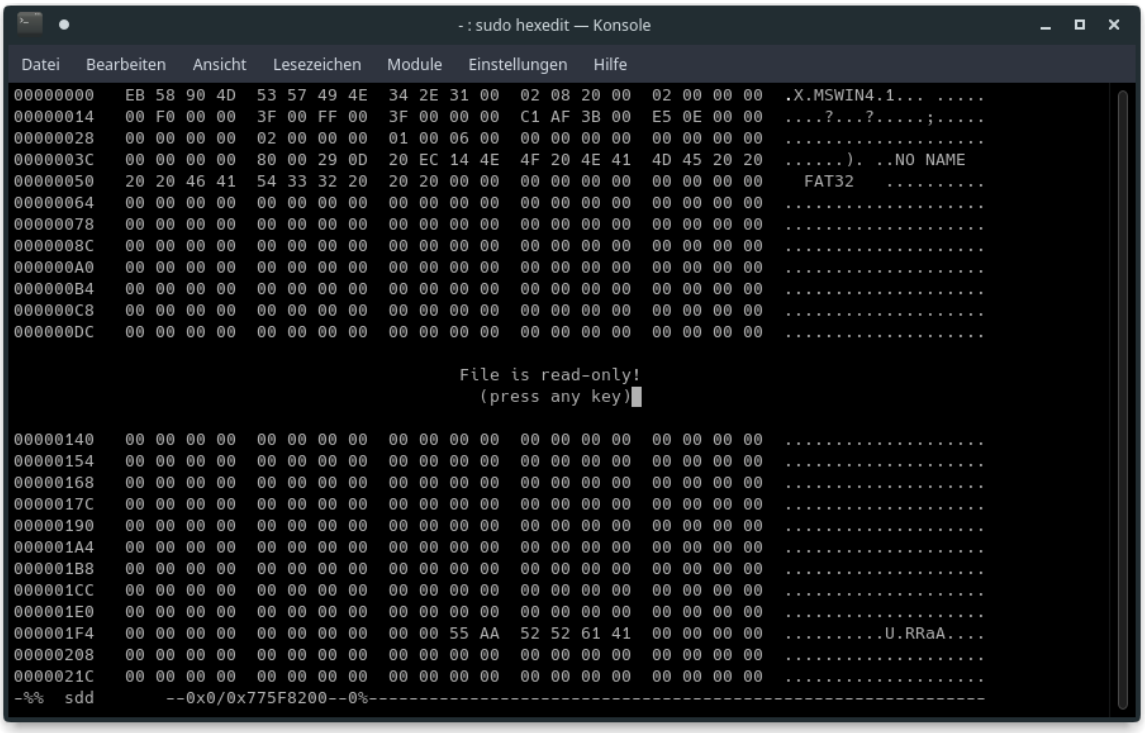

Bild 31: Udeck - Ausgabe eines Fehlers im Hexeditor

Die letzte Sicherung des Mediums ergab dabei die Hash-Werte:

MD5 checksum: 2c57db203873a6b4fa4e8b1c786259bf

SHA1 checksum: 1ee6da20a827f0a7d6d46a95c506f4c7f78ffff8

FAIL

Zwar wurde in Folge der Sicherungen keine Veränderung am Datenträger verursacht, eine Hash-identische physikalische Sicherung der Datenträger war jedoch nicht möglich. Eine Sicherung der Partitionen eines Datenträgers ist in der vorliegenden Version des Mount-Skriptes aktuell die umfangreichste Möglichkeit der Datensicherung über das Udeck.

4.1.3.5 Sicherung weiterer Medien / Ergebnisse

Im weiteren Testverlauf wurde versucht, die vorhandenen Testmedien nach dem beschriebenen Verfahren zu sichern. Eine zuverlässige Bereitstellung am Host-System gelang jedoch nur für die Medien: Imation Nano 2GB und Sandisk Ultra 32GB. Das Medium Emtec USB 2.0 Stick 8GB wurde trotz mehrmaliger Versuche nicht am Host-System bereitgestellt. Weiterhin wurde der Versuch unternommen, die vorhandenen Festplatten über eine SATA/USB-Brücke und unter Verwendung eines zusätzlichen Netzteils zu sichern. Dabei konnte eine Verbindung zum Medium Seagate ST500DM002_1 hergestellt werden, welche nach einer ersten erfolgreichen Sicherung nicht erneut beobachtet werden konnte. Das Medium Western Digital WD500BPVT konnte nicht am Host-System ausgegeben werden.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Imation Nano 2GB	Sicherung 1:	0:03:40
	Sicherung 2:	0:03:41
	Sicherung 3:	0:03:41
	Durchschnitt:	0:03:41
Emtec USB 2.0 Stick 8GB	Sicherung 1:	keine Verbindung
Sandisk Ultra 32GB	Sicherung 1:	0:56:25
	Sicherung 2:	0:56:26
	Sicherung 3:	0:56:28
	Durchschnitt:	0:56:26
Western Digital WD500BPVT	Sicherung 1:	keine Verbindung
Seagate ST500DM002_1	Sicherung 1:	13:58:22
	Sicherung 2:	keine Verbindung

Eine Überprüfung des Udeck-Beaglebones über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit PASS quittiert:

Summary

PASS No sectors on the drive were modified during the test.

Results

Unmodified Sectors	**34**
Modified Sectors	**0**
Commands Not Supported	19
Commands Not Enabled	0
Incomplete Commands	2
Errors	0
Skipped	0

Options

Force commands	False
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	False

Da Tool keine Kenntnis vom eigentlichen Hash-Wert der Original-Sicherung hat, steht dies nicht im Gegensatz zu den Erkenntnissen der Test-Durchführung.

4.1.4 Magic USB-Hub (4Deck)

Bei dem 4Deck-Projekt (https://github.com/ppolstra/4deck) handelt es sich nicht um einen klassischen Hardware-Write-Blocker, sondern um ein Script zur Erstellung angepasster Udev-Regeln, welches als Addon für das von Dr. Polstra bereitgestellte Deck-Linux angeboten wird. Nach Angaben auf der Projektseite seien die Udev-Regeln jedoch auch auf anderen modernen Linux Distributionen anwendbar.

Bild 32: Einsatz eines USB 3.0 Hubs im Versuchsaufbau als 4Deck Hub

Der Schreibschutz wird hierbei über die generierten Udev-Regeln realisiert, welche auf die VID und PID Nummern des USB-Hubs abgestimmt werden und USB-Massenspeicher, welche über diesen Hub angeschlossen werden automatisch im read-only Mode einbinden.

Zunächst wurde der Versuch unternommen, das Script unter Manjaro KDE 21 auszuführen. Zwar werden dabei Udev-Regeln erstellt; die erwünschte Funktion des automatischen read-only Mounts konnte jedoch nicht beobachtet werden. Auch die Ausführung unter Xubuntu 20.04 war nicht vollständig erfolgreich. Ein Automount findet auch hier nicht statt, es lassen sich jedoch erstellte Mount-Scripte ausführen und Datenträger so händisch mounten. Es wurde daher ein Xubuntu 16.04 Live-System per USB gebootet und auch hier die Udev-Regeln über das Script erstellt.

Dazu wurde zunächst via Git das 4Deck Projekt geklont:

```
xubuntu@xubuntu:~$ git clone https://github.com/ppolstra/4deck
Cloning into '4deck'...
```

Anschließend galt es die VID und PID-Nummern des USB-Hubs zu ermitteln und an das Script zu übergeben:

```
xubuntu@xubuntu:~/4deck$ lsusb | grep VIA
Bus 004 Device 003: ID 2109:0817 VIA Labs, Inc.
Bus 003 Device 011: ID 2109:2817 VIA Labs, Inc.
xubuntu@xubuntu:~/4deck$ sudo ./install.sh --vid 2109 --pid 2817 --pid2 0817
```

Auf diesem System konnte das erwünschte Verhalten beobachtet werden. Nach dem Einstecken eines USB-Massenspeichers am USB-Hub wurde dieser automatisch als read-only eingebunden. Dabei tauchen die Geräte im Dateimanager doppelt auf: einmal unter dem vergebenen Gerätenamen (z.B. „Stick“) und ein weiteres Mal unter der fortlaufenden Systembezeichnung (z.B. sdc). Für den Dateiaufruf ist dieses Detail jedoch unerheblich, da beide Bezeichnungen zum selben Gerät weisen, welches lediglich lesend eingebunden wird.

4.1.4.1 Testablauf

Als Testsystem wurde hierbei Xubuntu 16.04 genutzt. Nach Einrichtung der Udev-Regeln, wurde das Testmedium Imation Nano USB 2.0 über den USB-Hub an das Host-System angeschlossen. Dabei spielte es keine Rolle, ob das Medium zunächst am Hub und dieser anschließend am Host-System angeschlossen oder ob das Medium am bereits angesteckten USB-Hub verbunden wurde. Über den Dateimanager Thunar konnte das Medium nach erfolgter Verbindung eingesehen werden.

4.1.4.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen oder von diesem zu löschen, wurden mit einer Fehlermeldung quittiert:

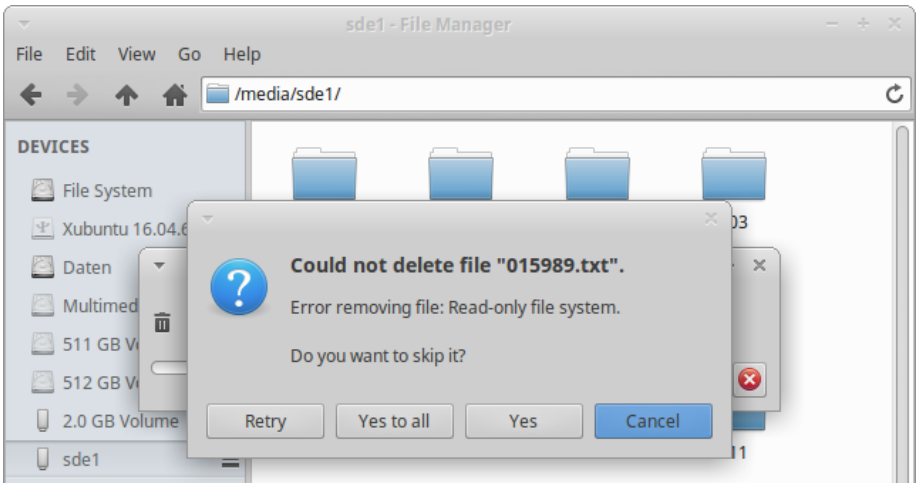

Bild 33: 4deck - Ausgabe eines Fehlers beim Versuch, eine Datei zu löschen

Die Sicherung in Folge der Dateioperationen wies folgende Hash-Werte auf:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

Eine Veränderung am Datenträger in Folge der Dateioperationen fand nicht statt.

4.1.4.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im Fat32-Format neu zu formatieren. Hierbei vermeldete das System den Erfolg der Formatierung und zeigte im Anschluss einen veränderten (leeren) Füllstand der Partition.

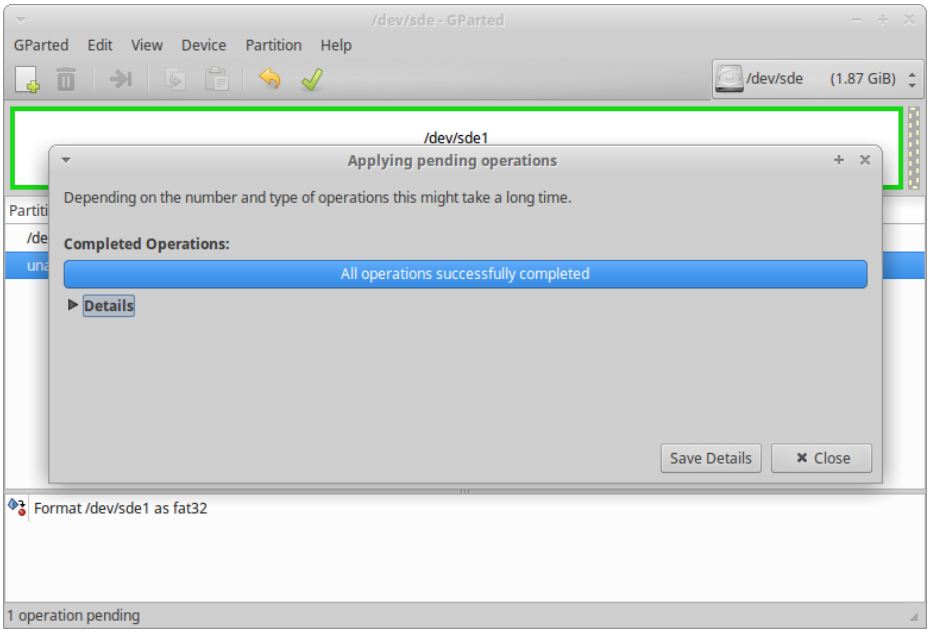

Bild 34: 4deck - Ausgabe der Erfolgsmeldung beim Versuch der Formatierung

Im Rahmen der zweiten Sicherung wurde folgender Hash berechnet:

MD5 checksum: a3e8183e0416388b40fec7851e28b2f4

SHA1 checksum: 14181de212bc73405697b2fe95f6b9c2b1c6ad7d

FAIL

Hierbei kam es nachweislich zu Veränderungen am Medium, welche sich in einen veränderten Hashwert im Rahmen der physikalischen Sicherung ausdrücken.

Um den ursprünglichen Zustand des Mediums wiederherzustellen, wurde das Original-Image per dd erneut auf das Medium geschrieben.

4.1.4.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium durchzuführen waren hier augenscheinlich erfolgreich. Wie bereits beim DIY Writeblocker, wurde auch hier das erste Wertepaar 00 durch 10 überschrieben.

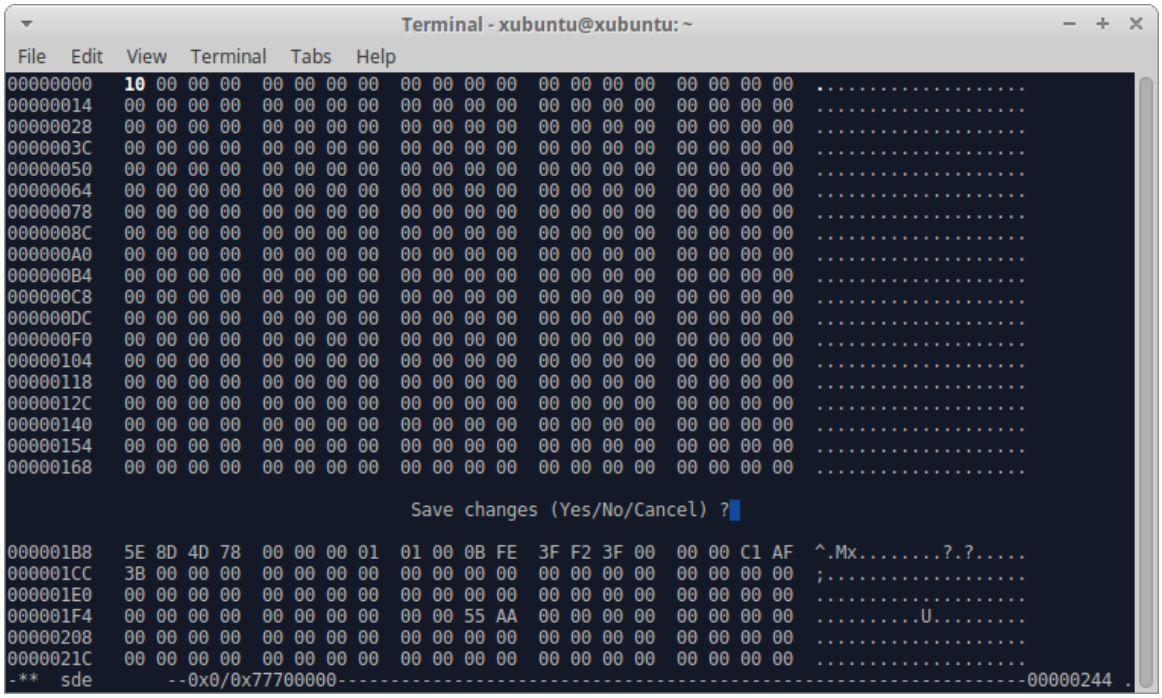

Bild 35: 4Deck – Hexedit: Speicherung der Veränderungen ohne Fehlermeldung

Die letzte Sicherung des Mediums ergab dabei die Hash-Werte:

MD5 checksum: 74d9dda28e6a1ff0b4b8242e41e3053c

SHA1 checksum: 05deeb9077145fd00b06db711c3204be748c15f8

FAIL

Durch die gesetzten Udev Regeln wird lediglich ein oberflächlicher Schutz gegen Dateioperationen gewährleistet. Veränderungen auf Partitions- oder Blockebene wurden hingegen nicht blockiert.

Die Herstellung des Original-Zustandes konnte nach Beendigung des Testes durch ein Rückeditieren des veränderten Wertepaares auf den Ursprungswert 00 erreicht werden.

4.1.4.5 Sicherung weiterer Medien / Ergebnisse

Die Medien Imation Nano 2GB und Sandisk Ultra 32GB konnten erwartungsgemäß automatisch nach dem Einstecken als read-only am Host-System eingesehen werden. Bei dem Medium Emtec USB 2.0 Stick 8GB fand kein Automount statt. Das Zugreifen auf den Datenträger über den Dateimanager Thunar führte hierbei zum Einbinden des Mediums im read-write Modus. Von einer Sicherung und weiteren Verwendung des Emtec Sticks wurde bei dieser Testrunde jedoch abstand genommen. Im Rahmen des Tests des CRU Write-Blockers wurde festgestellt, dass es bereits zu einer Veränderung am Datenträger kam und dessen Hash-Wert bei der Sicherung vom Original abwich, so dass auch hier zunächst eine Wiederherstellung des Ausgangszustandes über dd erforderlich war. Die vorhandenen Festplatten konnten über eine SATA/USB-Brücke an den Hub angeschlossen werden und wurden erwartungsgemäß als read-only eingebunden.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Imation Nano 2GB	Sicherung 1:	0:01:32
	Sicherung 2:	0:01:32
	Sicherung 3:	0:01:32
	Durchschnitt:	0:01:32
Emtec USB 2.0 Stick 8GB	Sicherung 1:	Verbindung nur r/w
Sandisk Ultra 32GB	Sicherung 1:	0:08:13
	Sicherung 2:	0:08:13
	Sicherung 3:	0:08:13
	Durchschnitt:	0:08:13
Western Digital WD500BPVT	Sicherung 1:	1:48:54
	Sicherung 1:	1:48:54
	Sicherung 1:	1:48:55
	Durchschnitt:	1:48:54

Seagate ST500DM002_1	Sicherung 1:	1:19:35
	Sicherung 2:	1:19:33
	Sicherung 2:	1:19:37
	Durchschnitt:	1:19:35

Eine Überprüfung mittels der WriteBlocking Validation Utility war aufgrund der Art der Erstellung des 4Deck (Linux Udev Regeln) nicht möglich.

4.1.5 Sharkoon DriveLink Combo USB 3.0 V2

Als „Low Cost" Alternative zu kostspieligeren forensischen Write-Blockern (Verkaufspreis 2022 ca. 30€) versteht sich der Sharkoon DriveLink Combo USB 3.0 V2.

Bild 36: DriveLink Combo USB 3.0

Bei dem Gerät handelt es sich um eine USB3.0 zu SATA/IDE Brücke, bei der die Schreibschutzfunktion über einen Schalter auf der Geräteoberseite nach Anschlusstyp getrennt aktiviert und deaktiviert werden kann.

Auffallend ist die Ähnlichkeit des Geräts zum Coolgear SS-127ASD Write-Blocker, welcher im Handel nicht mehr erhältlich ist. Coolgear bewarb seinen Write-Blocker als „NIST approved". Über den NIST Tools Catalog (https://toolcatalog.nist.gov) wird das Coolgear-Gerät ebenfalls als Hardware-Write-Blocker ausgewiesen.

Eine gesonderte Treiberinstallation war für den Betrieb nicht erforderlich. Nach dem Anschluss, dem Setzen des Schreibschutzes und der Betätigung des ON/OFF Schalters wurde das Angeschlossene Medium unter Windows und Linux angezeigt und konnte lesend eingesehen werden.

4.1.5.1 Testablauf

Das Medium Western Digital WD500BPVT wurde zunächst an den Write-Bocker über dessen SATA-Port angeschlossen. Nach der Verbindung des Netzkabels und des USB-Kabels zum Host-System wurde das Gerät über den Schalter an der Geräteoberseite eingeschaltet. Das Test-Medium wurde daraufhin umgehend vom System (Manjaro KDE 21.2.6) erkannt und konnte eingesehen werden. Dabei wurde auf die korrekte Stellung des SATA-Schreibschutzschalters geachtet. Im Rahmen der folgenden Sicherung kam es beim Testmedium WD500BPVT drei Mal zu einem Verlust der Geräteverbindung, so dass die Sicherung wiederholt werden musst. Dieses Verhalten wurde nur bei gesetztem Schreibschutz beobachtet. Wurde das Gerät ohne Schreibschutz als SATA/USB-Brücke verwendet, kam es zu keinen Abbrüchen. Bei dem Testmedium Seagate ST500DM002_1 trat das Problem nicht auf.

4.1.5.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen oder von diesem zu löschen, wurden mit einer Fehlermeldung quittiert:

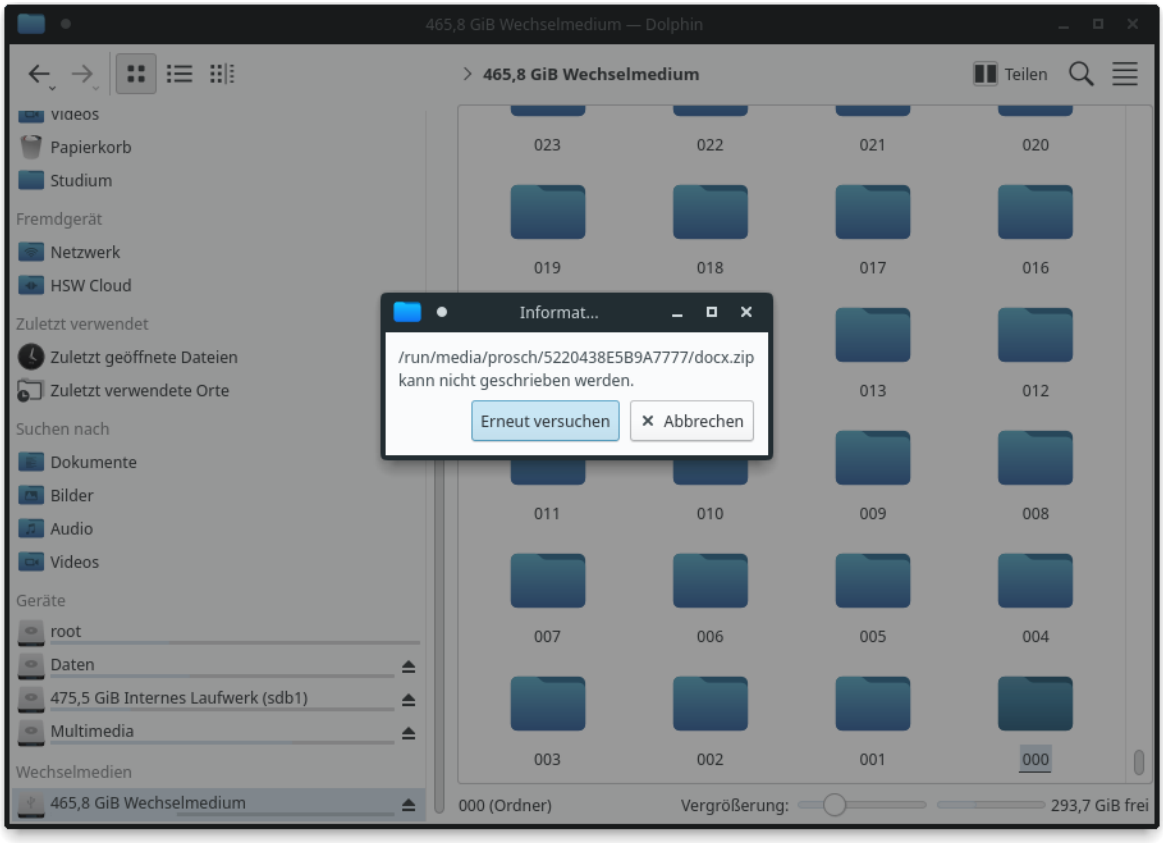

Bild 37: Sharkoon - Ausgabe eines Fehlers beim Versuch, eine Datei abzulegen

Die Sicherung in Folge der Dateioperationen wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der Dateioperationen fand nicht statt.

4.1.5.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im NTFS-Format neu zu formatieren. Dabei wurde eine Fehlermeldung ausgegeben, wonach ein Schreibzugriff auf das Medium nicht möglich sei:

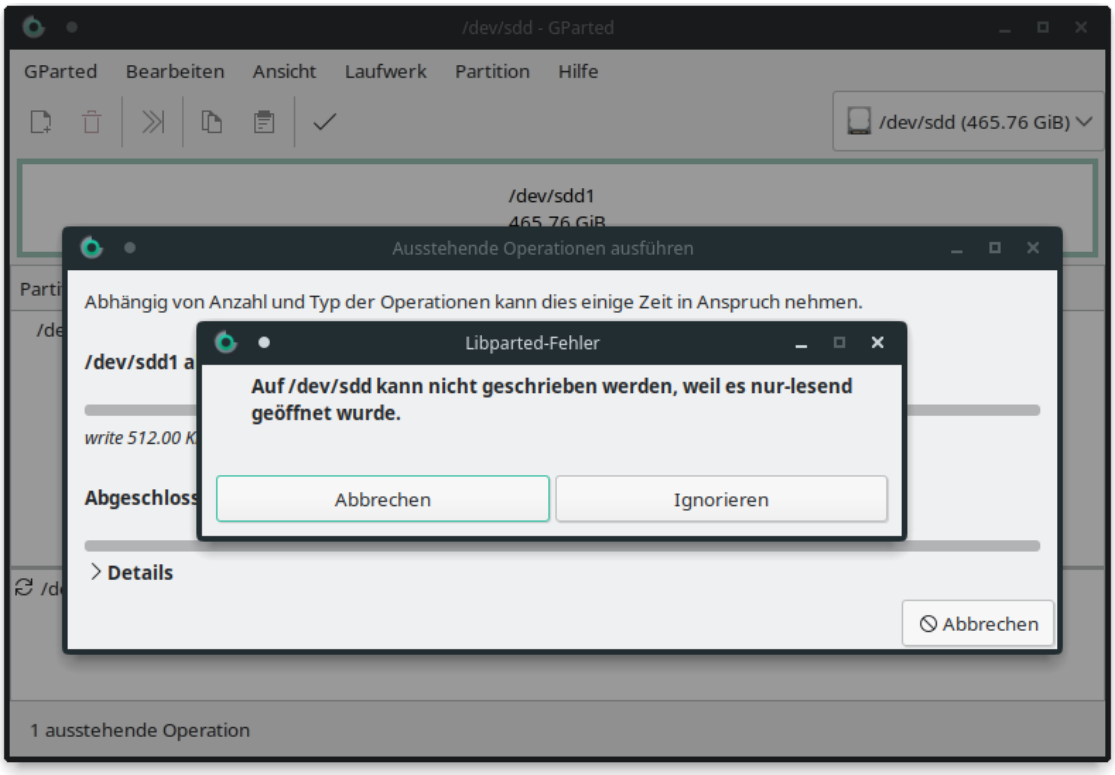

Bild 38: Sharkoon - Ausgabe eines Fehlers beim Versuch der Formatierung

Im Rahmen der zweiten Sicherung wurde folgender Hash berechnet:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

4.1.5.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium durchzuführen, werden mit dem Hinweis blockiert, dass es sich um ein read-only Device handelt:

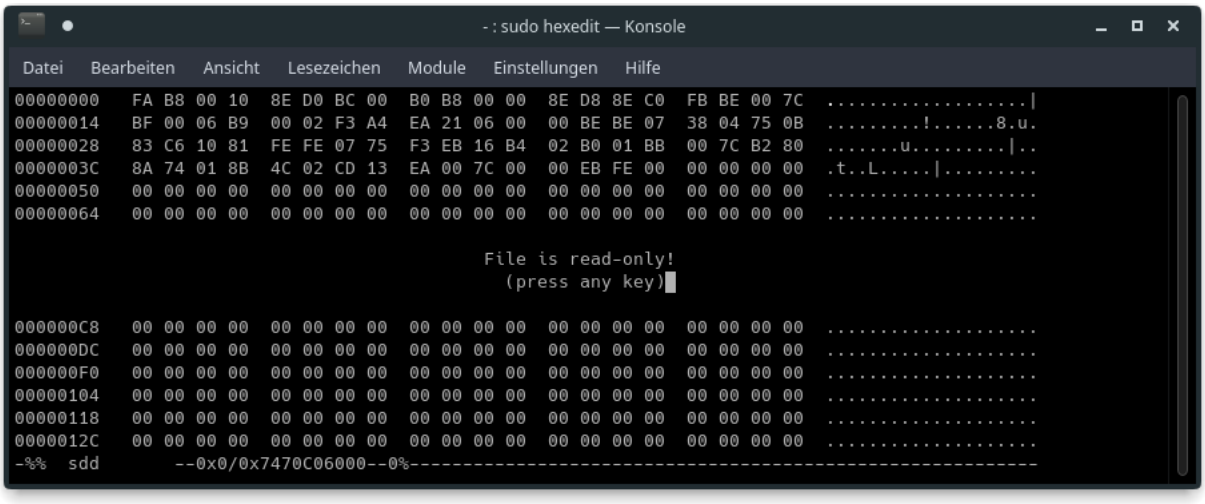

Bild 39: Sharkoon - Ausgabe eines Fehlers im Hexeditor

Die letzte Sicherung des Mediums ergab dabei die Hash-Werte:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger fand im Rahmen der durchgeführten Tests nicht statt.

4.1.5.5 Sicherung weiterer Medien / Ergebnisse

Da der Schreibschutz des Sharkoon DriveLink Combo USB 3.0 nur für die SATA-Schnittstelle bereitgestellt wird, wurden nur die Test-Festplatten gesichert.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Western Digital WD500BPVT	Sicherung 1:	1:49:11
	Sicherung 2:	1:49:03
	Sicherung 3:	1:49:07
	Durchschnitt:	1:49:07
Seagate ST500DM002_1	Sicherung 1:	1:20:12
	Sicherung 2:	1:20:12
	Sicherung 3:	1:20:15
	Durchschnitt:	1:20:13

Eine Überprüfung des Sharkoon DriveLink Combo USB 3.0 V2 über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit FAIL quittiert:

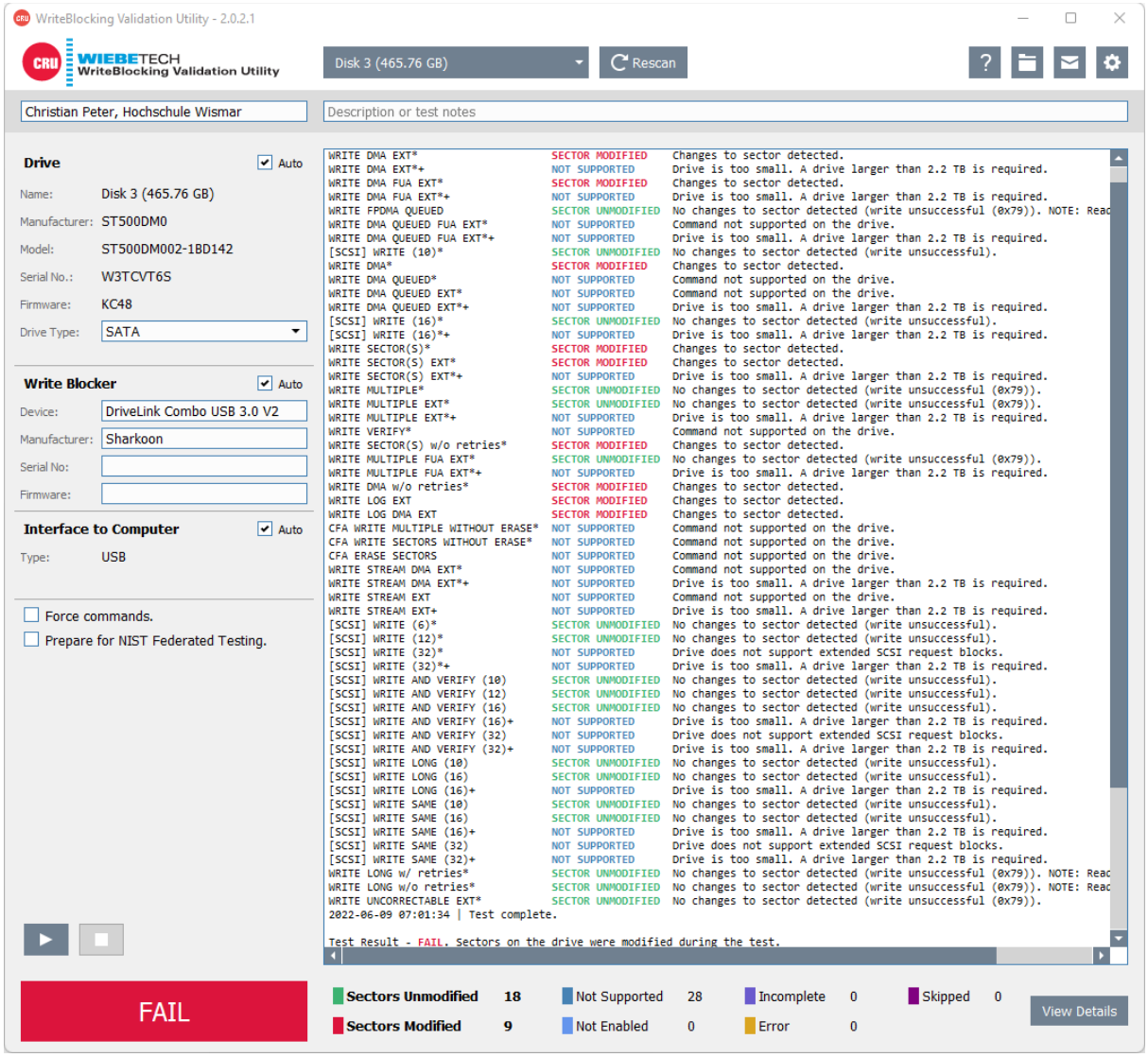

Bild 40: Sharkoon – nicht geblockte Schreibzugriffe

Dieses Ergebnis ähnelt dem des Coolgear SS-127ASD, welcher in einem Test der Nova Southeastern University im März 2020 ebenfalls nicht alle Schreibzugriffe blocken konnte. (8)

4.1.6 Delock 62652 SATA / USB Converter

Eine weitere „Low Cost“ Variante stellt der Delock 62652 SATA / USB Converter dar. (Verkaufspreis 2022 ca 30€)

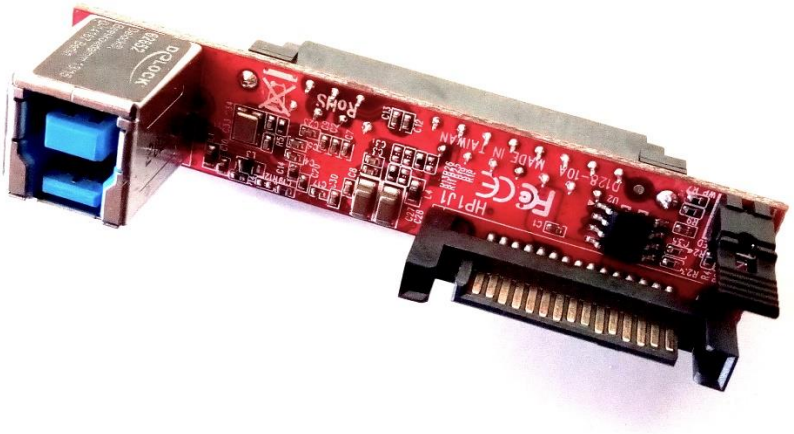

Bild 41: Delock 62652 mit gesetztem Schreibschutz-Jumper

Bei dem Gerät handelt es sich um eine USB3.0 zu SATA Brücke, bei welcher die Schreibschutzfunktion über einen Jumper auf den Pins 3 und 4 der Pin-Leiste gesetzt werden kann. Der Adapter wird direkt auf die SATA Power und Data Anschlüsse des Mediums aufgesetzt und dann per USB 3.0 Kabel mit dem Host-System verbunden. Zum Betrieb bedarf es zusätzlich eines Netzteils mit einem SATA-Power-Anschluss. Ein solches Netzteil war dem Gerät nicht beigelegt und musste zusätzlich angeschafft werden. Ein Betrieb nur über den USB 3.0 Port war auch mit angeschlossener 2,5“ Festplatte nicht möglich.

Eine gesonderte Treiberinstallation war für den Betrieb nicht erforderlich. Nach dem Setzen des Schreibschutzes und dem Anschluss an das Host-System wurde das Angeschlossene Medium unter Windows und Linux angezeigt und konnte lesend eingesehen werden.

4.1.6.1 Testablauf

Das Medium Western Digital WD500BPVT wurde zunächst an den Write-Bocker über dessen SATA-Port angeschlossen. Nach der Verbindung des Netzteiles und des USB-Kabels zum Host-System wurde das Test-Medium umgehend vom System (Manjaro KDE 21.2.6) erkannt und konnte eingesehen werden.

4.1.6.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen oder von diesem zu löschen, wurden mit einer Fehlermeldung quittiert:

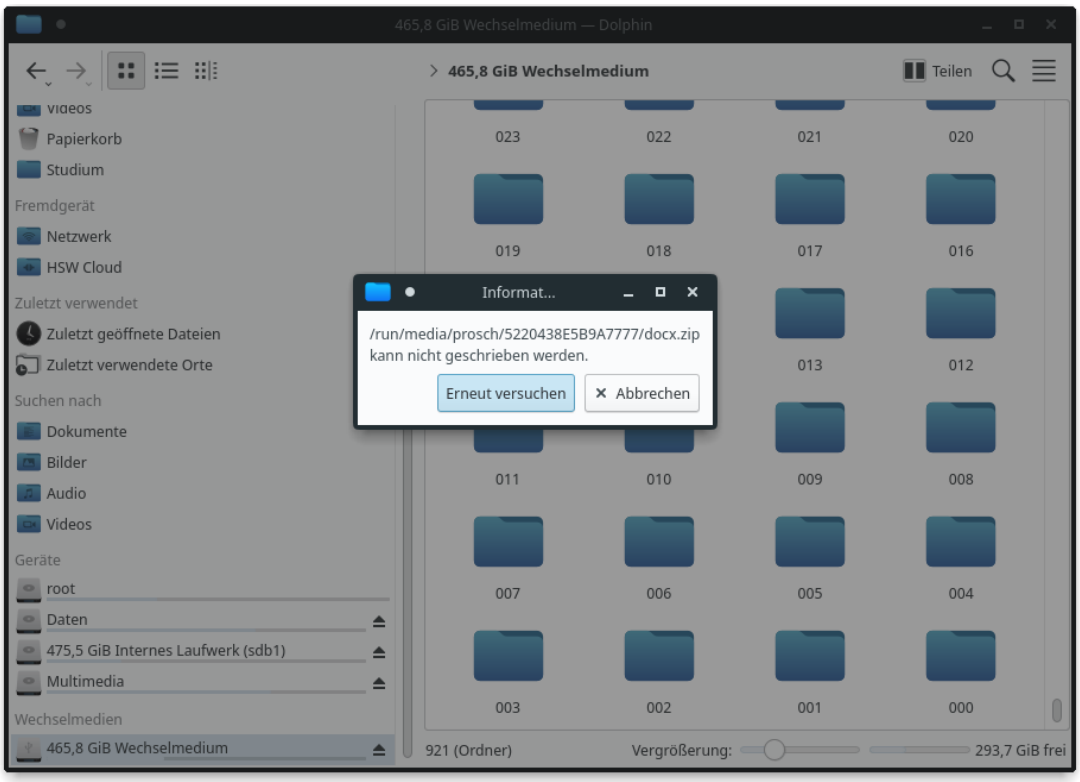

Bild 42: Delock - Ausgabe eines Fehlers beim Versuch, eine Datei abzulegen

Die Sicherung in Folge der Dateioperationen wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der Dateioperationen fand nicht statt.

4.1.6.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im NTFS-Format neu zu formatieren. Dabei wurde eine Fehlermeldung ausgegeben, wonach ein Schreibzugriff auf das Medium nicht möglich sei:

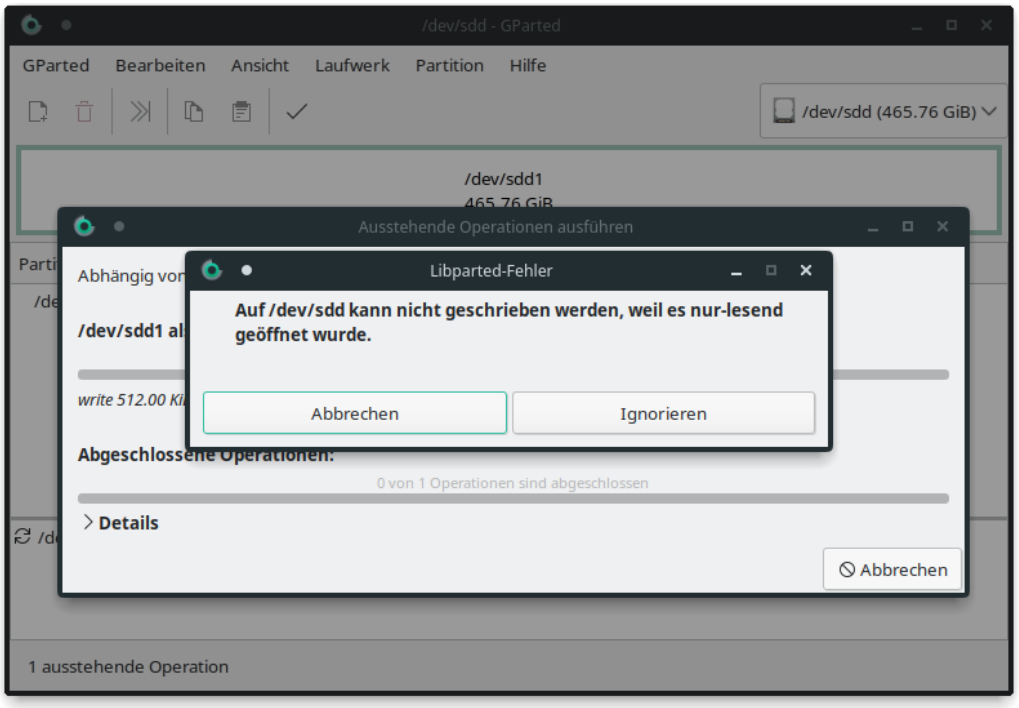

Bild 43: Delock - Ausgabe eines Fehlers beim Versuch der Formatierung

Im Rahmen der zweiten Sicherung wurde folgender Hash berechnet:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

4.1.6.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium durchzuführen, werden mit dem Hinweis blockiert, dass es sich um ein read-only Device handelt:

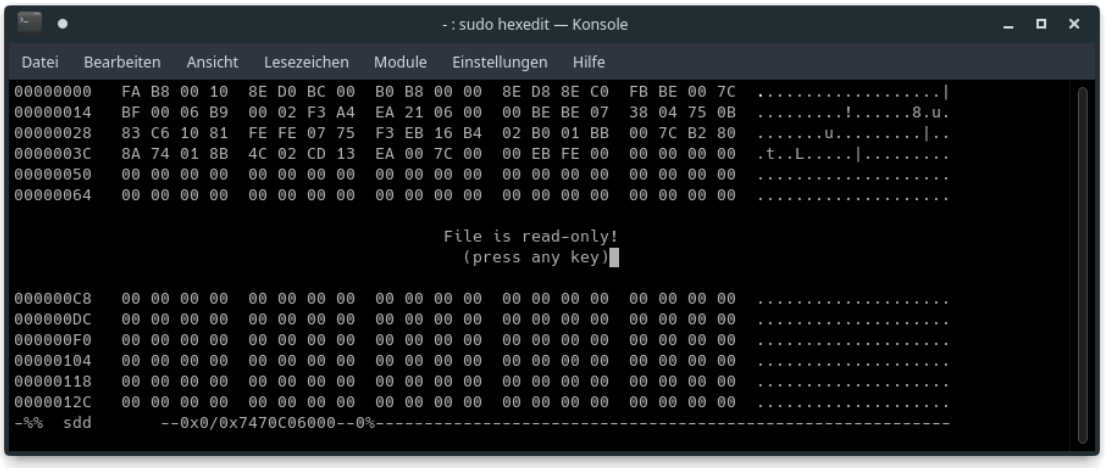

Bild 44: Delock - Ausgabe eines Fehlers im Hexeditor

Die Sicherung in Folge der Dateioperationen wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der Dateioperationen fand nicht statt.

4.1.6.5 Sicherung weiterer Medien / Ergebnisse

Da der Schreibschutz des Delock 62652 nur für die SATA-Schnittstelle bereitgestellt wird, wurden nur die Test-Festplatten gesichert. Die zweite Sicherung des Mediums Seagate ST500DM002_1 wies hier eine Besonderheit auf. Mit 2 Stunden 5 Minuten und 22 Sekunden dauerte diese ca. 45 Minuten länger als die erste und dritte Sicherung. Darüber hinaus wurde auch ein anderer Hash generiert:

MD5 checksum: f8a24a8572294e16d54d85bcb1155bb2
SHA1 checksum: e7184f9f0dd2ab8eaac39f746995b533da6249bb

Da im Rahmen der dritten Sicherung wieder der korrekte Hash-Wert ausgegeben wurde, ist ersichtlich, dass es zu keiner Veränderung am Datenträger kam. Es ist anzunehmen, dass Lesefehler auftraten, über welche keine Rückmeldungen an das System erfolgten. Derartige Fehler bei der Sicherung mit dem FTKImager lassen sich über den Parameter „--verify" erkennen. Dies bedeutet jedoch eine Verdoppelung der Sicherungszeit.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Western Digital WD500BPVT	Sicherung 1:	1:58:51
	Sicherung 2:	1:49:04
	Sicherung 3:	1:49:06
	Durchschnitt:	1:52:20
Seagate ST500DM002_1	Sicherung 1:	1:20:17
	Sicherung 2:	2:05:22
	Sicherung 3:	1:20:49
	Durchschnitt:	1:35:29

Eine Überprüfung des Delock 62652 über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit PASS quittiert:

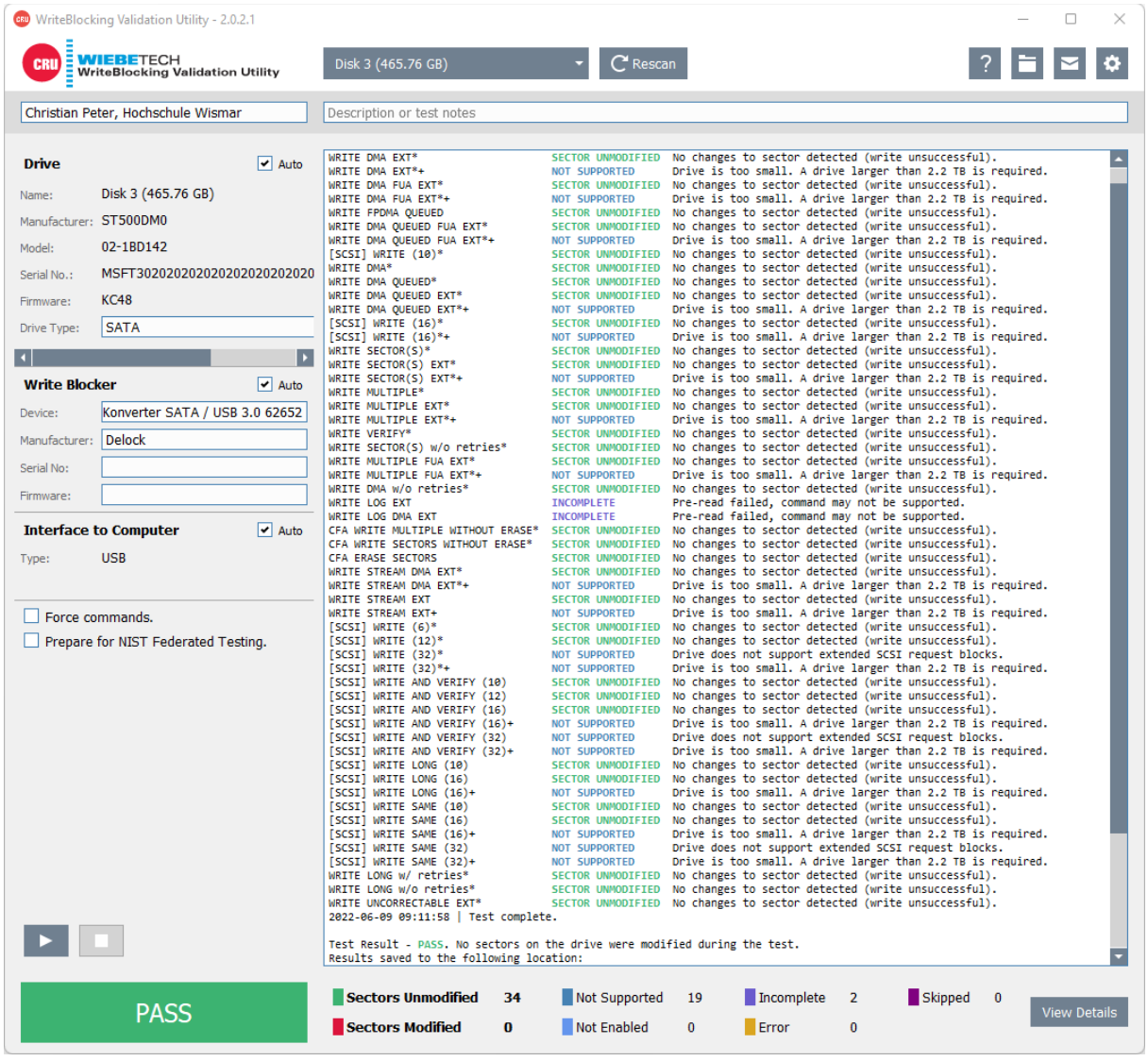

Bild 45: Delock 62652 – alle Schreibzugriffe wurden geblockt

4.1.7 WiebeTech USB 3.1 WriteBlocker

Bei dem USB 3.1 WriteBlocker von WiebeTech handelt es sich um einen Write-Blocker mit forensischem Anspruch. Dies schlägt sich auch im Handelspreis nieder, welcher mit 484,00€ ausgewiesen wird (Stand: Juni 2022)

Bild 46: WiebeTech USB 3.1 WriteBlocker

Das Quellmedium wird hier wahlweise über USB 3.0 (A-Port) oder USB 3.1 (C-Port) an dem Writeblocker eingesteckt und dieser anschließend über den Host-USB-Anschluss mit dem Sicherungs-PC verbunden.
Eine Verbindung des Write-Blockers unter Manjaro KDE 21.2.6 war nicht möglich, da zur korrekten Funktion des Geräts eine Treiberinstallation erforderlich ist. Dieser Treiber wird nur für Windows-Betriebssysteme bereitgestellt. Daher wurden die nachfolgenden Tests unter Windows 11 durchgeführt.

Nach dem Einstecken des Gerätes am Host zeigte dieser zunächst eine gelbe Status-LED. In diesem Zustand wird das Medium nicht an das Host-System weiter gereicht. Die Betätigung des „Host Validate“ Buttons führte zur Anzeige einer roten Status-LED.
Der passende Treiber des Geräts lässt sich von der Herstellerseite beziehen: https://wiebetech.com/downloads/1229/CRUWBlocker-1.2.1.2-(2018.09.04).exe
Nach erfolgreicher Installation des Treiberpaketes, konnte nach erneuter Betätigung des „Host Validate“ Buttons eine Verbindung zum Write-Blocker hergestellt werden. Dabei wechselte die Status-LED des Gerätes auf grün und die Ordnerstruktur des Quellmediums konnte über den Explorer eingesehen werden.

4.1.7.1 Testablauf

Als Testsystem wurde hierbei Windows 11 21H2 genutzt. Das Testmedium Imation Nano USB 2.0 wurde zunächst an den USB-Write-Blocker und dieser an das Host-System angeschlossen. Nach der Betätigung des „Host Validate“ Buttons war die Ordnerstruktur des USB-Sticks über den Windows-Explorer einsehbar.

4.1.7.2 Dateioperationen:

Es wurde versucht, eine Datei (docx.zip) auf den Datenträger zu kopieren und einen Ordner vom Datenträger zu löschen (Ordner 015).

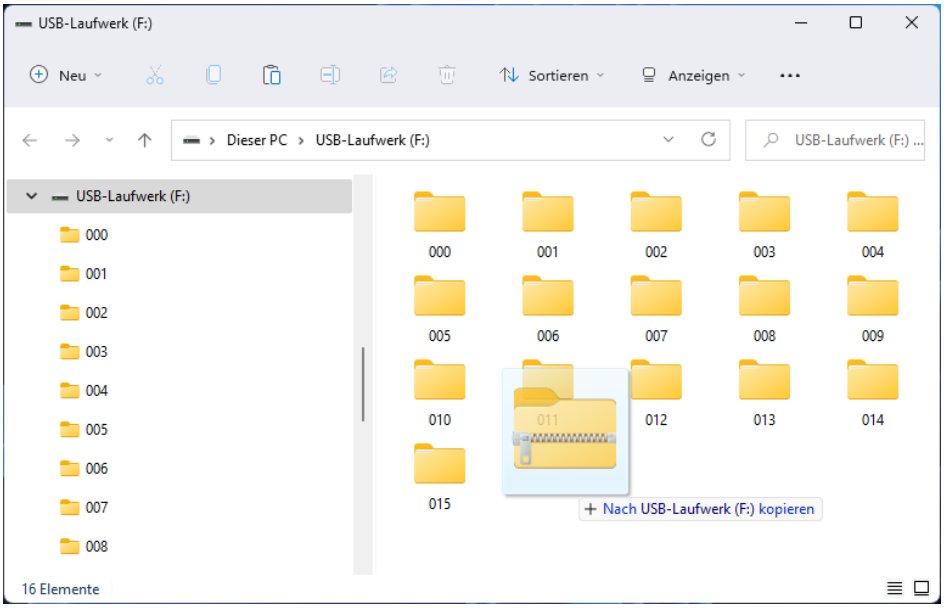

Bild 47: WiebeTech USB – Kopieren einer Datei auf das Medium

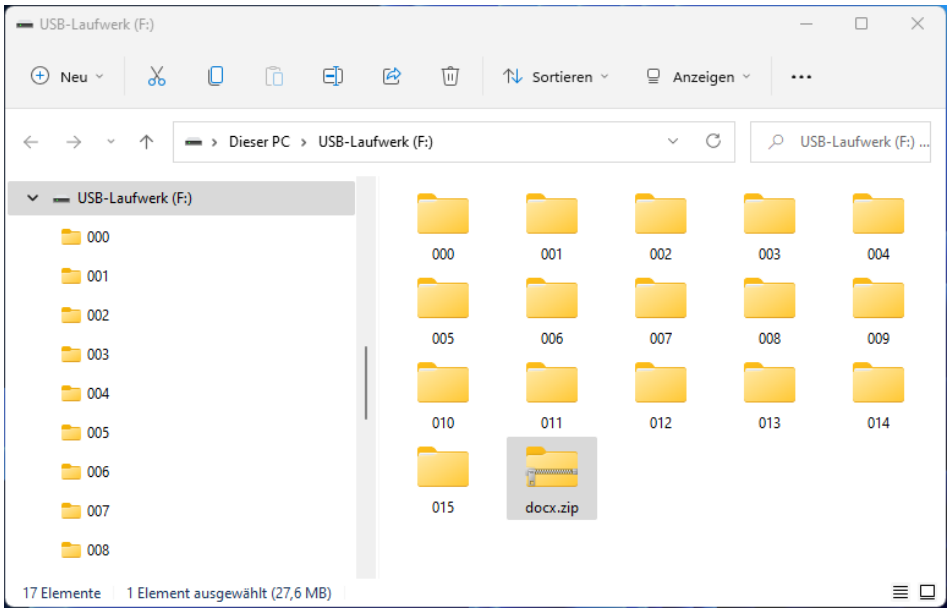

Bild 48: WiebeTech USB – augenscheinlich erfolgreiche Kopieroperation

Beide Operationen wurden augenscheinlich vom System durchgeführt.
Im Anschluss an die Dateioperationen wurde mittels des FTKImagers eine physikalische Sicherung des Datenträgers erstellt:

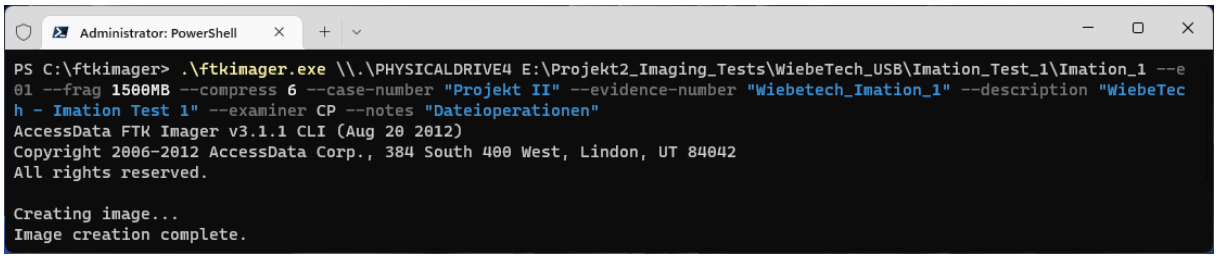

Bild 49: Nutzung der CLI Version des FTKImagers unter Windows

Diese Sicherung war wies folgende Hash-Werte auf:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

Eine Änderung am Datenträger ist demzufolge trotz gegenteiliger Rückmeldung vom Betriebssystem nicht verursacht worden.

4.1.7.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Windows-eigenen Formatierfunktion im NTFS-Format neu zu formatieren. Dabei wurde eine Fehlermeldung ausgegeben.

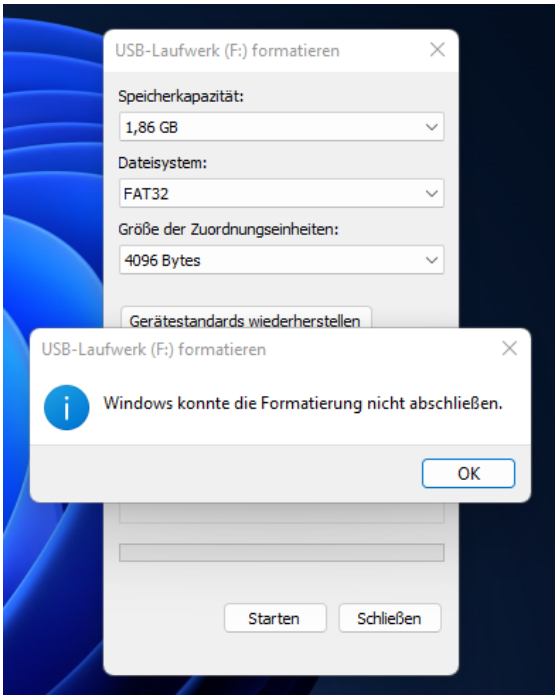

Bild 50: WiebeTech USB – Ausgabe eines Fehlers beim Versuch des Formatierens

Im Rahmen der zweiten Sicherung wurde folgender Hash berechnet:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

4.1.7.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium über die Software HxD durchzuführen führen zu keiner schreibenden Operation. Lediglich der „Schreibgeschützt“ Hinweis in der Status-Leiste des Programms wird dabei hervorgehoben:

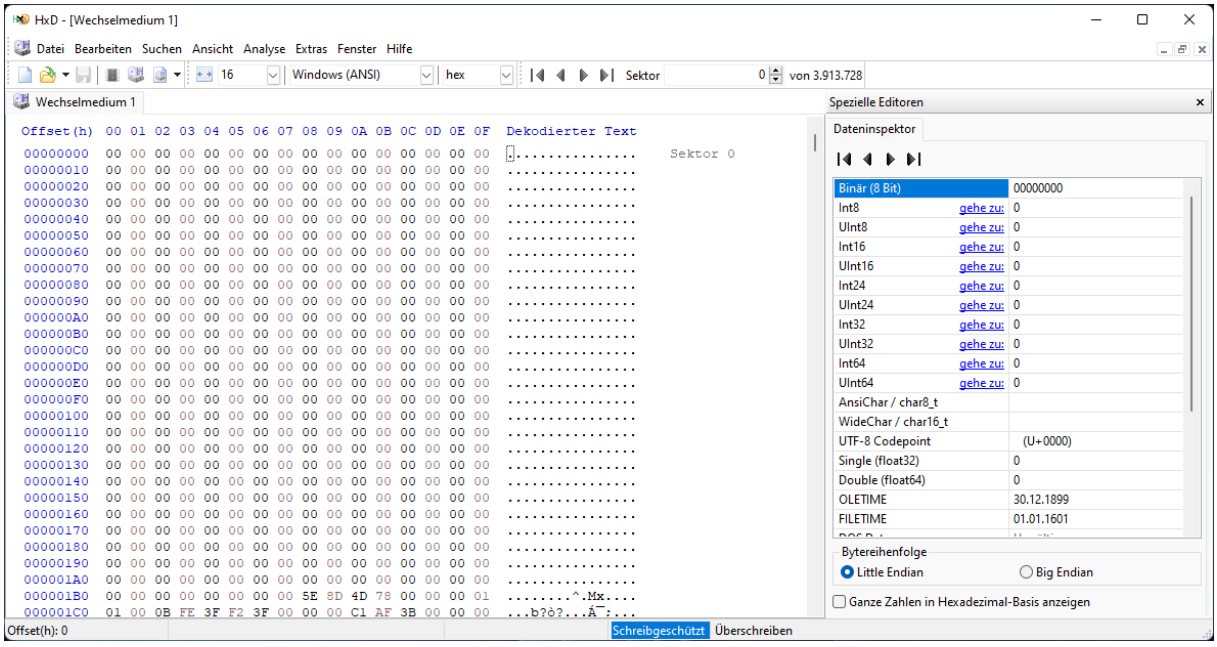

Bild 51: WiebeTech USB – HEX-Ansicht des Imation Nano USB Sticks

Die abschließende Sicherung des Mediums wies die folgenden Hash-Werte auf:

MD5 checksum: 88746e861790fea1ebd4dcdfc39b4e60

SHA1 checksum: 28e7672958273cfacf0ca39fa631c6c4276af35f

PASS

Eine Veränderung des Datenträgers fand in keinem der durchgeführten Tests statt.

4.1.7.5 Sicherung weiterer Medien / Ergebnisse

Im weiteren Testverlauf wurden die vorhandenen Testmedien nach dem beschriebenen Verfahren gesichert. Die Verbindung zu den Medien Seagate ST500DM002_1 und Western Digital WD500BPVT konnte über eine SATA / USB Brücke und ein zusätzliches Netzteil bewerkstelligt werden.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Imation Nano 2GB	Sicherung 1:	0:01:58
	Sicherung 2:	0:01:57
	Sicherung 3:	0:01:58
	Durchschnitt:	0:01:58
Emtec USB 2.0 Stick 8GB	Sicherung 1:	0:12:35
	Sicherung 2:	0:12:33
	Sicherung 3:	0:11:59
	Durchschnitt:	0:12:22
Sandisk Ultra 32GB	Sicherung 1:	0:17:32
	Sicherung 2:	0:17:36
	Sicherung 3:	0:17:37
	Durchschnitt:	0:17:35
Western Digital WD500BPVT	Sicherung 1:	2:11:00
	Sicherung 2:	2:11:03
	Sicherung 3:	2:11:02
	Durchschnitt:	2:11:02
Seagate ST500DM002_1	Sicherung 1:	1:49:34
	Sicherung 2:	1:48:55
	Sicherung 3:	1:48:49
	Durchschnitt:	1:49:06

Eine Überprüfung des WiebeTech USB 3.1 WriteBlockers über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit PASS quittiert:

Summary

PASS — No sectors on the drive were modified during the test.

Results

Unmodified Sectors	34
Modified Sectors	0
Commands Not Supported	19
Commands Not Enabled	0
Incomplete Commands	2
Errors	0
Skipped	0

Options

Force commands	False
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	False

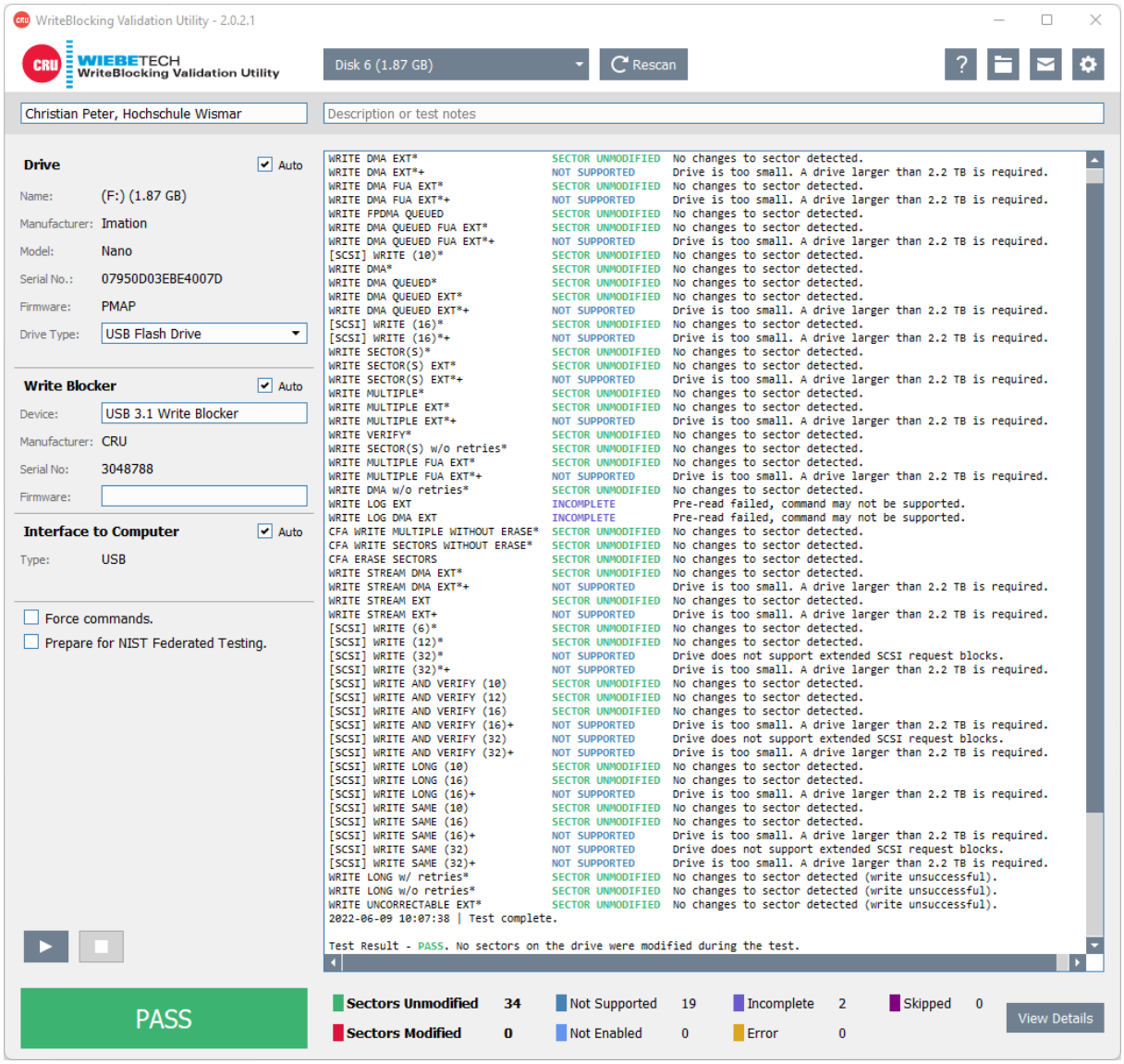

Bild 52: WiebeTech USB – geblockte Schreibzugriffe

4.1.8 Tableau T3iu Forensic SATA Imaging Bay

Auch bei dem Tableau T3iu Forensic SATA Imaging Bay Adapter handelt es sich um einen forensischen Write-Blocker. Als aktueller Listenpreis wird in Europa 350€ angegeben. (Stand: Juni 2022).

Vorgesehen ist die Verwendung des Gerätes in einem 5,25“ Schacht eines klassischen Tower-PCs. Die Verbindung erfolgt dabei über den Mainboard-USB3.0 Port oder klassisch über ein USB3.0 Kabel, welches über die Rückseite des PC nach Außen geführt wird. Über den USB3.0 Anschluss lässt sich das Gerät jedoch auch extern verwenden. Dabei ist eine geeignete Stromquelle mit SATA-Power Anschluss erforderlich.

Bild 53: Tableau T3iu Forensic SATA Imaging Bay mit Test-Medium

Für die Verwendung des Gerätes war keine gesonderte Treiber-Installation notwendig. Nach dem Einsetzen des Mediums und der Betätigung des Power Schalters wurde das Medium unter Windows und Linux erkannt. Ein Betrachten der Daten gelang jedoch nur unter Linux (Manjaro KDE 21.2.6). Unter Windows wurde beim Versuch, das Medium einzusehen eine Fehlermeldung ausgegeben:

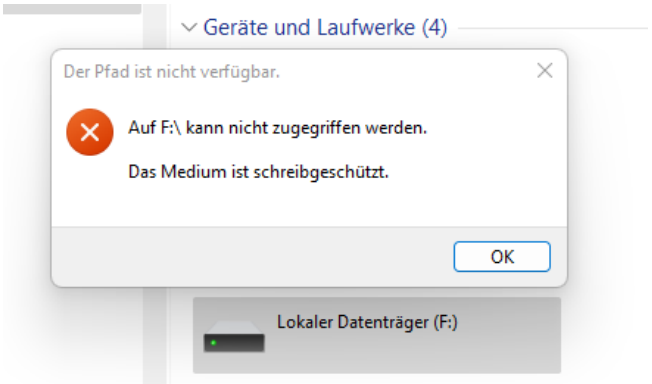

Bild 54: Tableau – Ausgabe einer Fehlermeldung beim Aufruf des Datenträgers unter Windows

4.1.8.1 Testablauf

Das Medium Western Digital WD500BPVT wurde zunächst in den passenden Einschub des Gerätes eingesetzt. Nach der Verbindung des Netzkabels und des USB-Kabels zum Host-System wurde das Gerät über den Power-Schalter eingeschaltet. Das Test-Medium wurde daraufhin umgehend vom System (Manjaro KDE 21.2.6) erkannt und konnte eingesehen werden.

4.1.8.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen oder von diesem zu löschen, wurden mit einer Fehlermeldung quittiert:

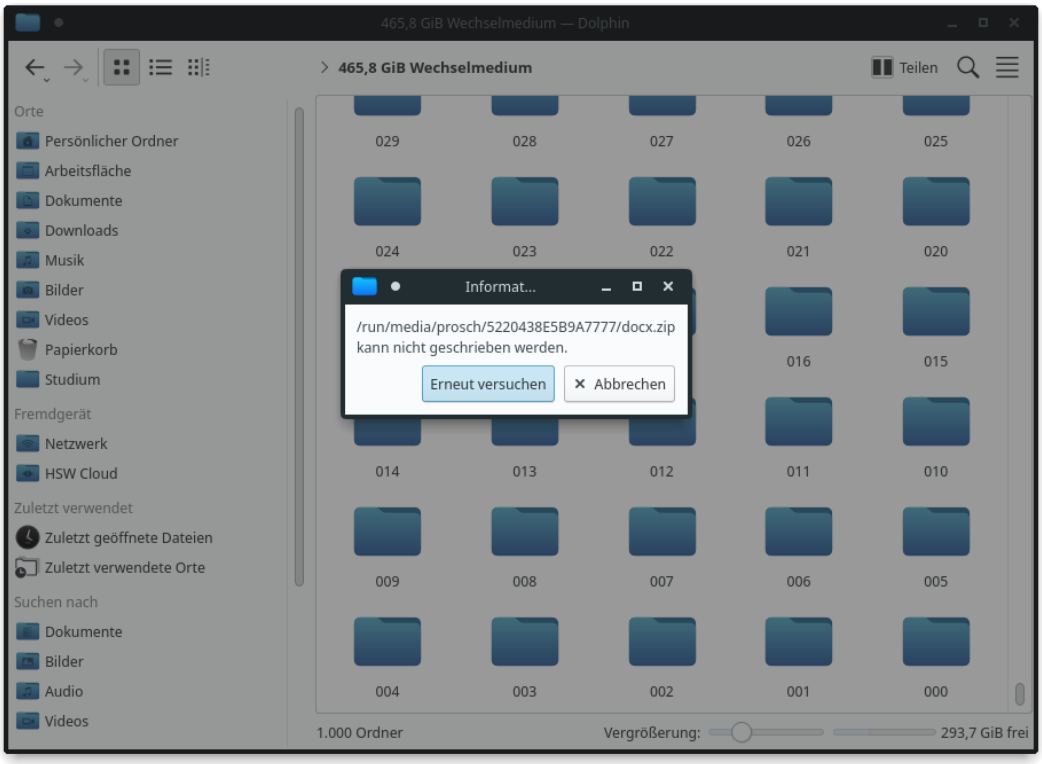

Bild 55: Tableau – Fehlermeldung beim Versuch, eine Datei abzulegen

Die Sicherung in Folge der Dateioperationen wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der Dateioperationen fand nicht statt.

4.1.8.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im NTFS-Format neu zu formatieren. Dabei wurde eine Fehlermeldung ausgegeben, wonach ein Schreibzugriff auf das Medium nicht möglich sei:

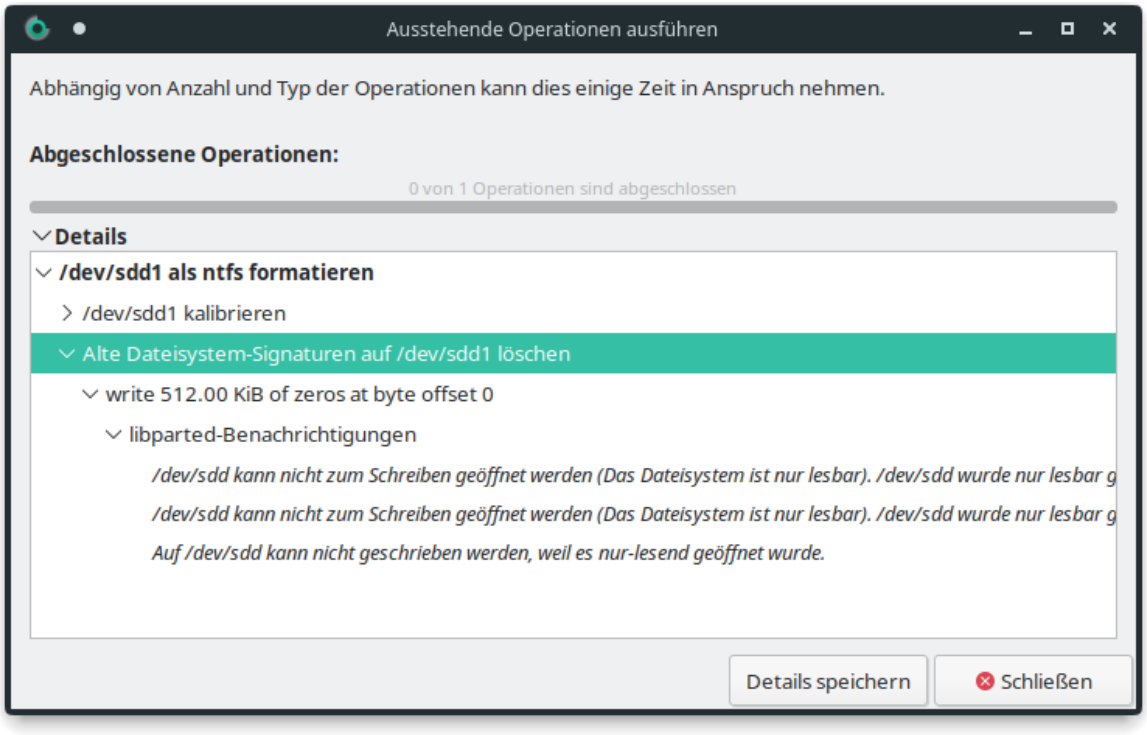

Bild 56: Tableau – Fehlermeldung beim Versuch, den Datenträger zu formatieren

Im Rahmen der zweiten Sicherung wurden folgenden Hash-Werte generiert:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

4.1.8.4 Operationen auf Blockebene / Hexedit:

Versuche, Änderungen am Medium durchzuführen, werden mit dem Hinweis blockiert, dass es sich um ein read-only Device handelt:

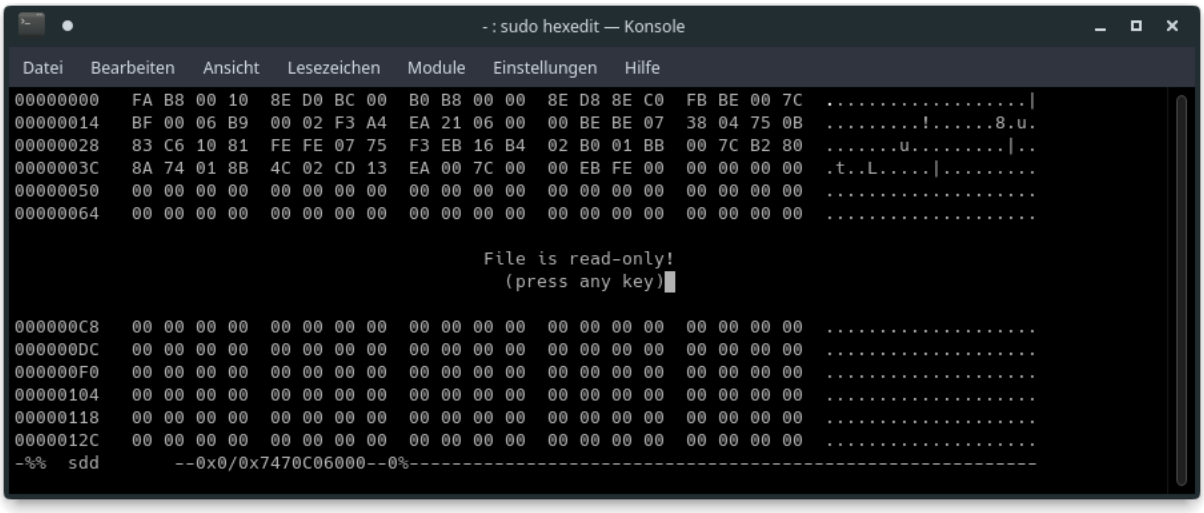

Bild 57: Tableau – Ausgabe eines Fehlers im Hexeditor

Die dritte Sicherung des Datenträgers wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der durchgeführten Tests fand nicht statt.

4.1.8.5 Sicherung weiterer Medien / Ergebnisse

Da Writeblocking über die Tableau T3iu Forensic SATA Imaging Bay nur für die SATA-Schnittstelle bereitgestellt wird, wurden nur die Test-Festplatten gesichert.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Western Digital WD500BPVT	Sicherung 1:	1:56:07
	Sicherung 2:	1:49:06
	Sicherung 3:	1:49:01
	Durchschnitt:	1:51:25
Seagate ST500DM002_1	Sicherung 1:	1:20:12
	Sicherung 2:	1:20:31
	Sicherung 3:	1:20:09
	Durchschnitt:	1:20:17

Eine Überprüfung der Tableau T3iu Forensic SATA Imaging Bay über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit PASS quittiert:

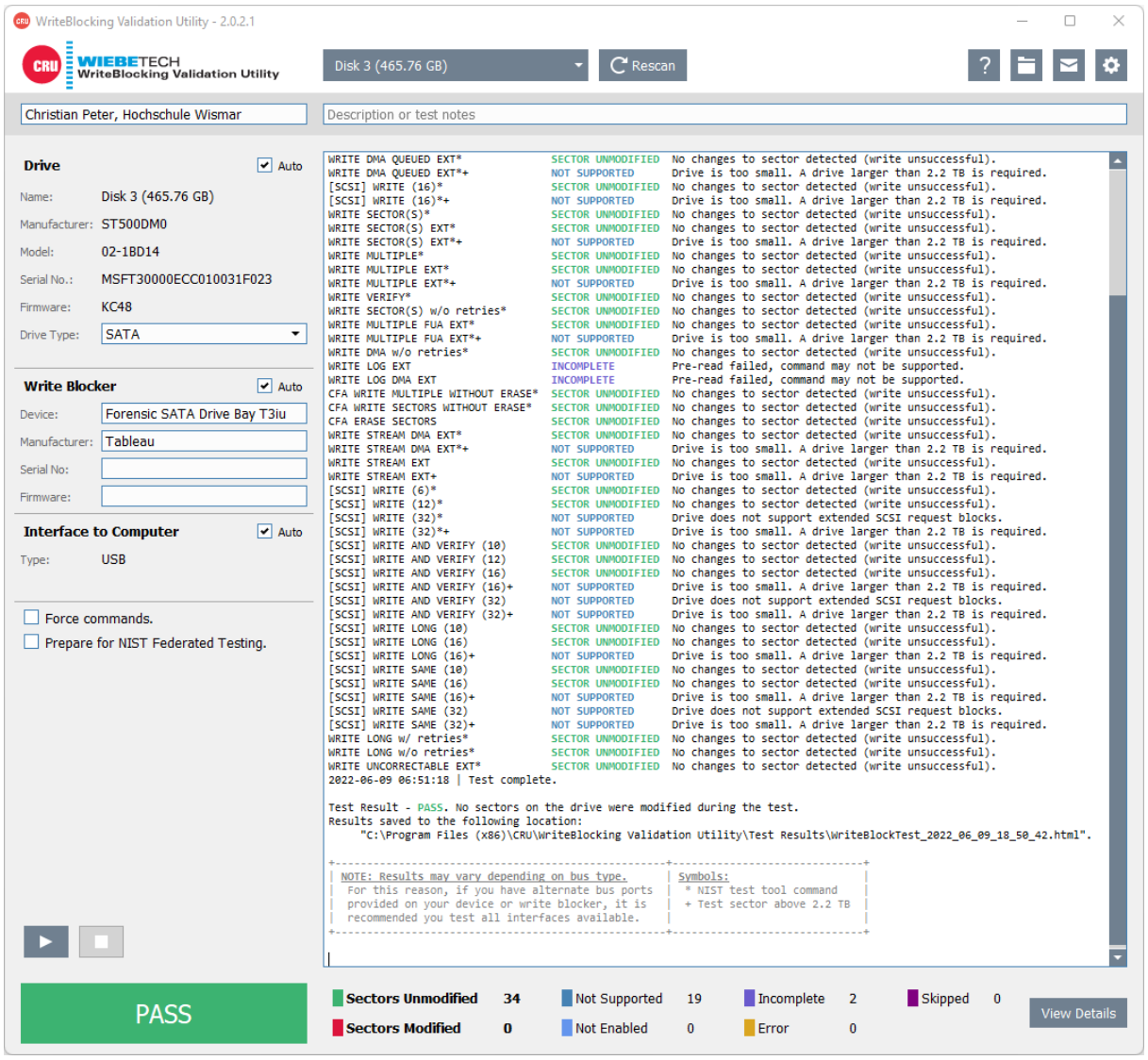

Bild 58: Tableau – geblockte Schreibzugriffe

4.1.9 WiebeTech Forensic Ultradock V5

Bei dem WiebeTech Forensic Ultradock V5 handelt es sich ebenfalls um einen forensischen Write-Blocker. Diese Version des Produkts wird zwar nicht weiter vertrieben. Der Nachfolger Forensic UltraDock FUDv6.0 wird für einen Preis von ca. 446€ angeboten.

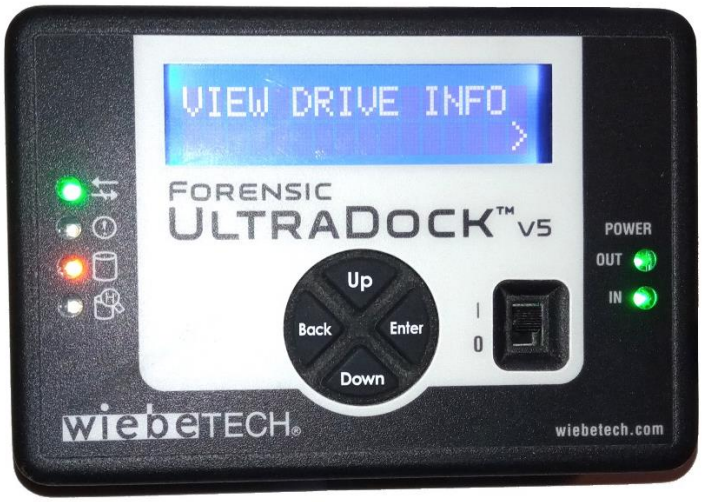

Bild 59: WiebeTech Forensic Ultradock V5

Dieses Gerät bietet ein Display, über welches Informationen zum angeschlossenen Datenträger oder zum Write-Blocker selbst eingesehen werden können.

Eine Treiberinstallation war zum Betrieb des Ultradock nicht notwendig. Nach der Verbindung über USB- und Power-Kabel vermeldet Die Power-IN LED die Betriebsbereitschaft. Die Betätigung des Power Schalters führte nach kurzer Ladezeit zur Bereitstellung des Mediums am Hostsystem.

4.1.9.1 Testablauf

Das Medium Western Digital WD500BPVT wurde zunächst an den Write-Bocker über dessen SATA-Port angeschlossen. Nach der Verbindung des Netzteiles und des USB-Kabels zum Host-System wurde das Test-Medium nach Betätigung des Power Schalters umgehend vom System (Manjaro KDE 21.2.6) erkannt und konnte eingesehen werden.

4.1.9.2 Dateioperationen:

Versuche, Dateien auf dem Datenträger abzulegen oder von diesem zu löschen, wurden augenscheinlich durchgeführt:

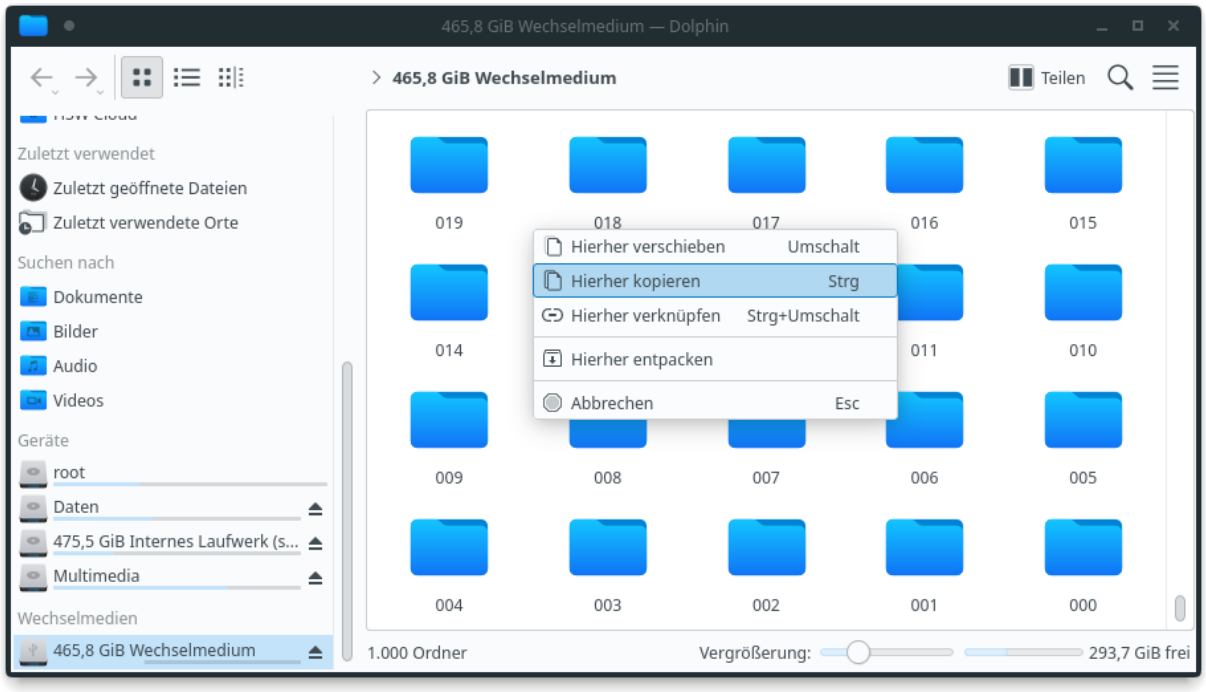

Bild 60: Ultradock – Kopieren von Dateien ist augenscheinlich möglich

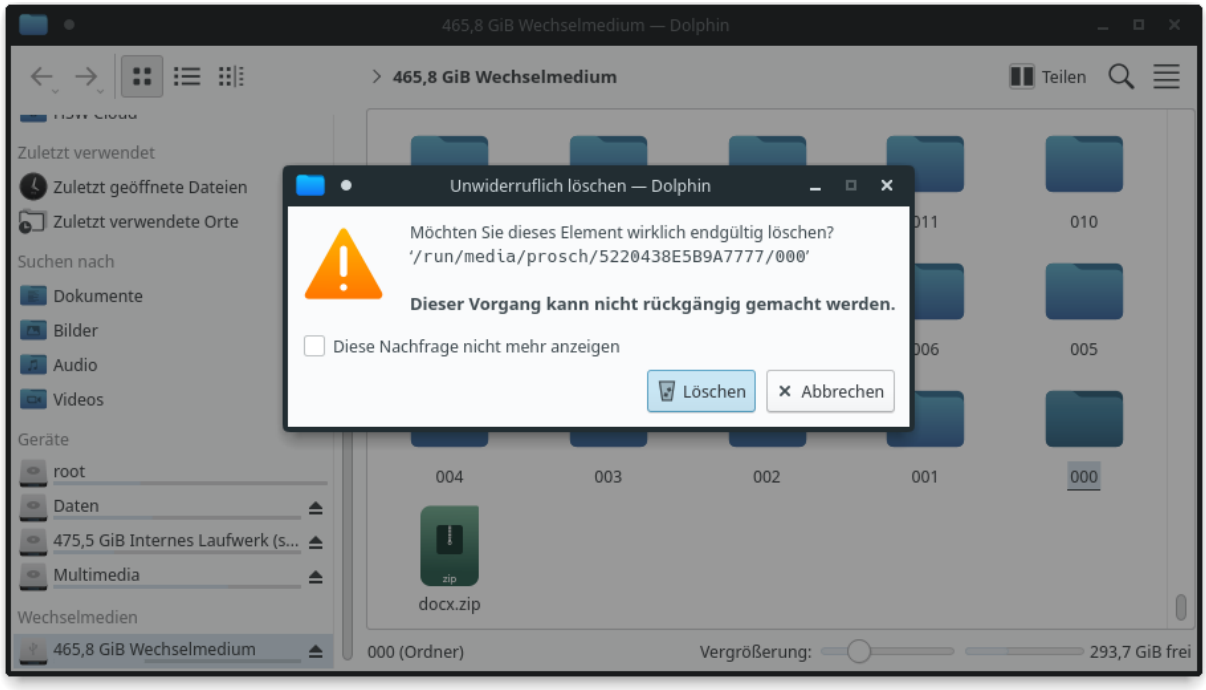

Bild 61: Ultradock – Löschen von Dateien ist augenscheinlich möglich

Die Sicherung in Folge der Dateioperationen wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der Dateioperationen fand nicht statt.

4.1.9.3 Formatierung / Partitionierung:

Es wurde versucht, den Datenträger mittels der Software GParted im NTFS-Format neu zu formatieren. Diese Operation wurde augenscheinlich durchgeführt:

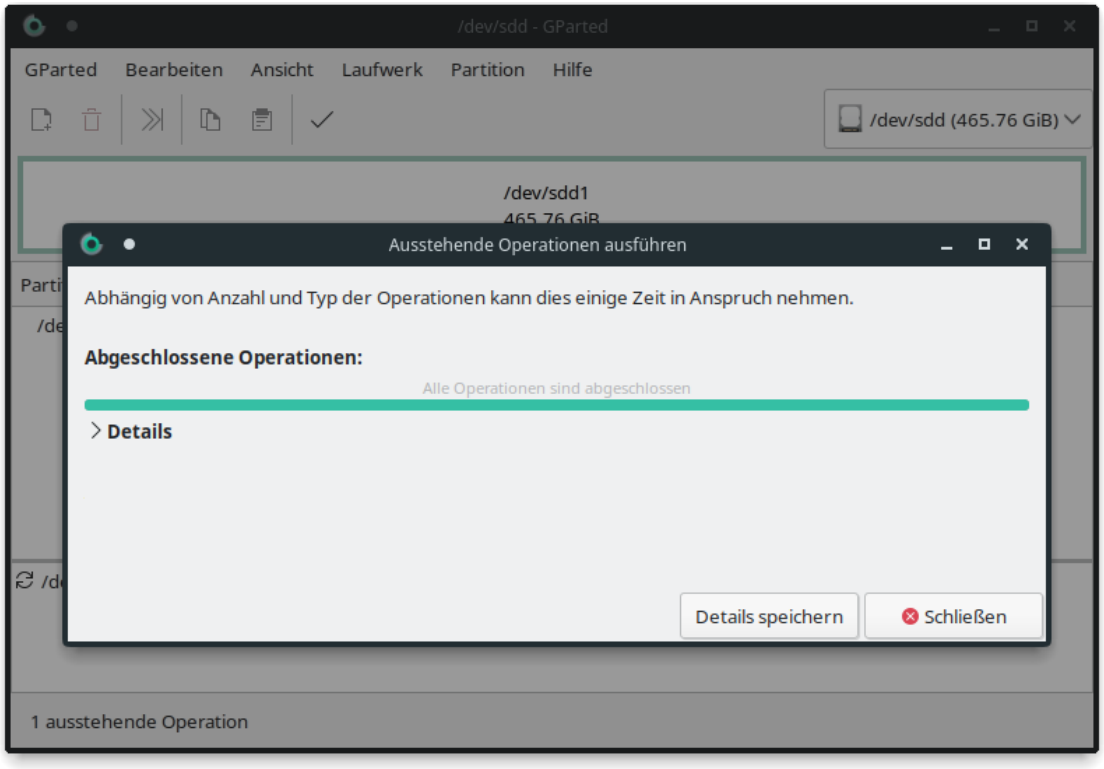

Bild 62: Ultradock – Formatieren ist augenscheinlich möglich

Im Rahmen der zweiten Sicherung wurden folgenden Hash-Werte generiert:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger fand tatsächlich, trotz gegenteiliger Meldungen des Betriebssystems, nicht statt.

4.1.9.4 Operationen auf Blockebene / Hexedit:

Es wurde versucht, mittels der Software Hexedit das erste Wertepaar des eingelesenen Datenträgers zu editieren. Dabei wurde der Wert FA durch 1A ersetzt. Beim Beenden der Software meldet diese keinen Fehler beim Speichern der Datei:

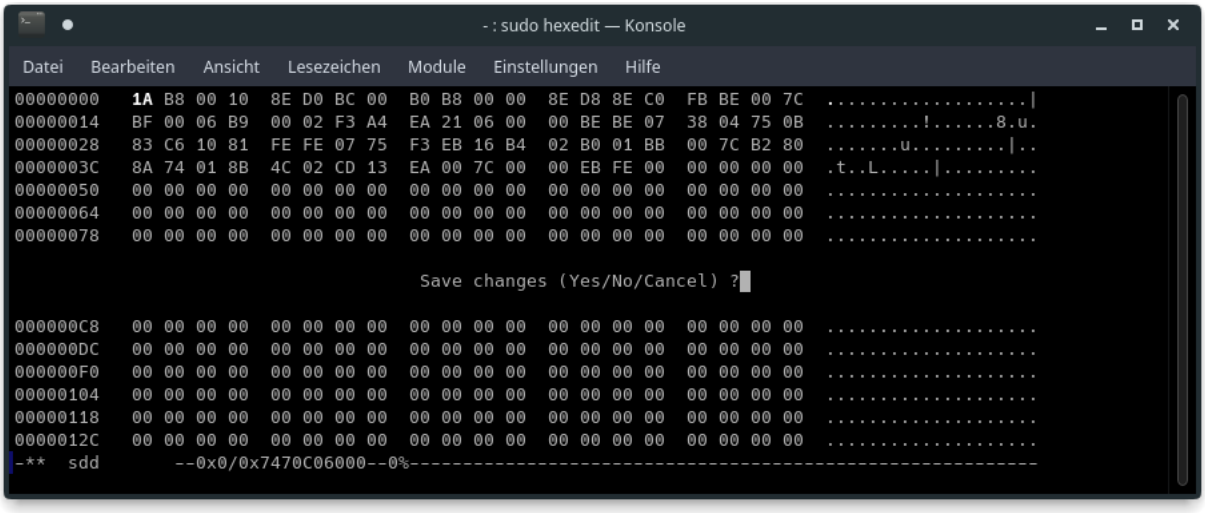

Bild 63: Ultradock – Änderungen über den Hexeditor werden augenscheinlich geschrieben

Ein erneutes Aufrufen des Gerätepfades über den Hexeditor zeigt hingegen wieder den ursprünglichen Wert.

Die dritte Sicherung des Datenträgers wies folgende Hash-Werte auf:

MD5 checksum: a62ea7f89c14c7f921124c598893a99f

SHA1 checksum: 82198285ffe1226f1db9333e557a8ac1a63ad99e

PASS

Eine Veränderung am Datenträger in Folge der durchgeführten Tests fand nicht statt.

4.1.9.5 Sicherung weiterer Medien / Ergebnisse

Da Writeblocking über den WiebeTech Forensic Ultradock V5 nur für die SATA-Schnittstelle bereitgestellt wird, wurden nur die Test-Festplatten gesichert.

Bei der Sicherung der Testmedien wurden folgende Zeiten erreicht (h/m/s):

Western Digital WD500BPVT	Sicherung 1:	2:03:12
	Sicherung 2:	1:49:19
	Sicherung 3:	1:49:16
	Durchschnitt:	1:53:56
Seagate ST500DM002_1	Sicherung 1:	1:20:29
	Sicherung 2:	1:20:26
	Sicherung 3:	1:20:29
	Durchschnitt:	1:20:28

Eine Überprüfung der Tableau T3iu Forensic SATA Imaging Bay über die CRU WriteBlocking Validation Utility wurde durchgeführt und mit PASS quittiert:

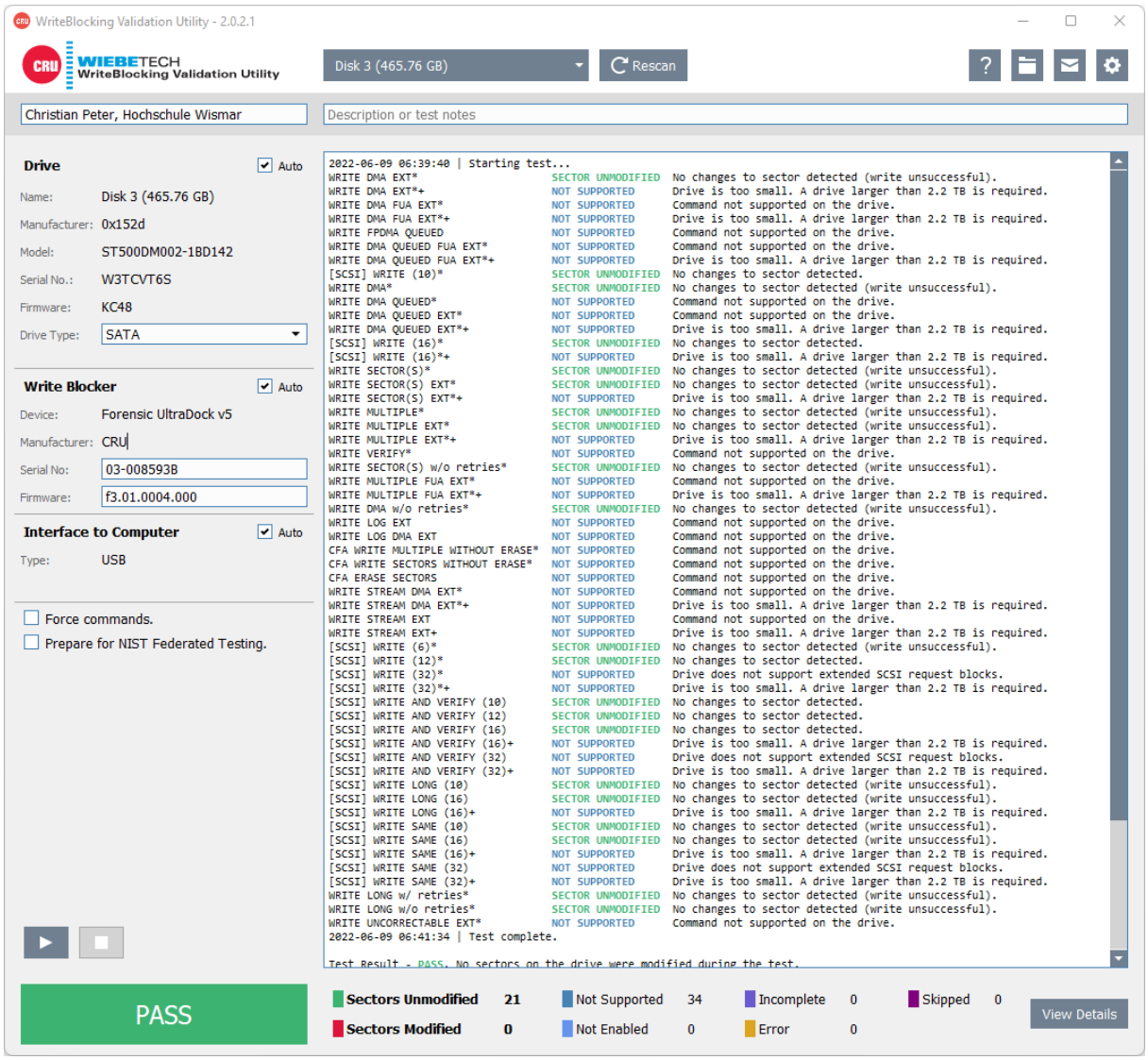

Bild 64: WiebeTech Forensic Ultradock – geblockte Schreibzugriffe

4.2 Software-Writeblocker

Das Host-System zum Testen der Software-Writeblocker in diesem Unterabschnitt ist ein Intel BOXNUC7PJYH2 mit einem Windows 10 Betriebssystem, installiert auf einer SSD (Solid State Drive). Das System besitzt insgesamt vier USB 3.0-Schnittstellen, an denen die Testmedien angeschlossen werden können. Es wird - abgesehen von den bereitgestellten 2,5‘ und 3,5“-Festplatten - keine weitere Hardware zwischen dem Host und dem zu sichernden Medium geschaltet. Zum Anschluss der Festplatten wird der USB 3.0-kompatible USB/SATA-Adapter ICY-BOX IB-AC704-6G genutzt.

Zu den genutzten Software-Writeblocker werden native Möglichkeiten der Betriebssysteme Microsoft Windows und LINUX (in diesem Fall TSURUGI) sowie mit SAFEBlock der Fa. ForensicSoft eine proprietäre Softwarelösung zusätzlich getestet.

4.2.1 Windows Registry Key

Windows bietet nativ die Möglichkeit, anhand eines Registry Keys das Standardverhalten von extern angeschlossenen Speichermedien anzupassen. Im Registry Tree

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

wird durch den Schlüssel *WriteProtect* als REG_DWORD der Schreibschutzmechanismus aktiviert. Der Wert 1 aktiviert den standardmäßigen „read-only“-Modus bei neu angeschlossenen externen Speichermedien. Ein schreibender Zugriff sollte fortan nicht mehr gestattet sein. (15)

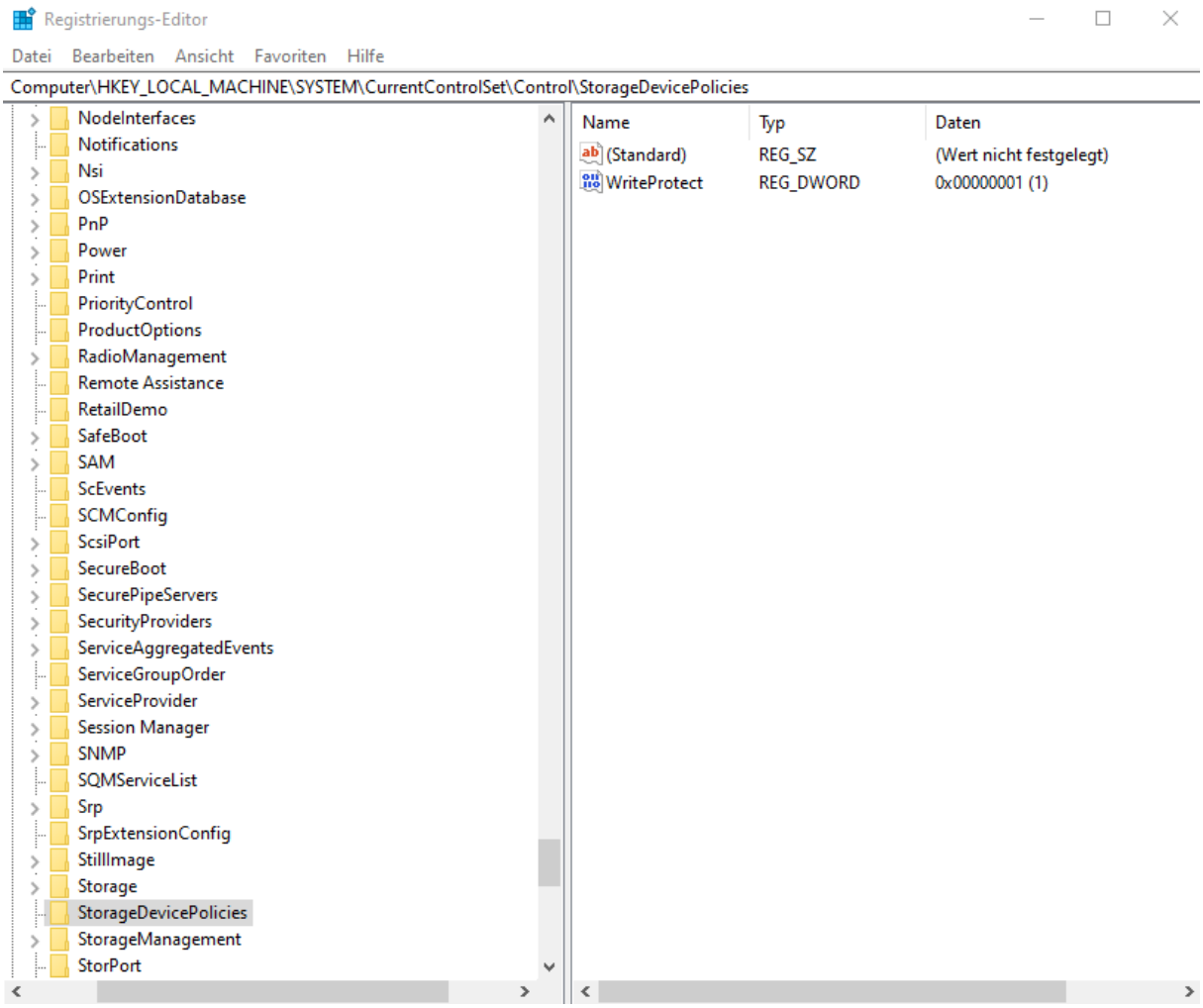

Bild 65: Regedit – WriteProtect Eintrag

4.2.1.1 Dateioperationen

Der eingerichtete Schreibschutz wird hinsichtlich Dateioperationen getestet. Es war nicht möglich, Dateien auf das Medium zu transferieren oder zu löschen. Das Bearbeiten von Dateien war ebenfalls nicht möglich. Jeweils wurde vom System zurückgemeldet, dass das Medium schreibgeschützt ist und ein Speichern nicht möglich ist.

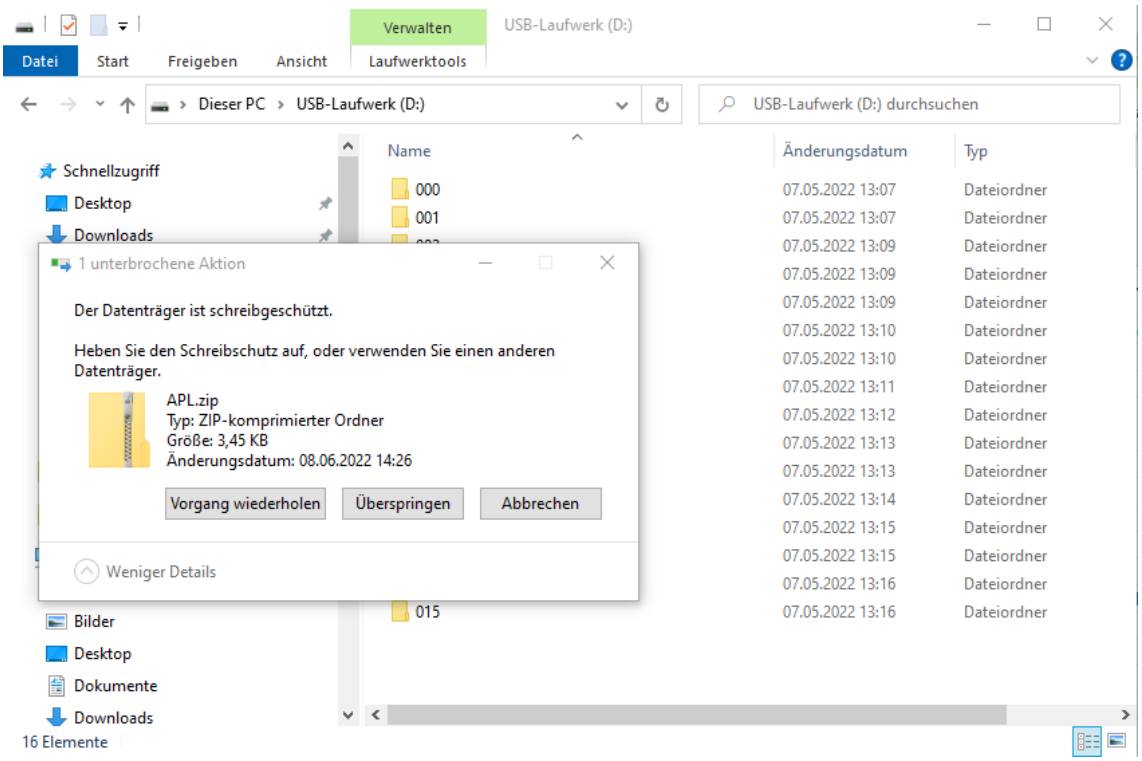

Bild 66: geblockte Schreibzugriffe nach setzen des Regedit Eintrags

Nach den versuchten Dateioperationen wurde ein Image von dem Speichermedium erstellt. Die Hashwerte stimmen mit dem ursprünglichen Hashwert überein.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Datei-OP	f4bc5f9fa365c3aa076a11c38514c78f	

4.2.1.2 Versuch der Partitionierung

Es wird versucht, das Medium zu partitionieren. Der Partitionierungsversuch über die grafische Oberfläche scheiterte mit dem Hinweis, dass der Datenträger schreibgeschützt ist. Mittels DISKPART war es jedoch möglich, die Partition zu löschen und somit schreibend beziehungsweise manipulierend trotz der Einstellung „WriteProtect“ auf den Datenträger einzuwirken. Hierfür wurde in DISKPART versucht, die Partition des Speichermediums zu löschen.

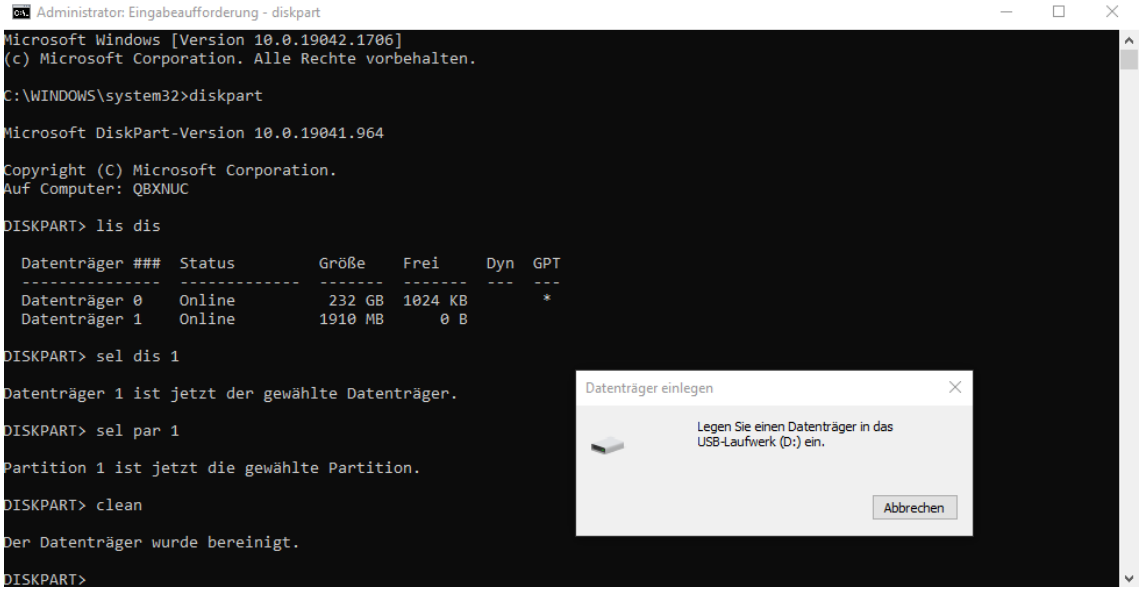

Bild 67: Regedit – erfolgreiche Partitionierung mit Diskpart

Die Partition konnte mit admistriativen DISKPART-Befehlen trotz aktiviertem „WriteProtect“ gelöscht werden. Der Datenträger weist ferner im Explorer keine einsehbaren Partitionen und Dateien mehr auf. Es ist festzustellen, dass die Registry-Einstellung „WriteProtect“ keinen hundertprozentigen Schreibschutz bietet. Ein anschließend generiertes Image des formatierten Datenträgers bestätigt Veränderungen hinsichtlich der Integrität.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	FAIL
Hash nach Formatierungs-versuch	090cd04df9bbf30d88b925089fa7d1a0	

Der Datenträger wurde mittels des Backups wieder auf seinen Ursprungszustand zurückgespielt.

4.2.1.3 Operationen auf Blockebene / Hexedit:

Es wird geprüft, ob Manipulationen von Bytes mittels eines Hex-Editors möglich sind. Mit dem Hex-Editor HxD urde das angeschlossene Speichermedium eingelesen und im Sektor 3119250 ab dem Offset 5F12490 eine zufällig generierte Bytefolge eingefügt. Eine Speicherung mittels des Editors war möglich.

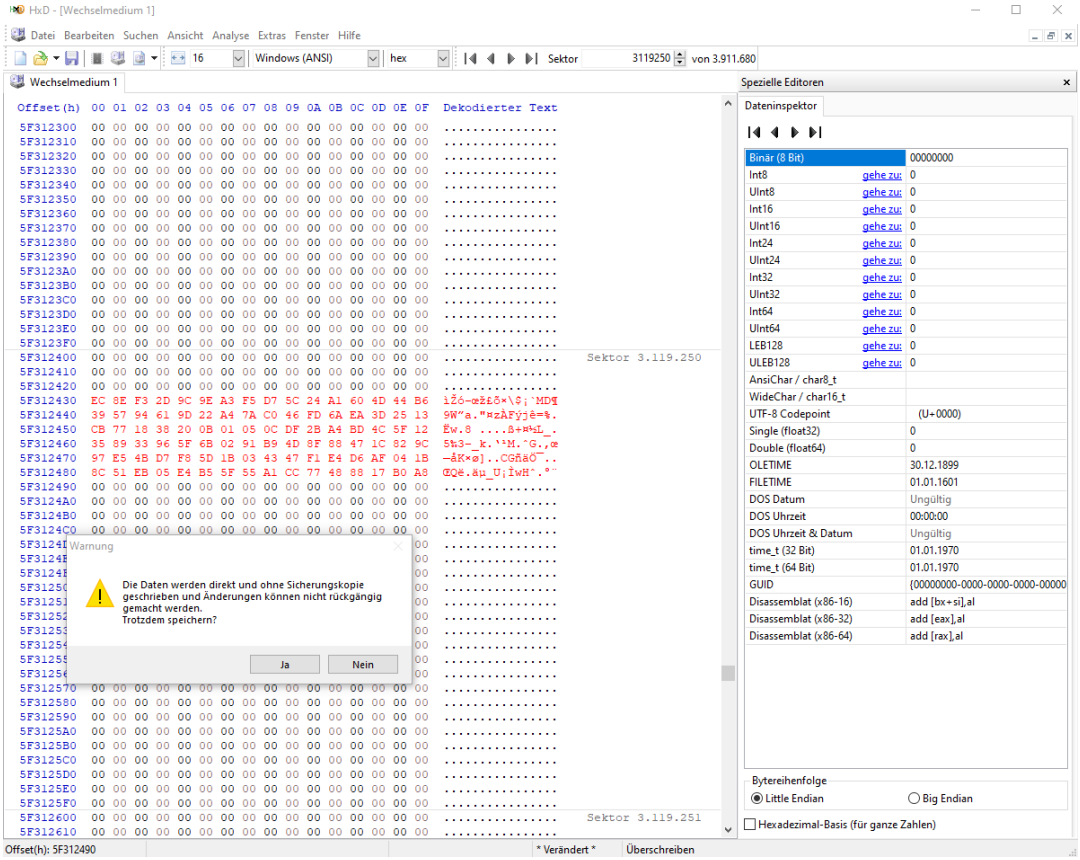

Bild 68: Speichern der Veränderungen über HxD

Eine anschließende Sicherung offenbart, dass sich der Hashwert verändert hat. Die WriteProtect-Funktion unterbindet diese Art des Schreibzugriffes nicht.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	FAIL
Hash nach Hex-Edit	b9b1ea77d493db362edd7451bcb8ac26	

4.2.1.4 NIST / CRU Write Blocker Validation Tool

Der Schreibschutz mittels Registry Key wird folgend mit dem CRU Writeblocking Validation Tool (Ver. 2.0.2.1) am USB-Stick imation überprüft. Der WriteBlock mittels Registry Key hat den Test nicht bestanden. Es konnten durch die automatisierten Testcommands zwei Sektoren modifiziert werden.

Summary

FAIL Sectors on the drive were modified during the test.

Results

Unmodified Sectors	20
Modified Sectors	2
Commands Not Supported	19
Commands Not Enabled	0
Incomplete Commands	14
Errors	0
Skipped	0

Options

Force commands	False
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	False

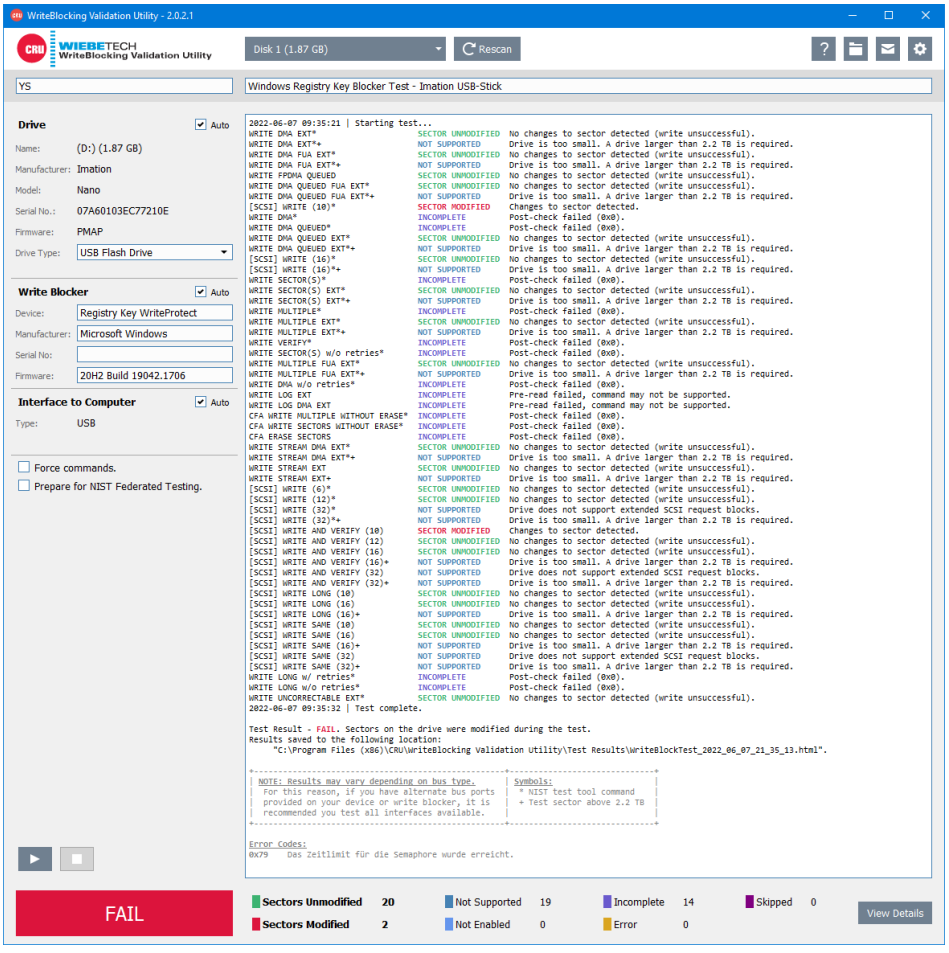

Bild 69: Regedit – geblockte Schreibzugriffe

Eine anschließende, erneute Sicherung des USB-Sticks offenbart eine Abweichung vom ursprünglichen Hashwert des Originals.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	FAIL
Hash nach CRU Validation	9e23e54eb3fa6cd543fa7892042bea4b	

4.2.1.5 Performance

Imation Nano 2GB:	Sicherung 1:	0:02:02
	Sicherung 2	0:02:01
	Sicherung 3:	0:01:59
	Durchschnitt:	0:02:01
Emtec USB2.0 Stick 8GB:	Sicherung 1:	0:09:38
	Sicherung 2	0:09:35
	Sicherung 3:	0:09:35
	Durchschnitt:	0:09:36
SanDisk Ultra 32GB:	Sicherung 1:	0:07:24
	Sicherung 2	0:07:30
	Sicherung 3:	0:07:36
	Durchschnitt:	0:07:30
Western Digital WD500BPVT:	Sicherung 1:	2:00:46
	Sicherung 2	2:00:54
	Sicherung 3:	2:00:55
	Durchschnitt:	2:00:52
Seagate ST500DM002_1:	Sicherung 1:	1:24:48
	Sicherung 2	1:28:52
	Sicherung 3:	1:23:58
	Durchschnitt:	1:25:58

4.2.1.6 Erkenntnisse

Der Schreibschutz mittels Registry Key WriteProtect bietet aus IT-forensischer Sichtweise offensichtlich nur einen rudimentären Schutz vor einer Veränderung des Speichermediums. Während es einfache Dateioperationen durchaus unterbindet, kann das Medium trotzdem durch Formatierung oder zielgerichtete Manipulationen durch einen Hex-Editor verändert werden. Diese Schreibschutzmethode hat die Tests des CRU WriteBlocking Validation Tools nicht bestanden.

4.2.2 SAFE Block Software-WriteBlocker

SAFEBlock ist ein unter Microsoft Windows installierbarer, proprietärer Software-Write-Blocker der Fa. ForensicSoft.

Das Unternehmen bewirbt sein Produkt als erste und einzige kommerziell verfügbaren Windows Write-Blocker. Ferner sei er im Vergleich zu physischen Write-Blockern deutlich schneller in der Sicherung und mit 549 Dollar preiswerter (16). Für diese Projektarbeit wird mit der kostenlos verfügbaren Testlizenz gearbeitet.

SAFEBlock bietet nach der Installation an, angeschlossene Geräte automatisch den Schreibzugriff zu blockieren. Geräte werden über die grafische Oberfläche aufgelistet, wo sie gegebenenfalls auch in einen schreibenden Zustand entsperrt werden können. Vorteilhaft ist ferner, dass softwareseitig keine Begrenzung der blockierbaren Speichermedien existiert. Die vier verfügbaren USB-Ports des Testsystems können beispielsweise mit einem USB-Hub erweitert werden.

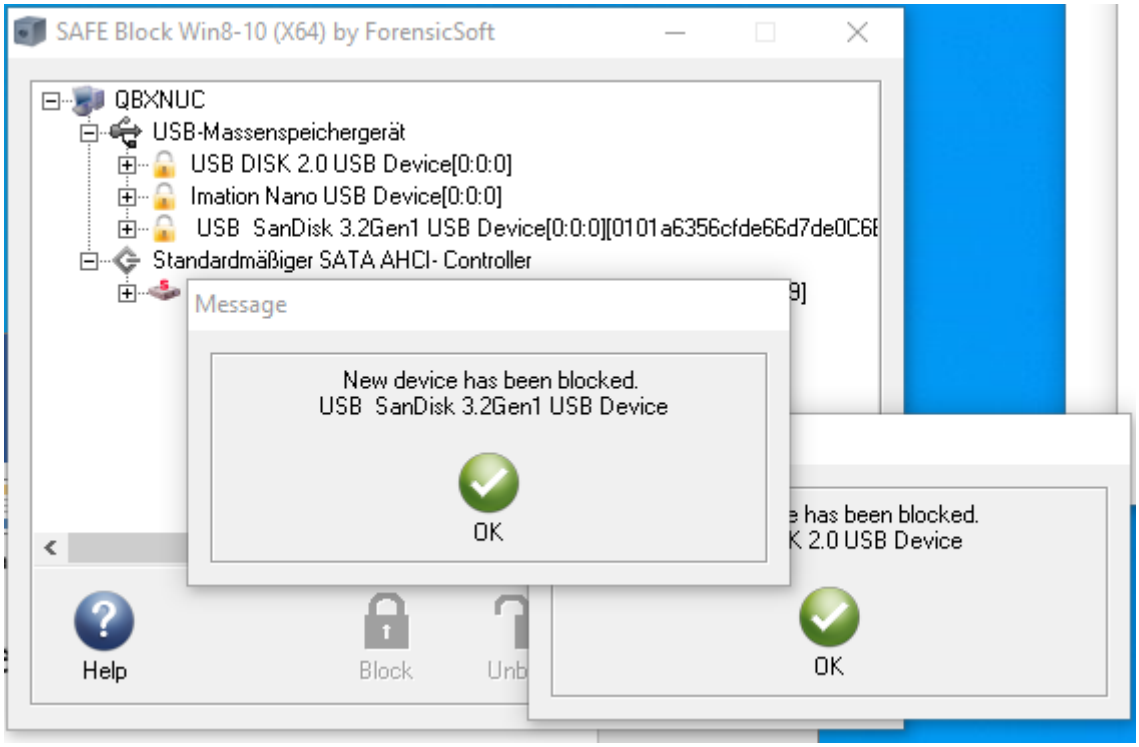

Bild 70: SAFE Block

4.2.2.1 Dateioperationen

Dateioperationen wurden jeweils mit der Fehlermeldung unterbunden, dass das angeschlossene Laufwerk schreibgeschützt sei. Es konnten keine Dateien verschoben, gelöscht oder modifiziert werden.

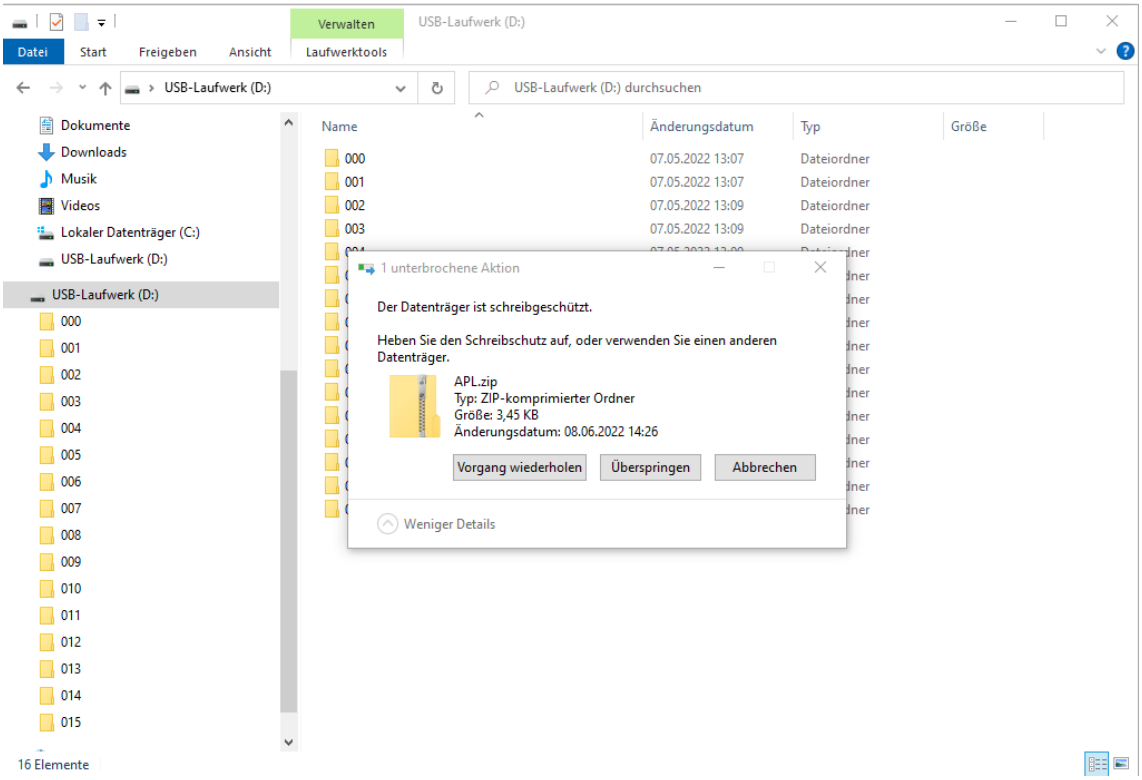

Bild 71: SAFE Block – geblockte Schreibzugriffe auf Dateiebene

Eine erneute Sicherung nach den versuchten Dateioperationen bestätigt die Integrität zum ursprünglich erzeugten Medium.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Datei-OP	f4bc5f9fa365c3aa076a11c38514c78f	

4.2.2.2 Versuch der Partitionierung

Eine Formatierung des Mediums war mittels administrativer DISKPART-Commands nicht möglich. Löschaktionen oder Neuformatierungen werden mit einer Fehlermeldung quittiert, dass das Medium schreibgeschützt sei.

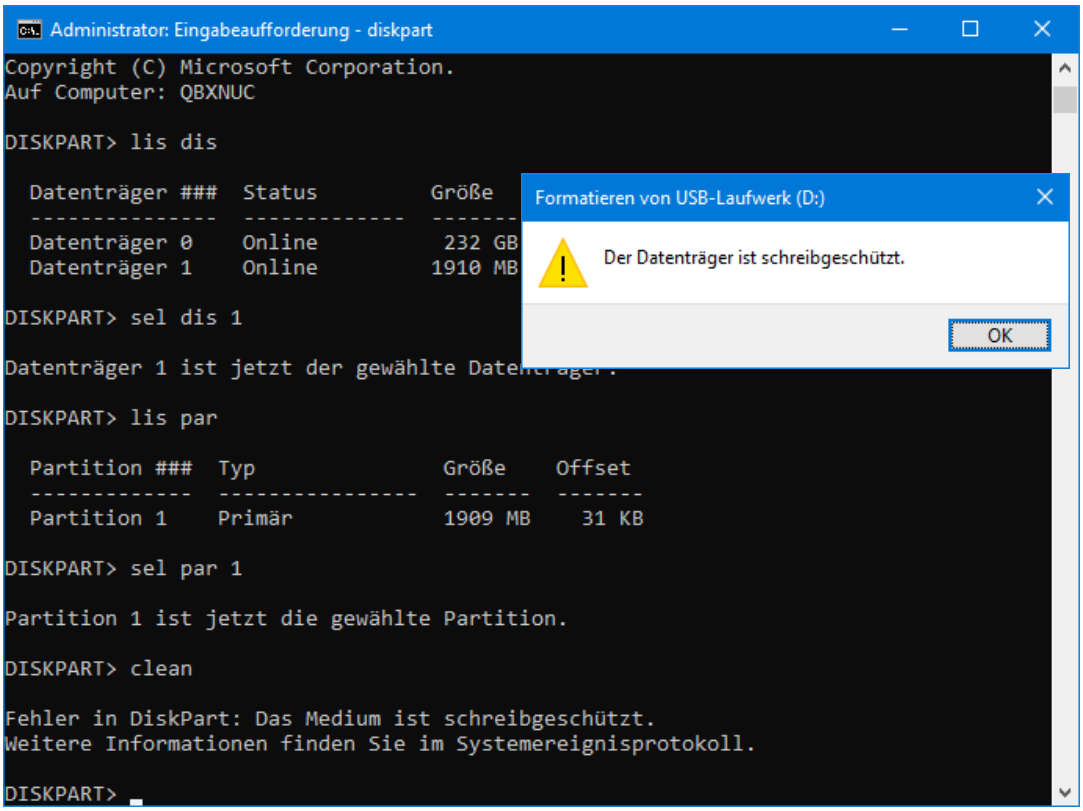

Bild 72: SAFE Block – geblockter Partitionierungsversuch

Durch die anschließende Sicherung des Mediums konnten keine Veränderungen aufgrund des unveränderten Hashwertes nachgewiesen werden.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Formatierungs-versuch	f4bc5f9fa365c3aa076a11c38514c78f	

4.2.2.3 Operationen auf Blockebene / Hexedit:

Mit dem Hex-Editor HxD (Ver) wurde das angeschlossene Speichermedium eingelesen und im Sektor 3366569 ab dem Offset 66BD5230 eine zufällig generierte Bytefolge eingefügt. Eine Speicherung mittels des Editors war möglich.

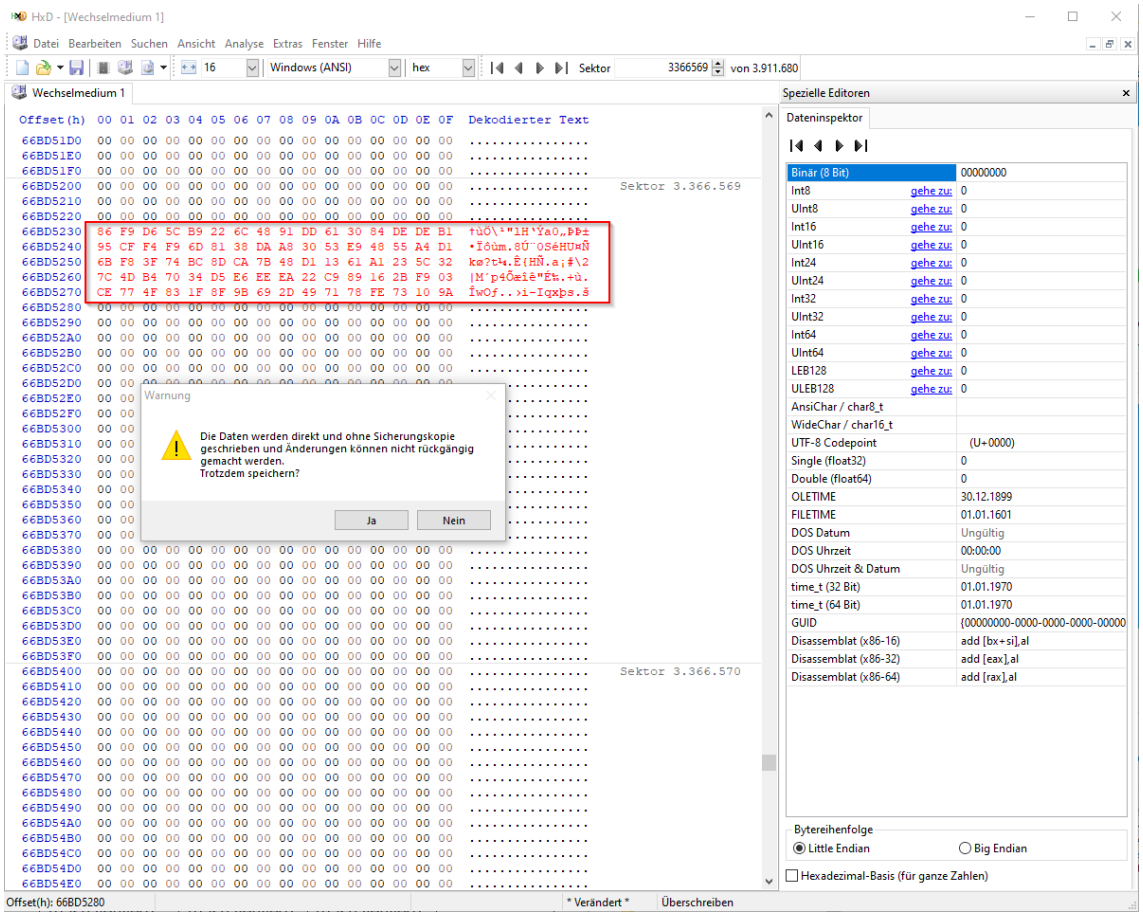

Bild 73: SAFE Block – augenscheinliche Änderungen mittels Hexeditor

Der anschließend bei der Sicherung errechnete Hashwert blieb unverändert zum ursprünglich erstellten Medium. Nach erneutem Einlesen des Datenträgers in HxD und Analyse des manipulierten Sektors war erkennbar, dass der betroffene Bereich unverändert mit Nullen beschrieben war. Eine Manipulation hat nicht stattgefunden, obschon die Bytefolge sich in dem Editor speichern ließ.

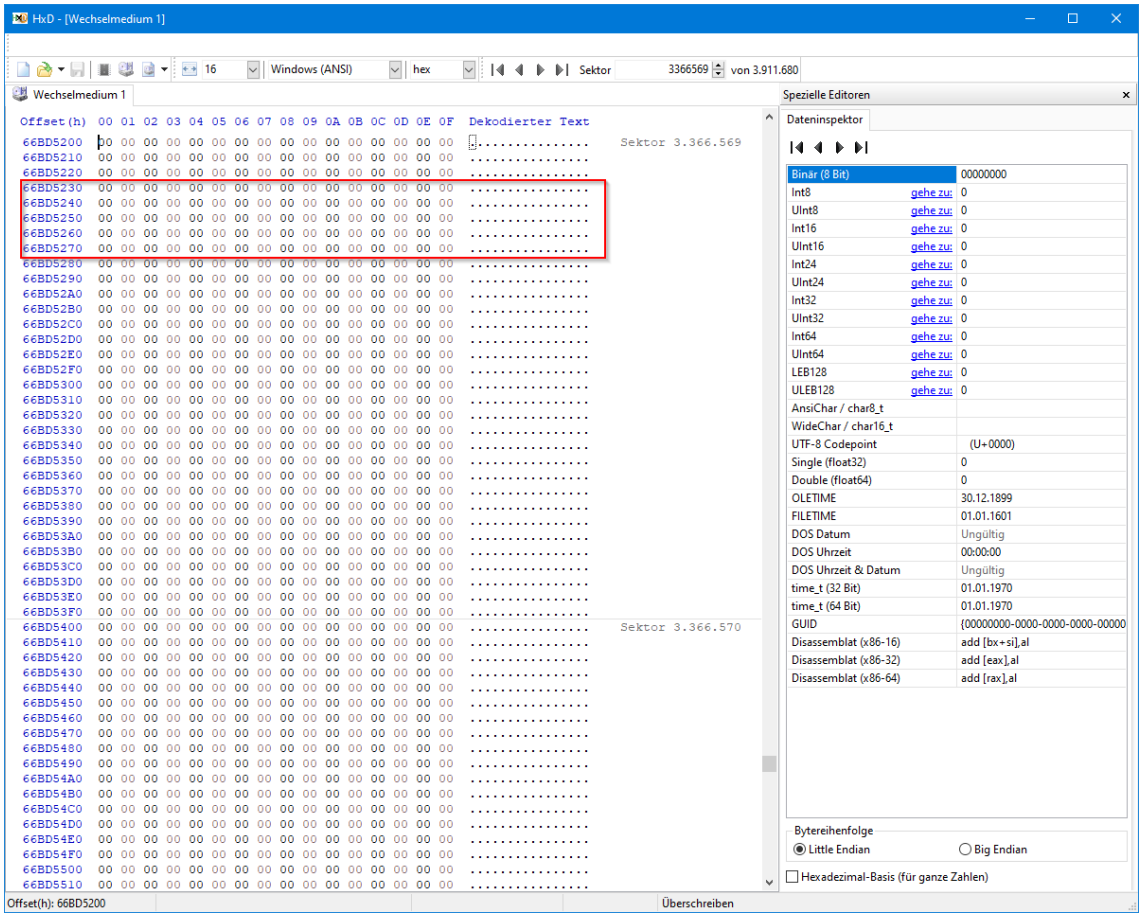

Bild 74: SAFE Block – ursprüngliche Werte in der Hexansicht

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Hex-Edit	f4bc5f9fa365c3aa076a11c38514c78f	

4.2.2.4 NIST / CRU Write Blocker Validation Tool

Der Schreibschutz mittels SAFEBlock wird folgend mit dem CRU Writeblocking Validation Tool (Ver. 2.0.2.1) exemplarisch am USB-Stick Imation überprüft. Der WriteBlock hat den Test bestanden. Es konnten durch die automatisierten Testcommands keine Sektoren modifiziert werden.

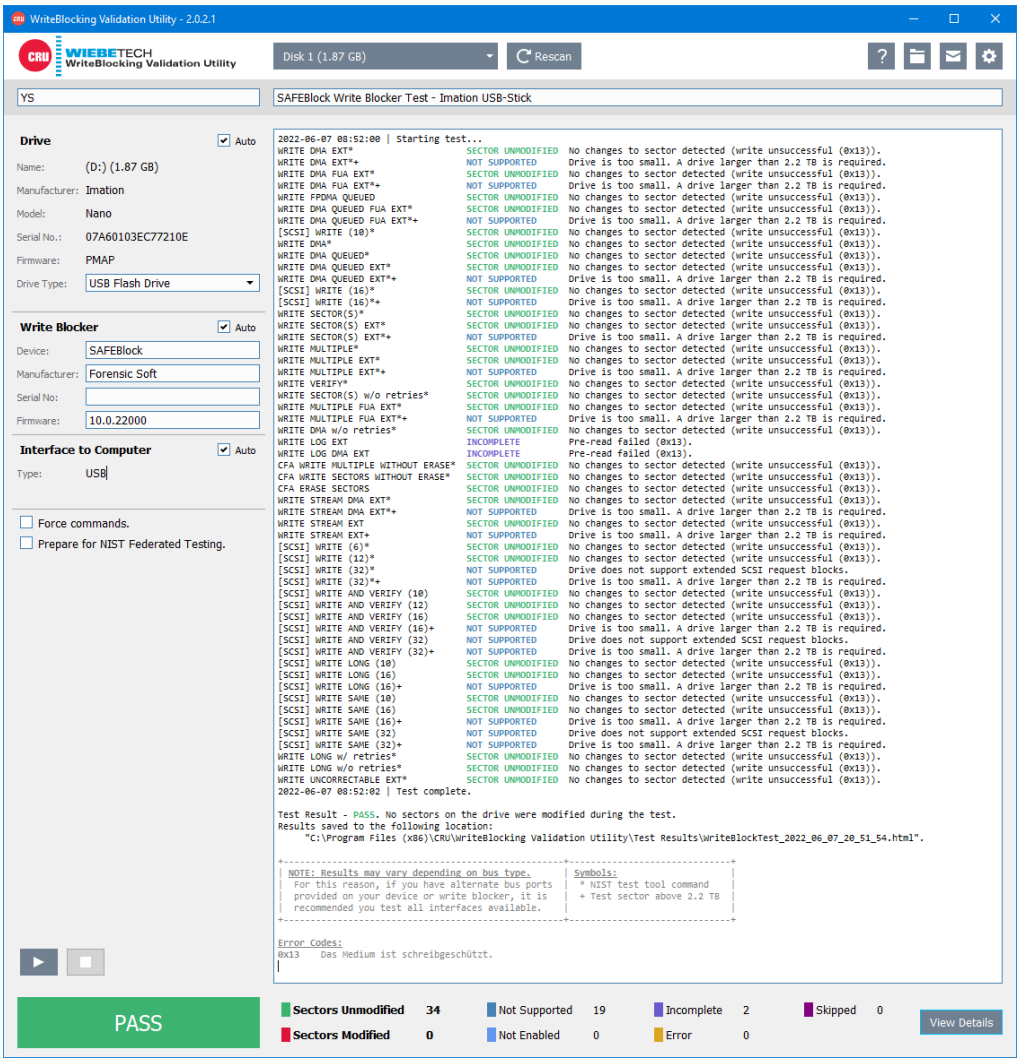

Bild 75: SAFE Block – geblockte Schreibzugriffe

Summary

PASS	No sectors on the drive were modified during the test.

Results

	Unmodified Sectors	**34**
	Modified Sectors	**0**
	Commands Not Supported	19
	Commands Not Enabled	0
	Incomplete Commands	2
	Errors	0
	Skipped	0

Options

Force commands	False
Test sectors above 2.2 TB (+)	True
Pause after each command	False
Prepare for NIST Federated Testing	False

Eine anschließende, erneute Sicherung des Mediums bestätigt, dass durch die vorangegangenen Tests keine Sektoren verändert wurden. Der Hashwert stimmt weiterhin mit dem ursprünglich, bei der Erzeugung des Mediums errechneten Hashwert überein.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach CRU Validation	f4bc5f9fa365c3aa076a11c38514c78f	

4.2.2.5 Performance

Imation Nano 2GB:	Sicherung 1:	0:01:59min
	Sicherung 2	0:02:04min
	Sicherung 3:	0:02:01min
	Durchschnitt:	0:02:02min
Emtec USB2.0 Stick 8GB:	Sicherung 1:	0:09:24
	Sicherung 2	0:09:39
	Sicherung 3:	0:09:37
	Durchschnitt:	0:09:33
SanDisk Ultra 32GB:	Sicherung 1:	0:07:24
	Sicherung 2	0:07:39

	Sicherung 3:	0:07:35
	Durchschnitt:	0:07:33
Western Digital WD500BPVT:	Sicherung 1:	2:00:51
	Sicherung 2	2:00:44
	Sicherung 3:	2:01:18
	Durchschnitt:	2:00:58
Seagate ST500DM002_1:	Sicherung 1:	1:24:39
	Sicherung 2	1:24:18
	Sicherung 3:	1:23:54
	Durchschnitt:	1:24:17

4.2.2.6 Erkenntnisse

Bei aktiviertem Schreibschutz des SAFEBlock war es in dieser Untersuchung mit keiner der aufgeführten Methode möglich, etwaige Veränderungen an dem angeschlossenen Speichermedium vorzunehmen. Diese Schreibschutzmethode hat ferner die Tests des CRU WriteBlocking Validation Tools bestanden.

4.2.3 Tsurugi Linux

TSURUGI Linux ist ein kostenlos erhältliches Debian-Derivat, das von seiner installierten Software speziell auf die Anwendungszwecke digitaler Forensik zugeschnitten ist. In der Distribution ist ein Schreibschutz kernelseitig installiert (17). Für die folgenden Tests wurde das aktuell verfügbare Tsurugi Linux Lab 2020.1 auf demselben Hostsystem wie für die vorherigen Tests als Live-CD gestartet.

Der vorinstallierte Schreibschutz sorgt dafür, dass jedwede eingesteckten Speichermedien „read-only“ eingebunden werden. Der TSURUGI DEVICE UNLOCKER listet übersichtlich den aktuellen Zustand der eingebundenen Geräte auf.

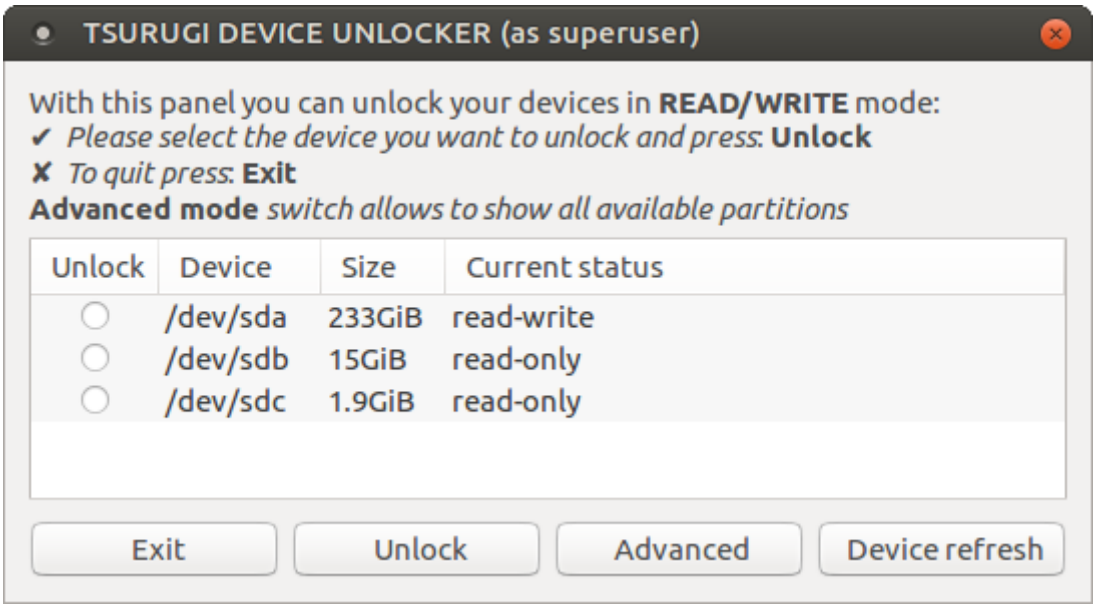

Bild 76: Tsurugi Device Unlocker

4.2.3.1 Dateioperationen

Es wird versucht, im read-only-Status Dateioperationen auf dem Datenträger zu realisieren. Weder grafisch noch per Kommandozeile unter root konnten Dateien verschoben/gelöscht/manipuliert werden.

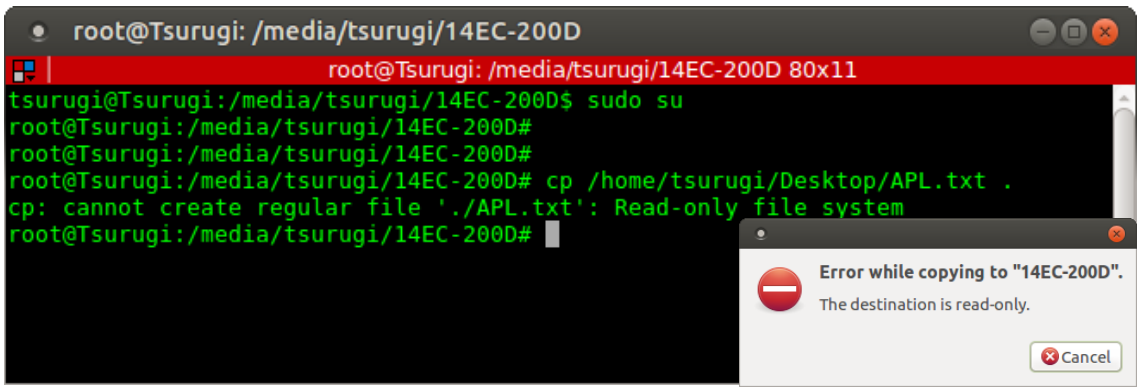

Bild 77: Tsurugi – geblockter Schreibzugriff auf Dateiebene

Die anschließende Sicherung des Mediums zeigt, dass keine Veränderungen am ursprünglichen Zustand zu verzeichnen sind.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Datei-operationen	f4bc5f9fa365c3aa076a11c38514c78f	

4.2.3.2 Versuch der Partitionierung

Mittels gparted, gestartet als superuser, wurde versucht, das Medium zu Formatieren. Es gelang der Zugriff auf das Speichermedium durch das Löschen der Partition. Der gespeicherte Datenbestand war fortan nicht mehr einsehbar.

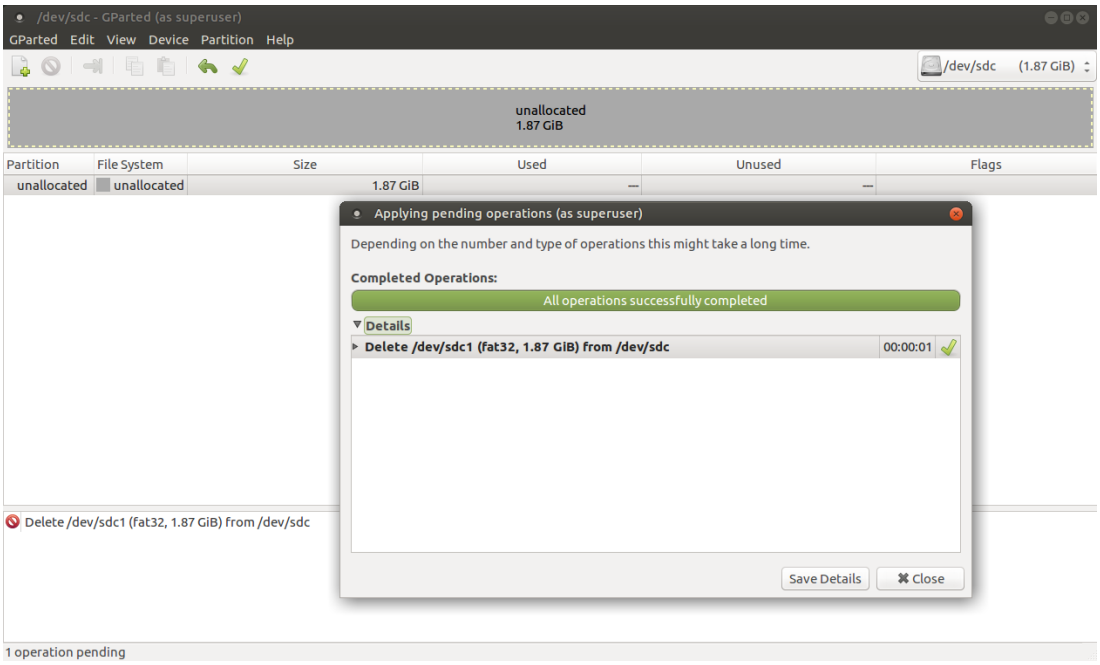

Bild 78: Tsurugi – durchgeführte Partitionierung

Auffallend ist, dass sich nach dieser Operation der Zustand des Geräts von read-only in read-write verändert hat. Ein Schreibschutz ist nicht mehr gewährleistet.

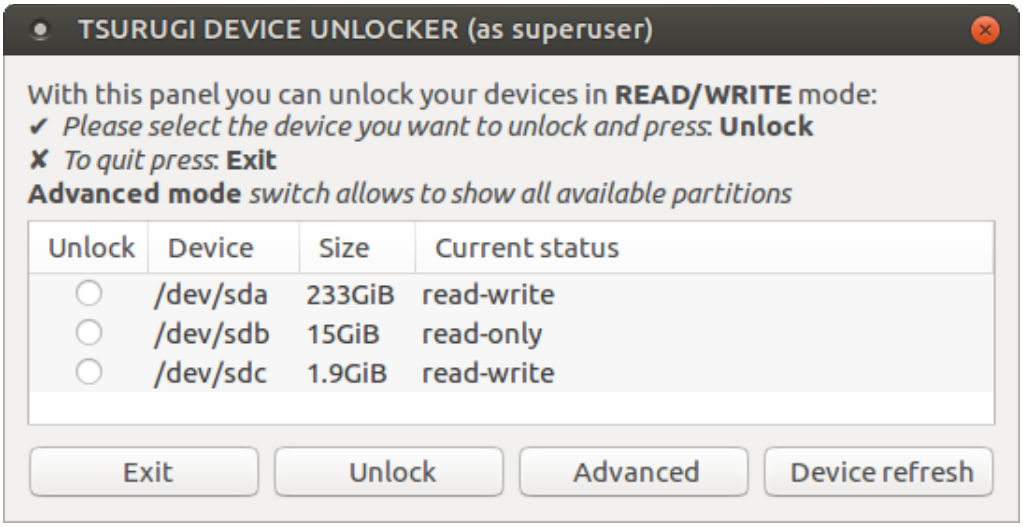

Bild 79: Tsurugi – veränderter Gerätestatus

Die Manipulationen konnten aufgrund des veränderten Hashwertes bei der anschließenden Sicherung belegt werden.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	FAIL
Hash nach Formatierung	63e6476e3a85cb3667a8c67e2b0099b8	

4.2.3.3 Operationen auf Blockebene / Hexedit:

Mit dem vorinstallierten Programm hexedit wurde für das schreibgeschützte Gerät /dev/sdc versucht, eine zufällige Bytefolge ab dem Offset 0x70 einzufügen. Es gelang, die zuvor aus Nullen bestehenden Blöcke zu modifizieren und zu speichern.

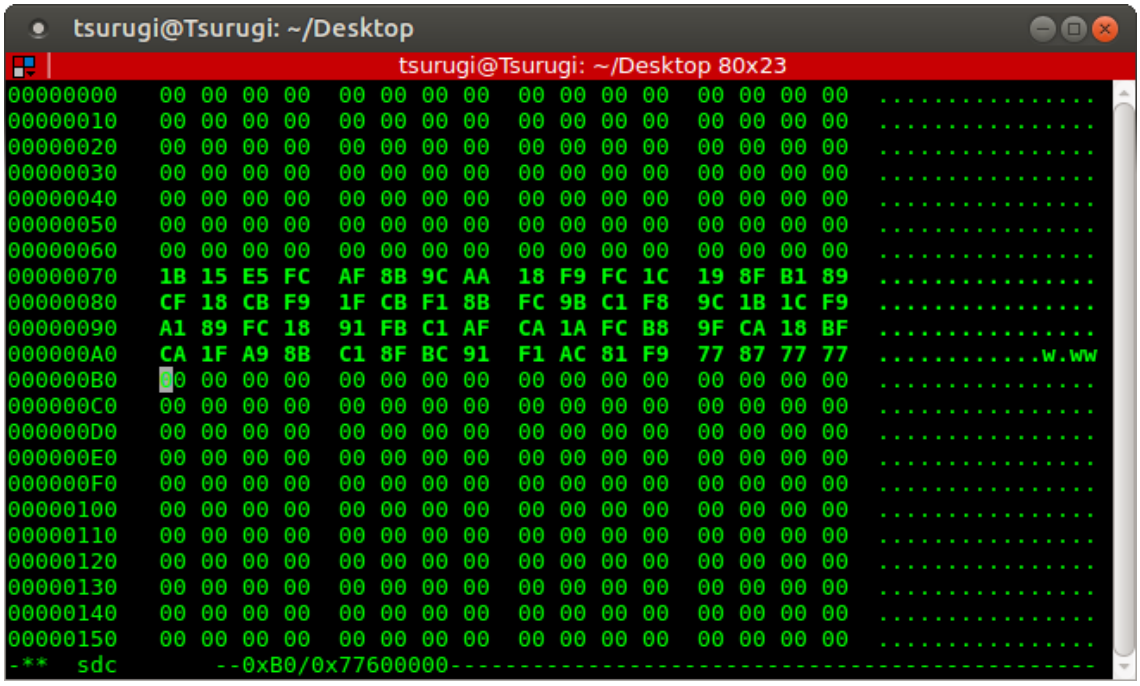

Bild 80: Tsurugi – Änderungen über den Hexeditor

Auffallend nach der Speicherung war, dass sich ähnlich wie bei dem Versuch der Formatierung der Zustand des Geräts im Hintergrund sich von read-only in read-write verändert hat.

Die folgende Sicherung des Geräts und der damit einhergehende verändert Hashwert belegen, dass Abweichungen vom ursprünglichen Zustand bestehen.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	FAIL
Hash nach Hex-Edit	9bea2599abda24784c0265b778698e68	

4.2.3.4 Performance

Imation Nano 2GB:	Sicherung 1:	0:01:53
	Sicherung 2	0:01:53
	Sicherung 3:	0:01:53
	Durchschnitt:	0:01:53
Emtec USB2.0 Stick 8GB:	Sicherung 1:	0:08:49
	Sicherung 2	0:08:52
	Sicherung 3:	0:08:51
	Durchschnitt:	0:08:51
SanDisk Ultra 32GB:	Sicherung 1:	0:07:51
	Sicherung 2	0:07:49
	Sicherung 3:	0:08:04
	Durchschnitt:	0:07:55
Western Digital WD500BPVT:	Sicherung 1:	2:02:14
	Sicherung 2	2:03:33
	Sicherung 3:	2:03:23
	Durchschnitt:	2:03:03
Seagate ST500DM002_1:	Sicherung 1:	1:37:08
	Sicherung 2	1:34:56
	Sicherung 3:	1:34:45
	Durchschnitt:	1:35:36

4.2.3.5 Erkenntnisse

Der integrierte Schreibschutz der forensischen Distribution TSURUGI Linux bietet nur einen rudimentären Schutz vor Schreibzugriffen. Während es garfische und kommandozeilenbasierte Dateioperationen unterbindet, werden gezielte Bearbeitungen durch Hexeditoren oder Formatierungsversuche nicht geblockt.

4.3 Software-Writeblocker auf macOS

Zur Verfügung stehen ein MacBook (12“ 2017) mit Intel i7 Chipsatz sowie 8GB RAM und macOS 12.4 sowie ein MacBook Pro (14“ 2021) mit M1 ARM Chipsatz und 16 GB RAM auf gleicher Software zur Verfügung.

Da das 12“ MacBook nur über einen USB-C Anschluss verfügt, muss ein Redstar24 6-in-1 USB-C HUB zwischen zu prüfende Datenträger und dem Host gelegt werden. Somit lassen sich die USB-Sticks direkt anschließen. Die SATA Festplatten werden über einen USB to SATA Cable CE Adapter mit den USB-A Ports des Hubs verbunden. So kann auch die Stromversorgung des MacBooks über den Hub realisiert und schnellere Übertragungen gewährleistet werden. Warnmeldungen des MacBooks hinsichtlich des Stromverbrauches wurden deaktiviert. Gegen die deutliche Wärmeentwicklung bei diesen langen Laufzeiten wurde das MacBooks belüftet.

Das Ergebnis der Recherche ist eindeutig. Es gibt keine Möglichkeiten für Writeblocker auf Apples neuem Chipsatzmodell. Weder kommerziell verfügbare Software noch Open Source Projekte konnten für diesen Usecase gefunden werden. Ursache dafür ist, dass Befehle über Apples Rosetta 2 Projekt interpretiert und umgesetzt werden.

Die bei der Recherche gefundenen Softwareprodukte basieren auf der Intel-Architektur und werden hier in willkürlicher Reifenfolge aufgeführt.

Die Installation des FTK Imager ist einfach und sehr schnell durchgeführt. Die heruntergeladene .zip Datei muss nur entpackt werden. Danach lässt sich ein Terminal öffnen und der FTK Imager ausführen. Durch den Befehl „./ftkimager“ lässt sich die Hilfeseite anzeigen. Im Folgenden wird der ftkimager in Programme verschoben um eine bessere Ordnung zu haben.

4.3.1 macOS NTFS Einbindung

Ähnlich zu Linux und Windows gibt es bei macOS Betriebssystemen eigenen Schreibschutz für NTFS-Partitionen, denn diese werden in macOS nur lesend eingebunden. Apple von Haus unterstützt somit nur lesende Zugriffe. Es gibt viele Treiber und Tools sowohl aus dem AppStore als auch über alternative Bezugsquellen

damit man Medien auch als read-write mounten kann. In diesem Fall wird die NTFS for MAC Software von Paragon eingesetzt. Damit lassen sich Medien aktiv schalten.

4.3.2 Disk Arbitrator

Der Disk Arbitrator von aburgh lässt sich von GitHub (18) herunterladen. Die Installation erfolgt über die Verschiebung in den Applicationsordner (Programme). Danach findet sich die Software im Launchpad und kann gestartet werden. Über ein Einfaches und aus drei Farben bestehendes System wird der Status der Software angezeigt. Grün bedeutet die Software ist im Blockmodus, was das Mounten von neuen Medien betrifft. Orange ist der read-only Modus, der getestet werden soll und alle nach Aktivierung alle neu angehangene Medien nur read-only mounted und grau zeigt an, dass die Software deaktiviert ist. Bei der Benutzung wird darauf geachtet, alle anderen Programme zu deaktivieren und zu schließen, um möglichst viele Systemressourcen freizuhalten. Der Disk Arbitrator wird gestartet und die read-only Variante durch Anhaken aktiviert. Danach wird das zu sichernde Medium angeschlossen.

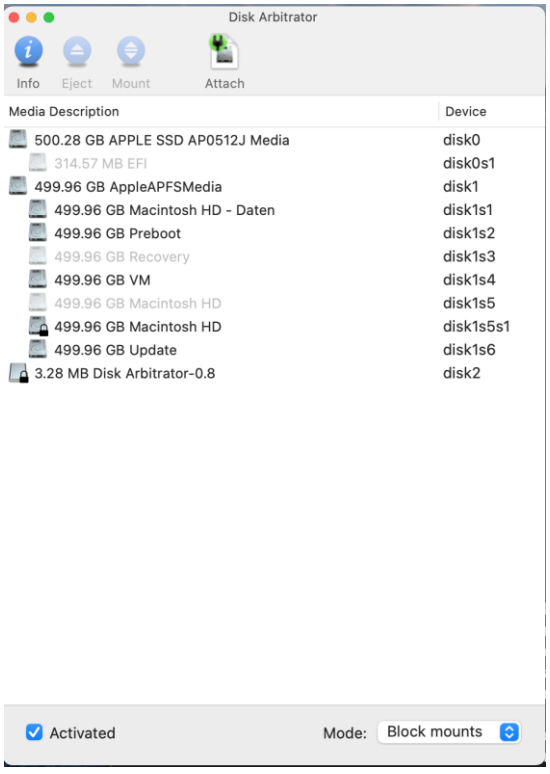

Bild 81: Disk Arbitrator - Dashboard im Blockmodus

4.3.2.1 Dateioperation

Es wird versucht eine Datei auf den Datenträger zu kopieren. Schon beim Mouseover ist durch das Verbotsschild ersichtlich, dass es verboten ist. Das Drag'n'Drop wird nicht ausgeführt. Es erscheint keine Information oder Fehlermeldung.

Eine Datei oder Ordner vom Medium zu löschen ist ebenfalls nicht auswählbar. Über das Terminal ist die Löschung einer Datei ebenfalls nicht möglich.

Danach wird eine Sicherung mit dem ftkimager erstellt. Mit nachfolgendem Befehl werden das Image und ein zugehöriges Log im angegebenen Ordner abgelegt.

```
[topher@f0:18:98:61:09:e0 ~ % sudo /Applications/ftkimager /dev/disk4 /Users/toph]
er/img/imation --e01 --frag 1500MB --compress 6 --case-number „Fachprojekt2“ --e
vidence-number „imation2GB“ --description „2GB“ --examiner CBublies --notes „aft
er-data“
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

Creating image...
33,28 / 1910,00 MB (5,55 MB/sec) - 0:05:38 left
```

Bild 82: ftkimager - Befehl und Ausführung

Der Vergleich des ursprünglichen Hashs mit dem Hash aus der Sicherung ist übereinstimmend und somit sind keine Änderungen am Medium vorgenommen worden.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Datei-operationen	f4bc5f9fa365c3aa076a11c38514c78f	

4.3.2.2 HEX Editor

Mit dem Programm Hex fiend als Alternative zu HEX-Editor wird eine Datei auf dem Datenträger geöffnet und bearbeitet. Beim Speichern erscheint eine Fehlermeldung.

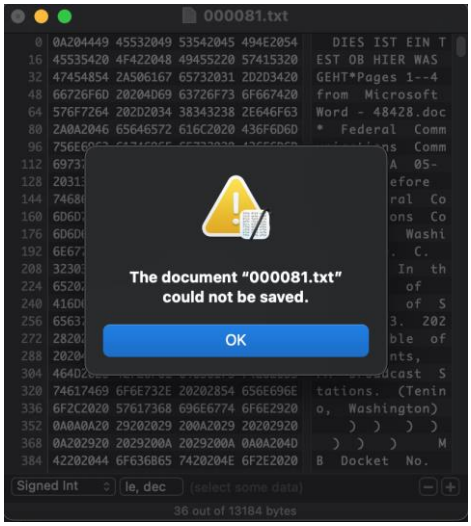

Bild 83: hex fiend – Fehler beim Speichern

Die anschließende Sicherung ergibt folgenden Hashwert und ist wieder mit Original übereinstimmend.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Datei-operationen	f4bc5f9fa365c3aa076a11c38514c78f	

4.3.2.3 Partitionierung

Über das macOS eigenes Festplattdienstprogramm soll der USB-Stick neu formatiert werden. Dabei ist der Punkt Partitionierung ausgegraut und nicht verfügbar.

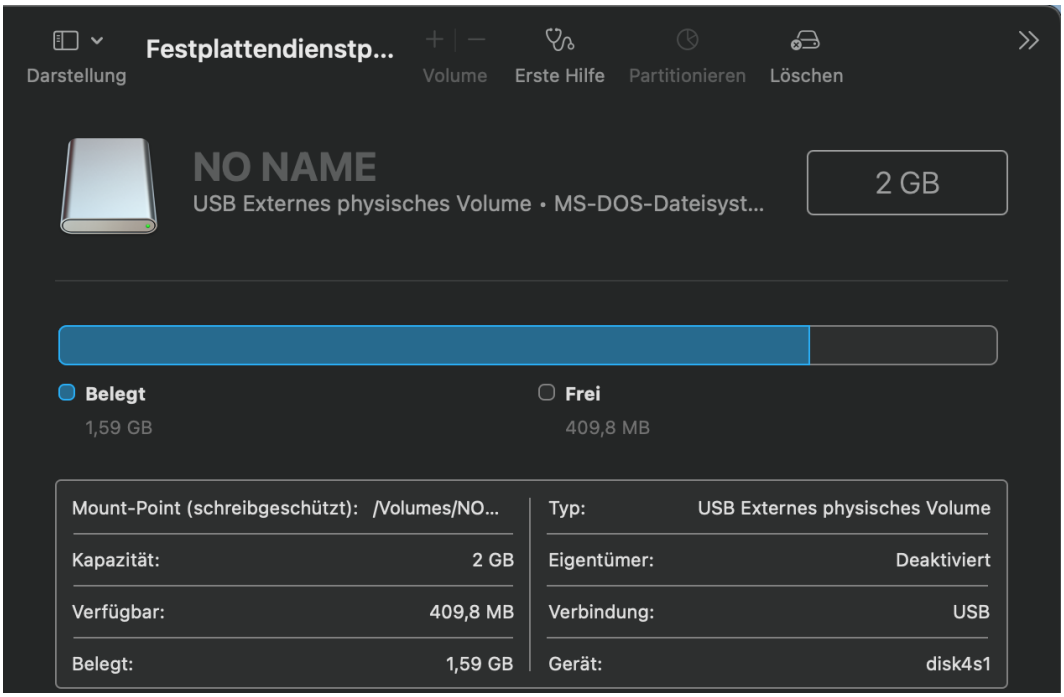

Bild 84: Festplattendienstprogramm – Partitionierung nicht möglich

Das Löschen des USB-Sticks ist hingegen möglich, wird aber nicht ausgeführt, da dann der Hashwert definitiv unterschiedlich ist. Die Sicherung wird wieder durchgeführt und ergibt ohne Änderungen der Partitionierung natürlich den gleichen Hashwert des Originales.

Ursprünglicher Hash	f4bc5f9fa365c3aa076a11c38514c78f	PASS
Hash nach Datei-operationen	f4bc5f9fa365c3aa076a11c38514c78f	

4.3.2.4 Performance

Aufgrund der langen Sicherungszeiten der Festplatten und Abbrüche der Sicherungen wird jeweils nur eine Sicherung durchgeführt und gewertet.

Imation Nano 2GB:	Sicherung 1:	0:04:49
	Sicherung 2	0:04:48
	Sicherung 3:	0:04:50
	Durchschnitt:	0:04:49
Emtec USB2.0 Stick 8GB:	Sicherung 1:	0:26:57
	Sicherung 2	0:27:02
	Sicherung 3:	0:26:54
	Durchschnitt:	0:26:58
SanDisk Ultra 32GB:	Sicherung 1:	0:39:19
	Sicherung 2	0:39:23
	Sicherung 3:	0:39:35
	Durchschnitt:	0:39:26
Western Digital WD500BPVT:	Sicherung 1:	14:16:04
Seagate ST500DM002_1:	Sicherung 1:	11:43:46

4.3.2.5 Erkenntnisse

Das Testvorgehen wird jeweils mit den anderen Medien wiederholt. Allerdings ergeben sich keine neuen Erkenntnisse hinsichtlich der Qualität des Writeblockers, dieser funktioniert auch mit anderen Datenträgern. Auffallend ist die deutlich langsamere Sicherung, wenn der Disk Arbitrator läuft. Zum Vergleich dazu ist die Sicherung des 2GB Imation USB-Sticks schon nach 00:04:20 fertig gestellt.

4.3.3 WriteController

Der WriteController ist eine Software der SubRosaSoft, die allerdings ihren Betrieb eingestellt hat. Über das Internetarchive ist die Software noch zum Download verfügbar. Die .zip-Datei konnte so heruntergeladen werden. Nach dem Entpacken und Starten der .dmg Datei öffnet sich das Installationsfenster. Hier ist deutlich, dass die Software nicht installiert werden kann.

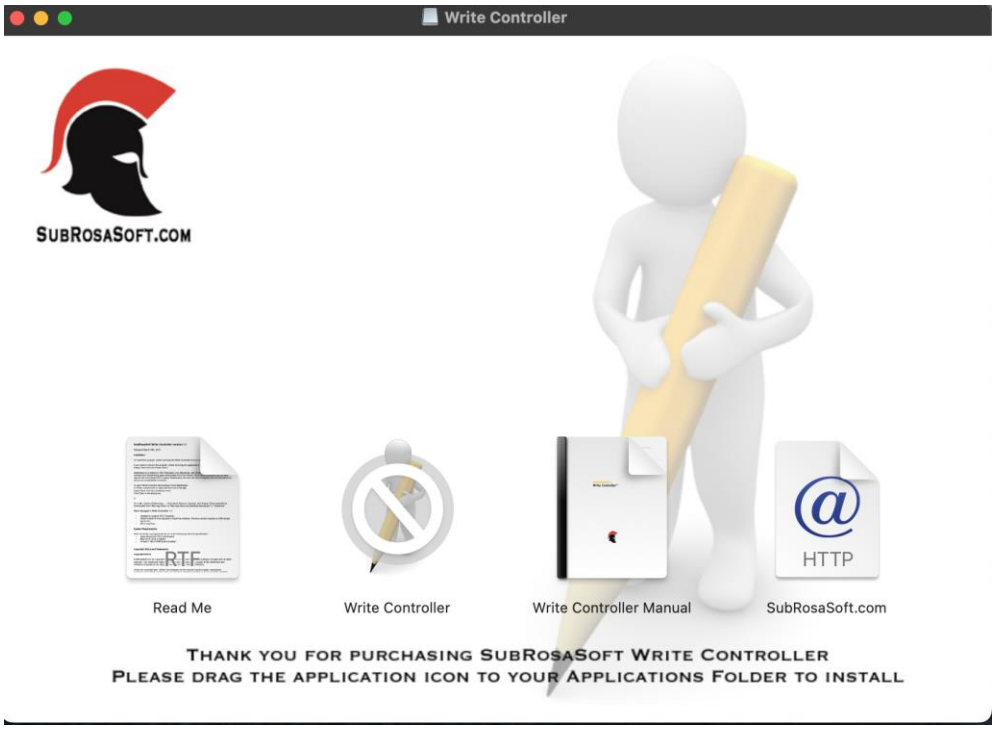

Bild 85: WriteController - Installation

Der Grund dafür ist die 64-Bit Architektur der aktuellen macOS Versionen, die auf Intel Chipsätzen beruhen. Der Write Controller ist allerdings eine 32-Bit Software, die seit macOS Mojave nicht mehr benutzt werden kann. Die Kompatibilität kann mit macOS 12.4 nicht mehr hergestellt werden.

Eine Installation einer macOS Mojave Version zur Benutzung des Write Controllers in einer Parallels Umgebung auf dem MacBook war nicht erfolgreich. Ein Dualboot konnte aus privaten Gründen nicht eingerichtet werden.

4.3.4 Softblock

Softblock von Cellebrite stellt ebenfalls einen SW-Writeblocker dar. Dieser ist allerdings kommerziell und somit kostenpflichtig. Eine Anfrage beim Hersteller war nicht erfolgreich. Zudem wurde mitgeteilt, dass sich die Entwicklung auf Windows spezialisiert und diese Software so nicht weiter bedacht wird. Der weitere Versuch über Firmenkontakte an diese Software zu gelangen, war ebenfalls nicht erfolgreich. Zusätzlich muss erwähnt werden, dass nach offiziellen Releasenotes die macOS Version 10.4 bis 10.8 unterstützt ist.

4.3.5 Recon ITR und Recon Imager

Der Recon Imager ist ein Teil der Recon ITR Softwaresuite und eine Sammlung von Analysewerkzeugen für forensische Fragestellungen. Als Student bekommt man eine 15-tägige Demoversion.

Die .dmg Datei lässt sich installieren und die Software danach starten. Ein Writeblocker beinhaltet die Software aber nicht mehr. Sie ist als Alternative zum FTK Imager benutzbar.

5 Auswertung

Alle der hier getesteten software- und hardwarebasierten Writeblocker unterbinden zuverlässig Dateioperationen und wahrten hierbei die forensische Integrität des angefertigten Datenträgers. Eine Ausnahme bildet das UDeck (Beaglebone Black), das als einziges Gerät bei vollzogenen Dateioperationen einen abweichenden Hashwert für das gesicherte Medium aufwies. Dies ist aufgrund des ausschließlichen, gerätespezifischen Zugriffs auf Partitionen und nicht auf das gesamte Gerät begründet. Eine physikalische Sicherung war demnach nicht möglich. Veränderungen am Datenträger wurden hingegen nicht verursacht. Da eine Betrachtung der Partitionen des Datenträgers im Falle einer forensischen Datenträgeranalyse als unzureichend betrachtet werden kann, wird keine Empfehlung für das Produkt in der vorliegenden Form gegeben.

Die Funktionialität einzelner Writeblocker war auf den Schutz vor Dateioperationen beschränkt. So ließ der Magic-USB-Hub (4Deck) im weiteren Testverfahren Schreibzugriffe durch Partitionierung und/oder Hex-Editoren zu. Dies gelang ebenfalls bei den Softwarelösungen Microsoft Windows (mit aktiviertem WriteProtect-Registry-Key) und dem auf der forensischen Distribution TSRUGI Linux. Im Falle des Emtec USB-Sticks zeigte sich der Magic-USB-Hub ebenfalls gegen Zugriffe auf Dateiebene unwirksam, da das begleitende Skript hierbei nicht zum gesicherten Zugriff auf das Medium führte. Das eingangs vorgestellte CRU CFTT Tool fungierte bei Writeblockern, die zuvor die in der Ausarbeitung durchgeführten Operationen bestanden hatten, den abschließenden Test. Hierbei fiel Sharkoon DriveLink Combo USB 3.0 V2 durch.

Mit Delock 62652 SATA / USB Converter, Firebrick3, Tableau T3iu Forensic SATA Imaging Bay, WiebeTech USB 3.1 WriteBlocker, WiebeTech Forensic Ultradock V5 und SAFEBlock konnten insgesamt sechs der dreizehn untersuchten Write-Blocker alle Tests bestehen und eignen sich für die sichere forensische Duplikation von Datenträgern. Der Selbstbau USB Writeblocker und die macOS Software Disk Arbitrator bestanden die einzelnen Testschritte, konnte jedoch nicht abschließend über das CRU CFTT Tool getestet werden.

SAFEBlock ist in dieser Untersuchung die einzige Softwarelösung, die hinsichtlich der forensischen Sicherheit durch die bestandenen Tests mit Hardwarelösungen gleich auf liegt. Der Vorteil einer Softwarelösung liegt vor allem in der Bandbreite der verfügbaren Schnittstellen. Die Software ist zwar von den Schnittstellen des Hosts-Systems abhängig, kann aber mit Hubs erweitert oder Konvertern ergänzt werden. Abgesehen vom WiebeTech USB 3.1 WriteBlocker waren nur die Softwarelösungen in der Lage, alle fünf Testmedien zu sichern.

Der Disk Arbitrator war ebenfalls in der Lage alle Tests zu bestehen und keine Schreibbefehle zu zulassen, allerdings ist hier die Geschwindigkeit ein großer Negativfaktor. Somit kann die macOS Lösung nicht mit den anderen Software Writeblockern messen.

Hinsichtlich der Geschwindigkeit der einzelnen Sicherungen ist festzuhalten, dass die Softwarelösungen untereinander kaum Unterschiede aufweisen. Limitierender Faktor ist hierbei die Geschwindigkeit des USB-Busports des Hostsystems. Im Vergleich zu Hardwarelösungen liegen die Softwarelösungen bei den Sicherungen der USB-Sticks im oberen Drittel und den Sicherungen der HDD-Festplatten im Mittelfeld.

Trotz des bestandenen Schreibschutz-Tests, kann keine Empfehlung für den DIY-Writeblocker auf Basis des FTDI-Boards gegeben werden. An das Gerät angeschlossene Medien reagieren ausgesprochen träge auf Nutzereingaben und die Medienkompatibilität ist sehr gering. Im Rahmen der Projektvorbereitung wurden verschiedene USB-Sticks verschiedener Marken getestet bis die hier verwendeten USB 2.0 Sticks Imation und Emtec als kompatibel vorgefunden werden konnten. Die Sicherungszeiten, welche mit dem DIY-Writeblocker erreicht werden, stehen in keiner Konkurrenz zu den weiter betrachteten Geräten und sind für einen Produktiven Einsatz ungeeignet:

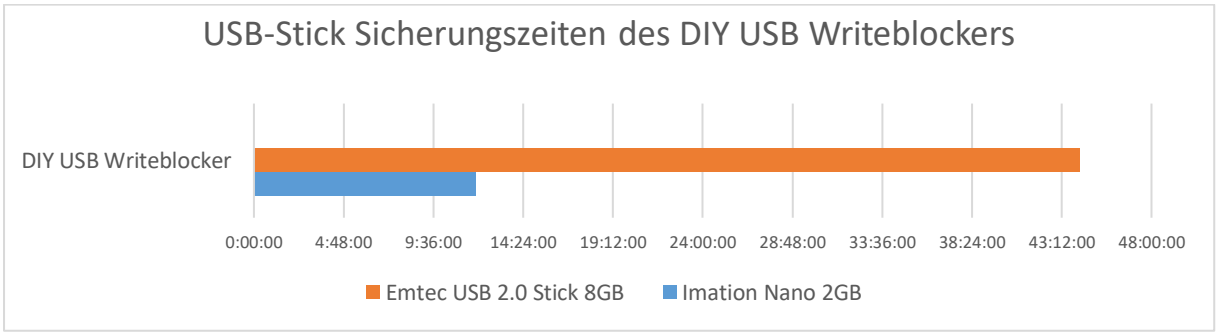

Bild 86: hohe Sicherungszeiten: 44:08:36h für die Sicherung des Emtec Sticks am DIY USB WriteBlocker

Die weiteren WriteBlocker liegen bei den Sicherungszeiten der USB-Sticks näher beieinander:

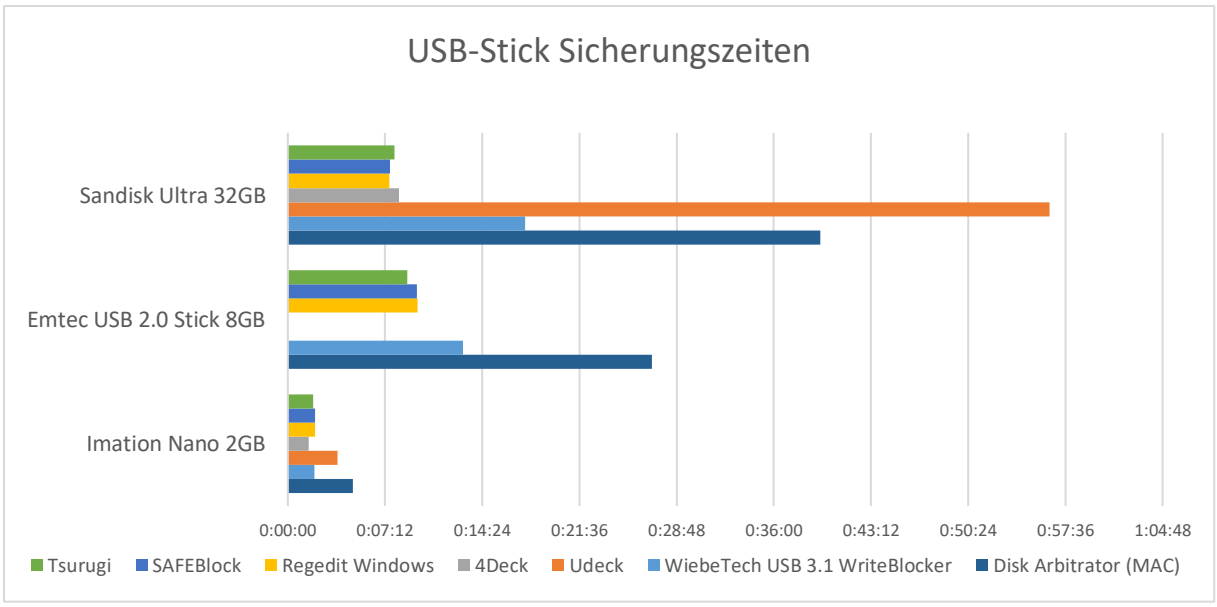

Bild 87: Sicherungszeiten bei der Sicherung der USB-Sticks im Vergleich

Eine größere Abweichung zeigt hier der Beaglebone Black bei der Sicherung des Sandisk Ultra 32GB Sticks. Diese ist auf die Beschränkung auf USB 2.0 zurückzuführen.

Auch der forensische WiebeTech USB 3.1 WriteBlocker fällt hier hinter die Vergleichsgruppe zurück. Dabei kann nicht ausgeschlossen werden, dass diese verminderten Geschwindigkeiten durch die verwendeten USB-Treiber unter Windows verursacht wurden. Stichprobenartige Vergleiche der weiteren WriteBlocker unter Windows führten ebenfalls zu einer Verlängerung der Sicherungszeit gegenüber der Sicherung unter Linux.

Bei den Sicherungszeiten der verwendeten Festplatten zeigen sich weniger intensive Ausschläge als bei den USB-Sticks. Bei allen hier dargestellten Methoden kann auf die USB 3.0 Schnittstelle zugegriffen werden.

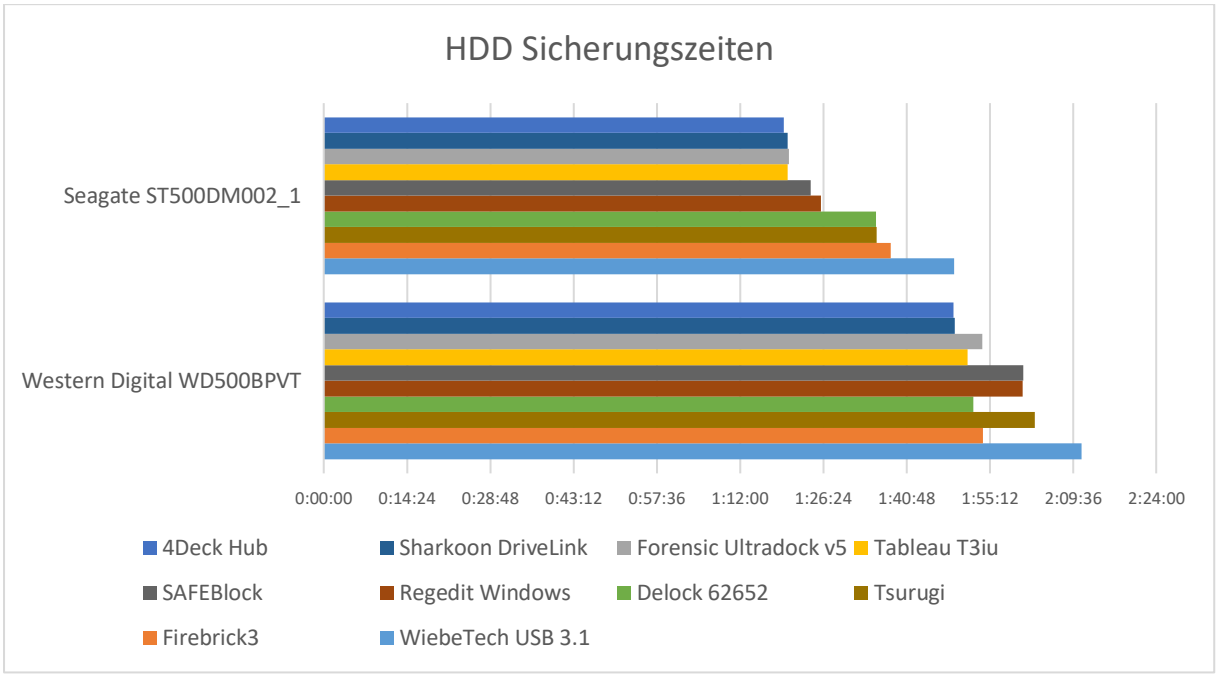

Bild 88: Sicherungszeiten bei der Sicherung der Festplatten im Vergleich

Die sehr guten Sicherungszeiten des 4Deck sind darauf zurückzuführen, dass es sich hierbei nicht um einen klassischen Hardware-Writeblocker handelt, sondern um Hardware-gestütztes Software-Writeblocking. In der Darstellung (Bild 83) wird der Disk Arbitrator nicht abgebildet, da dessen hohe Sicherungszeiten die Vergleichbarkeit der weiteren Datenträger erschweren würde.

Einleitend wurde festgehalten, dass ein Writeblocker den Abruf von Informationen zum Datenträger nicht unterdrücken darf. Dies ist bei den Writeblockern, welche den Schreibschutztest bestanden haben der Fall. Über die Art der Sicherung (iSCSI) werden vom Firebrick3 zunächst keine Informationen zum Datenträger selbst an das Hostsystem weitergegeben. Diese Informationen lassen sich jedoch über einen SSH-Zugriff auf das Gerät erlangen. Denkbar wäre auch eine Modifikation der Weboberfläche des Firebricks, um Datenträgerinformationen dort anzuzeigen.

6 Fazit

Die forensische Duplikation bei der Untersuchung von Datenträgern setzt hohe Maßstäbe an die Sicherheit des verwendeten Schreibschutzes. Aufgrund dessen sollte im Vorfeld des Einsatzes von Writeblockern individuell der Schreibschutz auf seine Funktion überprüft werden, um zuverlässigen Schutz hinsichtlich der forensischen Integrität zu bieten.

In dieser Projektarbeit wurden die Grundlagen von Writeblockern herausgearbeitet und im Anschluss verschiedene Implementierungen von Writeblockern überprüft, getestet, bewertet und miteinander verglichen.

Es konnte festgestellt werden, dass Softwarelösungen hinsichtlich der Schnittstellen deutlich flexibler als Hardwarelösungen sind. Jedes der fünf Speichermedien konnte mit dem Host-System verbunden und gesichert werden. Bezüglich der Geschwindigkeit von Sicherungen durch Software-Writeblocker konnten – bis auf die macOS Open Source Variante - keine gravierenden Unterschiede oder Vorteile festgestellt werden. Der allein durch Betriebssysteme gewährte Schreibschutz bietet selbst bei einer forensischen Distributaion wie TSURUGI Linux keine ausreichende forensische Sicherheit vor Schreibzugriffen. Hierfür bedarf es speziell zugeschnittene Software wie SAFEBlock oder einen physischen Writeblocker, der zwischen Speichermedium und Hosts verbunden wird.

Gegenüber den Hardware-Lösungen, die einen forensischen Anspruch ausweisen, konnte sich der Open Source Writeblocker Firebrick beweisen. Eine Erweiterung des Schreibschutzes auf andere Schnittstellen durch Codeanpassungen und PCI-Erweiterungsplatinen sind hierbei ebenfalls möglich. Mit rund 100€ liegen die Beschaffungskosten des Firebrick dazu deutlich unter denen kommerzieller Writeblocker (> 350€).

Auch der Delock 62652 SATA / USB Converter bestand den Writeblocking Test und führte zu keinen erheblichen Verzögerungen der Sicherungszeiten. Diese Low Cost Variante stellt damit für SATA-Datenträger eine kostengünstige Alternative (ca. 30€ + Netzteil) zur Ergänzung des forensischen Werkzeugkoffers dar.

Das Vorhalten verschiedener Writeblocker ist ohnehin zu empfehlen. Im Test zeigten sich vereinzelt Inkompatibilitäten einzelner Writeblocker mit verschiedenen Medien. Das Ausweichen auf einen anderen Schreibschutzmechanismus kann sich so erforderlich machen.

7 Ausblick

Im Rahmen dieser Projektarbeit konnte nur einige Aspekte des Write-Blockings beleuchtet werden. So wurden lediglich Sicherungen über SATA und USB betrachtet. Die Sicherung von Speicherkarten, SAS-Festplatten und RAID-Systemen bieten weitere Untersuchungsansätze.

Der Open-Source-Charakter des Firebrick Projekts erlaubt Modifikationen am System, um weitere Schnittstellen schreibgeschützt bereitzustellen. Eine Erweiterung dieses Projekts und gegebenenfalls die Anpassung auf modernere Hardware können im Rahmen einer Projektarbeit durchgeführt werden.

Bezogen auf den Linux-Kernel-Writeblock wurde im Rahmen der Ausarbeitung die Distribution Tsurugi betrachtet. Darüber hinaus gibt es zahlreiche forensische Distributionen auf Linux-Basis, welche im Rahmen einer Projektarbeit beleuchtet werden können. Als Beispiele seien hier genannt:

- CAINE
- Deft
- Sumori Paladin
- Kali Forensic Mode
- Helix3
- Grml

Daneben existieren auch Live Systeme auf Windows Basis, welche zur sicheren Erstellung von Datenträgerabbildern geeignet seien sollen. Einige Beispiele sind:

- Windows Forensic Edition (WinFE)
- WinPE for Forensics
- Windows Triage Environment (WTE)

Selbst für das Betriebssystem DOS existieren noch Software-Writeblocking Lösungen. Ob sich eine FreeDOS Installation mit HX-DOS und FTK unter der Verwendung eines Writblockers wie PDBlock auch heute produktiv zur Datensicherung einsetzen lässt, kann Inhalt weiterer Untersuchungen sein. Hierbei kann auch ein Vergleich mit der proprietären DOS-Software X-Ways Replica angestellt werden.

Da erforderliche proprietäre Software für macOS bis zur Abgabe der Projektarbeit nicht bereitgestellt werden konnte, wurde ausschließlich das Open Source Tool Disk-Arbitrator untersucht. Die Eignung eines Mac als Forensische Sicherungs- und Auswertestation kann Gegenstand weiterer Untersuchungen sein. Software, wie z.B. NUIX steht auch für macOS bereit.

Literaturverzeichnis

1. **Bolkart, J.** Polizeilich erfasste Straftaten mit dem Tatmittel Internet in Deutschland von 2009 bis 2019. [Online] 02. Juni 2022. [Zitat vom: 15. Juni 2022.] https://de.statista.com/statistik/daten/studie/295295/umfrage/polizeilich-erfasste-straftaten-mit-dem-tatmittel-internet-in-deutschland/.

2. **Bundesamt für Sicherheit in der Informationstechnik.** Leitfaden IT-Forensik. [Online] [Zitat vom: 11. Juni 2022.] (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1.

3. **Roos, Ute.** Heise.de. *Kritische Sicherheitslücken in Write-Blocker entdeckt.* [Online] 21. Dezember 2013. [Zitat vom: 13. Juni 2022.] https://www.heise.de/ix/meldung/Kritische-Sicherheitsluecken-in-Write-Blocker-entdeckt-2071582.html.

4. **AccessData.** Imager User Guide. [Online] 28. Januar 2020. [Zitat vom: 13. Juni 2022.] https://ad-pdf.s3.amazonaws.com/Imager/4_3_0/FTKImager_UG.pdf .

5. **Wikipedia.** ISO 9241. *ISO 9241-110 Interaktionsprinzipien.* [Online] [Zitat vom: 11. Juni 2022.] https://de.wikipedia.org/wiki/ISO_9241.

6. **National Institute of Standards and Technology (NIST).** Computer Forensics Tool Testing Program (CFTT). [Online] [Zitat vom: 11. Juni 2022.] https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

7. —. Software Write Block Tool Specification & Test Plan, Version 3.0. [Online] 1. September 2003. [Zitat vom: 11. Juni 2022.] Seite 6 von 28. https://www.nist.gov/system/files/documents/2017/05/09/swb-stp-v3_1a.pdf.

8. —. NIST Computer Forensics Tool Testing Program (CFTT). *Test Results for Hardware Write Block Device:Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection (Windows 10). March 2020.* [Online] [Zitat vom: 11. Juni 2022.] https://www.dhs.gov/sites/default/files/publications/testresults_for_cool_gear_sata-ide_adapter_windows.pdf.

9. **Wiebetech by CRU.** WiebeTech® WriteBlocking Validation Utility. [Online] [Zitat vom: 11. Juni 2022.] https://www.cru-inc.com/downloads/marketing/white-papers/2-Forensics/WiebeTech_WriteBlocking_Validation_Utility.pdf.

10. **Polstra, Philip.** Instructables - Cheap and Effective USB Write Blocker. [Online] 2013. [Zitat vom: 09. August 2021.] https://www.instructables.com/Cheap-and-Effective-USB-Write-Blocker/.

11. **Tobin, Lee.** Github.com. *firebrick3.* [Online] [Zitat vom: 10. Juni 2022.] https://github.com/leetobin/firebrick3.

12. **Polstra, Dr. Philip.** Github.com - UDeck. [Online] [Zitat vom: 10. Juni 2022.] https://github.com/ppolstra/UDeck.

13. —. Github - 4Deck. [Online] [Zitat vom: 10. Juni 2022.] https://github.com/ppolstra/4Deck) .

14. **Polstra, Philip.** GitHub - ppolstra / USB-Writeblocker. [Online] 03. September 2013. [Zitat vom: 03. August 2021.] https://github.com/ppolstra/USB-Writeblocker.

15. **Ullrich, Frank.** WinFAQ - Schreibschutz für USB Storage Device ein-/ausschalten. [Online] [Zitat vom: 11. Juni 2022.] http://www.winfaq.de/faq_html/Content/tip1500/onlinefaq.php?h=tip1686.htm.

16. **ForensicSoft.** ForensicSoft - FAQs. [Online] [Zitat vom: 11. Juni 2022.] https://www.forensicsoft.com/faq.

17. **Tsurugi Linux.** Documentation Tsurugi Linux [LAB]. [Online] [Zitat vom: 11. Juni 2022.] https://tsurugi-linux.org/documentation_tsurugi_linux_special_features.php.

18. **Burghardt, Aaron.** Github - Disk Arbitrator. [Online] [Zitat vom: 16. Juni 2022.] https://github.com/aburgh/Disk-Arbitrator.

Abbildungsverzeichnis

Anlagen

A.1 Beurteilung: Delock 62652 SATA / USB Converter

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	SATA
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Keiner der durchgeführten Tests verursachte eine Veränderung am Medium. Ein zusätzlicher Test über das CRU WriteBlocking Validation Utility war möglich. Auch dabei wurden keine Veränderungen verursacht.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit	X			Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit		X		Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler			X	Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Nach einmaligem Setzen des Schreibschutz-Headers werden angeschlossene Datenträger vor Veränderungen durch das Hostsystem geschützt. Weitere Rückmeldungen werden durch den Adapter nicht gegeben. Eine falsche Jumperstellung führt potentiell zu Schreibzugriffen auf das Medium.			
Bewertung Handhabung:	63%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	1:52:20	4.
Seagate ST500DM002_1	1:35:29	7.

A.2 Beurteilung: Sharkoon DriveLink Combo USB 3.0 V2

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	IDE / SATA
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**FAIL**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war möglich. Dabei konnte auf den Datenträger geschrieben werden	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit		x		Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	X			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler		x		Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Nach dem Einstellen des Schreibschutzschalters werden Schreibzugriffe, welche im Rahmen gewöhnlicher Nutzung verursacht werden geblockt. Eine LED zeigt an, ob der Schreibschutz aktiv ist. Wird das Fehlen des Schreibschutzes festgestellt, kann dieser vor dem Anstecken des Mediums gesetzt werden. Wird das Medium vor dem Aktivieren des Adapters angesteckt, fällt der fehlende Schreibschutz zu spät auf.			
Bewertung Handhabung:	63%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	1:49:07	2.
Seagate ST500DM002_1	1:20:13	2.

A.3 Beurteilung: Selbstbau USB-Writeblocker

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	USB (1.1)
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**nicht möglich**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war nicht möglich.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit			x	Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit			x	Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden. Dabei ist ein produktiver Umgang mit dem Medium nicht möglich da ein erheblicher Zeitverzug bei allen Operationen verursacht wird. Ein nicht schreibgeschützter Zugriff ist hier nicht möglich, so dass Fehler durch den Nutzer ausgeschlossen sind.			
Bewertung Handhabung:	25%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	-	
Seagate ST500DM002_1	-	
Imation Nano 2GB	11:49:09	7.
Emtec USB 2.0 Stick 8GB	44:08:36	5.
Sandisk Ultra 32GB	-	

A.4 Beurteilung: Firebrick3

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	SATA
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war möglich und verursachte keine Veränderungen.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit		x		Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	x			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden, dabei werden jedoch Informationen zum Medium (z.B. Seriennummer) nicht an das Host-System weitergereicht. Eine Webgui ermöglicht die Bereitstellung des Mediums. Der Zugriff über den Windows-iSCSI Initiator ist komfortabel möglich. Ein nicht schreibgeschützter Zugriff ist hier nicht möglich, so dass Fehler durch den Nutzer ausgeschlossen sind.			
Bewertung Handhabung:	75%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	1:54:04	6.
Seagate ST500DM002_1	1:38:02	9.

A.5 Beurteilung: UDeck (Beaglebone Black)

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**FAIL**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**FAIL**	USB (2.0)
Schutz gegen Operationen auf Blockebene / Hexedit	**FAIL**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Dennoch wurde ein anderer Hash generiert. Ein Test über das WriteBlocking Validation Utility war möglich und wurde bestanden.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit		x		Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit			x	Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler		x		Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Es werden nur Zugriffe auf Partitionen ermöglicht, nicht auf das Blockgerät. Vollständige Sicherungen sind so nicht möglich. Es bedarf einer SSH-Verbindung zum Gerät. Es ist nicht erkennbar, warum Medien nicht eingebunden werden. Die Ausführung des falschen Scripts führt zum schreibenden Zugriff auf das Medium.			
Bewertung Handhabung:	38%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	-	
Seagate ST500DM002_1	13:58:22	12.
Imation Nano 2GB	0:03:41	6.
Emtec USB 2.0 Stick 8GB	-	
Sandisk Ultra 32GB	0:56:26	7.

A.6 Beurteilung: Beurteilung: Magic USB-Hub (4Deck)

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**FAIL**	USB
Schutz gegen Operationen auf Blockebene / Hexedit	**FAIL**	
Verifikation über CRU CFTT Tool	**nicht möglich**	
Ergänzende Hinweise zum Schreibschutz	Die durchgeführten Tests auf Partitions- und Blockebene führten zu Veränderung am Medium. Ein Test über das WriteBlocking Validation Utility war nicht möglich.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit			X	Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit		X		Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler			X	Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden. Dabei wird ein Schutz nicht gewährleistet. Inkompatible Medien werden schreibend eingebunden. Die erfolgreiche Ausführung der Regel ist erkennbar, wenn der Automount des Mediums ausgeführt wird. Auch bei schreibgeschütztem Einbinden können Fehler des Nutzers zu Veränderungen führen.			
Bewertung Handhabung:	13%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	1:48:54	1.
Seagate ST500DM002_1	1:19:35	1.
Imation Nano 2GB	0:01:32	1.
Emtec USB 2.0 Stick 8GB	-	
Sandisk Ultra 32GB	0:08:13	4.

A.7 Beurteilung: Tableau T3iu Forensic SATA Imaging Bay

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	SATA
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war möglich und verursachte keine Veränderungen.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit		x		Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	x			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden. Unter Windows konnte das Medium nicht eingesehen werden. Eine Sicherung war jedoch möglich. Über DIP Schalter auf der Rückseite kann der Schreibschutz deaktiviert werden. Eine LED zeigt den aktiven Schreibschutz an.			
Bewertung Handhabung:	75%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	1:51:25	3.
Seagate ST500DM002_1	1:20:17	3.

A.8 Beurteilung: WiebeTech USB 3.1 WriteBlocker

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	USB 3.0 / 3.1
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war möglich und verursachte keine Veränderungen.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit	x			Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	x			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden. Eine Funktion des Geräts ist nur für Windows gegeben. Eine LED zeigt den aktiven Schreibschutz an. Bei Kommunikationsfehlern (fehlende Treiber) zum Host-System wird das Medium nicht eingebunden. Ein nicht geschützter Zugriff ist ausgeschlossen.			
Bewertung Handhabung:	100%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	2:11:02	10.
Seagate ST500DM002_1	1:49:06	10.
Imation Nano 2GB	0:01:58	3.
Emtec USB 2.0 Stick 8GB	0:12:22	4.
Sandisk Ultra 32GB	0:17:35	5.

A.9 Beurteilung: WiebeTech Forensic Ultradock V5

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	SATA / IDE
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war möglich und verursachte keine Veränderungen.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit	x			Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	x			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden. Eine LED zeigt den aktiven Schreibschutz an. Über ein Display und ein Steuerkreuz können Informationen zum Medium auch ohne Host-System eingesehen werden. Nutzungsfehler sind nahezu ausgeschlossen.			
Bewertung Handhabung:	100%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	1:53:56	5.
Seagate ST500DM002_1	1:20:28	4.

A.10 Beurteilung: Windows Regedit WriteBlock

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**FAIL**	USB-Schnittstelle
Schutz gegen Operationen auf Blockebene / Hexedit	**FAIL**	
Verifikation über CRU CFTT Tool	**FAIL**	
Ergänzende Hinweise zum Schreibschutz	Die durchgeführten Tests auf Partitions- und Blockebene führten zu Veränderung am Medium. Ein Test über das WriteBlocking Validation Utility zeigte ebenfalls, dass Schreibzugriffe möglich sind	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit			x	Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit		x		Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler			x	Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Nach Änderung des Registry Key wurde der Schreibschutz ohne Neustart des Systems übernommen. Nach Anschluss des Mediums konnten keine Dateioperationen auf USB-Schnittstellengeräte vollzogen werden. Das Windows-Kontextmenü wies für das Medium u.a. keine Einfüge- und Löschschaltflächen mehr auf. Ein darüber hinaus gehender Schutz vor Zugriffen war jedoch nicht gegeben.			
Bewertung Handhabung:	13%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	2:00:52	7.
Seagate ST500DM002_1	1:25:58	6.
Imation Nano 2GB	0:02:01	4.
Emtec USB 2.0 Stick 8GB	0:09:36	3.
Sandisk Ultra 32GB	0:07:30	1.

A.11 Beurteilung: SAFEBlock

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	IDE (PATA & SATA), SCSI, FC, SAS, M.2, NVMe, USB, USB-C and IEEE1394
Schutz gegen Operationen auf Blockebene / Hexedit	**PASS**	
Verifikation über CRU CFTT Tool	**PASS**	
Ergänzende Hinweise zum Schreibschutz	Durch die durchgeführten Tests wurde keine Veränderung am Medium verursacht. Ein zusätzlicher Test über das WriteBlocking Validation Utility war möglich und verursachte keine Veränderungen.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit	x			Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	x			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Angeschlossene Medien können eingesehen und gesichert werden. Eine Funktion des Geräts ist nur für Windows gegeben. Ein Schloss an der Geräteauflistung in der Software zeigt den Status des Schreibschutz an, der Status kann von der Software gespeichert werden. Standardmäßig werden angeschlossene Medium automatisch geschützt.			
Bewertung Handhabung:	100%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	2:00:58	8.
Seagate ST500DM002_1	1:24:17	5.
Imation Nano 2GB	0:02:02	5.
Emtec USB 2.0 Stick 8GB	0:09:33	2.
Sandisk Ultra 32GB	0:07:33	2.

A.12 Beurteilung: Tsurugi

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**FAIL**	IDE (PATA & SATA), SCSI, FC, SAS, M.2, NVMe, USB, USB-C, IEEE1394
Schutz gegen Operationen auf Blockebene / Hexedit	**FAIL**	
Verifikation über CRU CFTT Tool	**Nicht möglich**	
Ergänzende Hinweise zum Schreibschutz	Die durchgeführten Tests auf Partitions- und Blockebene führten zu Veränderung am Medium. Ein Test über das WriteBlocking Validation Utility konnte nicht durchgeführt werden.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit			x	Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit		x		Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler			x	Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Im TSURUGI-Kernel werden automatisch neu angeschlossene Geräte schreibgeschützt eingelesen. Der Status der Geräte kann über eine grafische Oberfläche eingesehen und verändert werden. Ein Schutz über Dateioperationen hinaus war nicht gegeben, Nach derartiger Operationen änderte sich der Status von ro zu rw.			
Bewertung Handhabung:	13%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	2:03:03	9.
Seagate ST500DM002_1	1:35:36	8.
Imation Nano 2GB	0:01:53	2.
Emtec USB 2.0 Stick 8GB	0:08:51	1.
Sandisk Ultra 32GB	0:07:55	3.

A.13 Beurteilung: Disk-Arbitrator

Beurteilung des Schreibschutzes:

Schutz gegen Dateioperationen	**PASS**	Schreibgeschützte Schnittstellen
Schutz gegen Formatierung / Partitionierung	**PASS**	IDE (PATA & SATA), USB, USB-C
Schutz gegen Operationen auf Blockebene / Hex fiend	**PASS**	
Verifikation über CRU CFTT Tool	**Nicht möglich**	
Ergänzende Hinweise zum Schreibschutz	Die durchgeführten Tests führten zu keinen Veränderungen am Medium. Ein Test über das WriteBlocking Validation Utility konnte nicht durchgeführt werden.	

Beurteilung der Handhabung (DIN EN ISO 9241):

Kriterium	voll erfüllt	teilw. erfüllt	nicht erfüllt	Beschreibung
Aufgabenangemessenheit		x		Funktionalität ist geeignet, Minimierung unnötiger Interaktionen (50%)
Selbstbeschreibungsfähigkeit	x			Verständlichkeit wird durch Hilfen / Rückmeldungen gewährleistet (25%)
Robustheit gegen Benutzerfehler	x			Das System toleriert Fehler oder ermöglicht eine leichte Fehlerkorrektur durch den Benutzer (25%)
Ergänzende Hinweise zur Handhabung / Begründung	Der Disk Arbitrator muss laufen um aktiv bedient zu werden. Der Status der Medien kann über eine grafische Oberfläche eingesehen und verändert werden. Ein Schutz ist voll gegeben, aber der Durchsatz von Daten ist deutlich geringer.			
Bewertung Handhabung:	75%			

Durchschnittliche Sicherungszeiten:

Datenträger	Durchschnittliche Sicherungszeit (h/m/s)	Platz in der Vergleichsgruppe
Western Digital WD500BPVT	14:16:04	11.
Seagate ST500DM002_1	11:43:46	11.
Imation Nano 2GB	0:04:49	7.
Emtec USB 2.0 Stick 8GB	0:26:58	6.
Sandisk Ultra 32GB	0:39:26	6.

A.14 Python-Script zur schnellen Betrachtung der Sicherungszeiten

```
import glob
import datefinder

for file in glob.glob("*.txt"):
    inputfile = file
file = open(inputfile,'r')

string1 = " Acquisition started:"
string2 = " Acquisition finished:"

for line in file:
    if string1 in line:
        d1 = line
        print(d1)
        date1 = list(datefinder.find_dates(d1))
    if string2 in line:
        d2 = line
        print(d2)
        date2 = list(datefinder.find_dates(d2))

print(date2[0] - date1[0])
                              # © Christian Peter
file.close()
```

A.15 mount-usb.sh (UDeck – Dr. Polstra)

```
#!/bin/bash
# stop the GETTY service if needed
if which 'systemctl' ; then
  systemctl stop serial-getty@ttyGS0.service >/dev/null
fi
# unload current composite gadget
modprobe -r g_multi
# these variables are used to export all partitions
fstr=""
rostr=""
# unmount the USB drive
for d in $(ls /dev/sd*) ; do
  if  echo "$d" | egrep '[1-9]$' >/dev/null ; then
    umount $d
    fstr+=",$d"
    rostr+=",1"
  fi
done
fstr=${fstr:1} # strip leading comma
rostr=${rostr:1} # strip leading comma
echo "$fstr" >/tmp/usbexports # save for later r/w export

# now export it
vend=$(( 0x1337 )) # pick your favorite vid/pid
prod=$(( 0x1337 ))
echo "$vend" >/tmp/usbvend # save vid/pid for r/w export
echo "$prod" >/tmp/usbprod
modprobe g_multi file=$fstr cdrom=0 stall=0 ro=$rostr \
  removable=1 nofua=1 idVendor=$vend idProduct=$prod
```

A.16 install.sh (4Deck – Dr. Polstra)

```
#!/bin/bash
#
# Install script for 4deck addon to "The Deck"
# This script will install udev rules which will turn a USB hub
# into a magic hub.  Every block device connected to the magic hub
# will be automatically mounted under the /media directory as read only.
# While this was designed to work with "The Deck" it will most likely
# work with most modern Linux distros.  This software is provided as is
# without warranty of any kind, express or implied.  Use at your own
# risk.  The author is not responsible for anything that happens as
# a result of using this software.
#
# Initial version created August 2012 by Dr. Phil Polstra, Sr.
# Version 1.1 created March 2015
#     new versions adds support for a second PID which is required
#     when using USB 3.0 hubs as they actually present as two hubs
#
#
# Author may be contacted at @ppolstra or DrPhil@polstra.org
# Author's site that may have updates http://philpolstra.com
#
# Enough blabbing - let's get on with it!

unset VID
unset PID
unset PID2

function usage {
  echo "usage: sudo $(basename $0) --vid 05e3 --pid 0608 [--pid2 0610]"
  cat <<EOF

Bugs email: "DrPhil at polstra.org"
Required Parameters:
--vid <Vendor ID of USB hub>
--pid <Product ID of USB hub>
Optional Parameters:
--pid2 <Second Product ID of USB 3.0 hub>
EOF
exit
}

function createRule {
  cat > /etc/udev/rules.d/10-protectedmount.rules <<-__EOF__
  ACTION=="add", SUBSYSTEM=="block", KERNEL=="sd?[1-9]",
ATTRS{idVendor}=="${VID}", ATTRS{idProduct}=="${PID}", ENV{PHIL_MOUNT}="1",
ENV{PHIL_DEV}="%k", RUN+="/etc/udev/scripts/protmount.sh %k %n"
  ACTION=="remove", SUBSYSTEM=="block", KERNEL=="sd?[1-9]",
ATTRS{idVendor}=="${VID}", ATTRS{idProduct}=="${PID}",
ENV{PHIL_UNMOUNT}="1", RUN+="/etc/udev/scripts/protmount3.sh %k %n"
  ENV{PHIL_MOUNT}=="1", ENV{UDISKS_PRESENTATION_HIDE}="1",
ENV{UDISKS_AUTOMOUNT_HINT}="never",    RUN+="/etc/udev/scripts/protmount2-
%n.sh"
  ENV{PHIL_MOUNT}!="1", ENV{UDISKS_PRESENTATION_HIDE}="0",
ENV{UDISKS_AUTOMOUNT_HINT}="always"
  ENV{PHIL_UNMOUNT}=="1", RUN+="/etc/udev/scripts/protmount4-%n.sh"
__EOF__

```

```
51    if [ ! "$PID2" = "" ] ; then
52      cat >> /etc/udev/rules.d/10-protectedmount.rules <<-__EOF__
53      ACTION=="add", SUBSYSTEM=="block", KERNEL=="sd?[1-9]",
      ATTRS{idVendor}=="${VID}", ATTRS{idProduct}=="${PID2}",
      ENV{PHIL_MOUNT}="1", ENV{PHIL_DEV}="%k",
      RUN+="/etc/udev/scripts/protmount.sh %k %n"
54      ACTION=="remove", SUBSYSTEM=="block", KERNEL=="sd?[1-9]",
      ATTRS{idVendor}=="${VID}", ATTRS{idProduct}=="${PID2}",
      ENV{PHIL_UNMOUNT}="1", RUN+="/etc/udev/scripts/protmount3.sh %k %n"
55      ENV{PHIL_MOUNT}=="1", ENV{UDISKS_PRESENTATION_HIDE}="1",
      ENV{UDISKS_AUTOMOUNT_HINT}="never",    RUN+="/etc/udev/scripts/protmount2-
      %n.sh"
56      ENV{PHIL_MOUNT}!="1", ENV{UDISKS_PRESENTATION_HIDE}="0",
      ENV{UDISKS_AUTOMOUNT_HINT}="always"
57      ENV{PHIL_UNMOUNT}=="1", RUN+="/etc/udev/scripts/protmount4-%n.sh"
58    __EOF__
59    fi
60
61    }
62
63    function copyScripts {
64      if [ ! -d "/etc/udev/scripts" ] ; then
65        mkdir /etc/udev/scripts
66      fi
67      cp ./protmount*.sh /etc/udev/scripts/.
68    }
69
70    # parse commandline options
71    while [ ! -z "$1" ]; do
72      case $1 in
73        -h|--help)
74          usage
75          ;;
76        --vid)
77          VID="$2"
78          ;;
79        --pid)
80          PID="$2"
81          ;;
82        --pid2)
83          PID2="$2"
84          ;;
85       esac
86       shift
87    done
88
89    # now actually do something
90    createRule
91    copyScripts
```

A.17 Sicherungs-Logs: DIY-USB-WB

Imation Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: DIY_USB_WB_Imation_1
Unique description: DIY USB WB - Imation Test 1
Examiner: CP
Notes: Dateioperationen

--------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/DIY_USB_Imager/Imation_Test_1/Imation_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1018
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3913728
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Wed May 25 14:59:40 2022
 Acquisition finished:  Thu May 26 02:54:08 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/DIY_USB_Imager/Imation_Test_1/Imation_1.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: DIY_USB_WB_Imation_2
Unique description: DIY USB WB - Imation Test 2
Examiner: CP
Notes: Partitionierung

--------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/DIY_USB_Imager/Imation_Test_2/Imation_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1018
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3913728
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Sun May 29 16:10:43 2022
 Acquisition finished:  Mon May 30 03:57:00 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/DIY_USB_Imager/Imation_Test_2/Imation_2.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: DIY_USB_WB_Imation_3
Unique description: DIY USB WB - Imation Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/DIY_USB_Imager/Imation_Test_3/Imation_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1018
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3913728
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Mon May 30 06:46:58 2022
 Acquisition finished:  Mon May 30 18:33:41 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/DIY_USB_Imager/Imation_Test_3/Imation_3.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: DIY_WB_Emtec_1
Unique description: DIY WB - Emtec Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Polstra_DIY_WB/Emtec_Test_1/Emtec_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Tue Jun  7 06:38:54 2022
 Acquisition finished:  Thu Jun  9 03:01:10 2022
 Segment list:
  /home/prosch/Projekt_II/Polstra_DIY_WB/Emtec_Test_1/Emtec_1.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: DIY_WB_Emtec_2
Unique description: DIY WB - Emtec Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Polstra_DIY_WB/Emtec_Test_2/Emtec_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Thu Jun  9 06:12:57 2022
 Acquisition finished:  Sat Jun 11 02:23:48 2022
 Segment list:
  /home/prosch/Projekt_II/Polstra_DIY_WB/Emtec_Test_2/Emtec_2.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: DIY_WB_Emtec_3
Unique description: DIY WB - Emtec Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Polstra_DIY_WB/Emtec_Test_3/Emtec_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sat Jun 11 04:28:55 2022
 Acquisition finished:  Mon Jun 13 00:21:35 2022
 Segment list:
  /home/prosch/Projekt_II/Polstra_DIY_WB/Emtec_Test_3/Emtec_3.E01
```

A.18 Sicherungs-Logs: Firebrick3

WD Test 1 (Segment list gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Firebrick_WD_1
Unique description: Firebrick3 - WD Test 1
Examiner: CP
Notes: Dateioperationen

--------------------------------------------------------------

Information for /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun  3 18:08:11 2022
 Acquisition finished:  Fri Jun  3 20:02:20 2022
 Segment list:
  /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_1.E01
...
  /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_1.E83
```

WD Test 2 (Segment list gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Firebrick_WD_2
Unique description: Firebrick3 - WD Test 2
Examiner: CP
Notes: Partitionierung

--------------------------------------------------------------

Information for /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_2/WD_Test_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun  3 20:22:06 2022
 Acquisition finished:  Fri Jun  3 22:16:06 2022
```

```
 Segment list:
  /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_2/WD_Test_2.E01
...
  /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_2/WD_Test_2.E83
```

WD Test 3 (Segment list gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Firebrick_WD_3
Unique description: Firebrick3 - WD Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_3/WD_Test_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun  3 22:20:40 2022
 Acquisition finished:  Sat Jun  4 00:14:42 2022
 Segment list:
  /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_3/WD_Test_3.E01
...
  /home/prosch/Projekt_II/Test/Firebrick3/WD_Test_3/WD_Test_3.E83
```

Seagate Test 1 (Segment list gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Firebrick_Seagate_1
Unique description: Firebrick3 - Seagate Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_1/Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a
```

```
Image Information:
 Acquisition started:   Sat Jun  4 10:42:52 2022
 Acquisition finished:  Sat Jun  4 12:20:47 2022
 Segment list:
  /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_1/Seagate_HDD_1.E01
  ...
  /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_1/Seagate_HDD_1.E83
```

Seagate Test 2 (Segment list gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Firebrick_Seagate_2
Unique description: Firebrick3 - Seagate Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_2/Seagate_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Sat Jun  4 12:37:05 2022
 Acquisition finished:  Sat Jun  4 14:15:21 2022
 Segment list:
  /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_2/Seagate_HDD_2.E01
...
  /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_2/Seagate_HDD_2.E83
```

Seagate Test 3 (Segment list gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Firebrick_Seagate_3
Unique description: Firebrick3 - Seagate Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_3/Seagate_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
```

```
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Sat Jun  4 14:16:35 2022
 Acquisition finished:  Sat Jun  4 15:54:29 2022
 Segment list:
  /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_3/Seagate_HDD_3.E01
...
  /home/prosch/Projekt_II/Test/Firebrick3/Seagate_Test_3/Seagate_HDD_3.E83
```

A.19 Sicherungs-Logs: UDeck (Beaglebone Black)

Imation Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_Imation_1
Unique description: Udeck_Beagle - Imation Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Imation_Test_1/Imation_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911617
 Source data size: 1909 MB
 Sector count:    3911617
[Computed Hashes]
 MD5 checksum:    2c57db203873a6b4fa4e8b1c786259bf
 SHA1 checksum:   1ee6da20a827f0a7d6d46a95c506f4c7f78ffff8

Image Information:
 Acquisition started:   Wed Jun  1 07:50:48 2022
 Acquisition finished:  Wed Jun  1 07:54:28 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Imation_Test_1/Imation_1.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_Imation_2
Unique description: Udeck_Beagle - Imation Test 2
Examiner: CP
Notes: Partitionierung

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Imation_Test_2/Imation_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
```

```
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911617
 Source data size: 1909 MB
 Sector count:    3911617
[Computed Hashes]
 MD5 checksum:    2c57db203873a6b4fa4e8b1c786259bf
 SHA1 checksum:   1ee6da20a827f0a7d6d46a95c506f4c7f78ffff8

Image Information:
 Acquisition started:   Wed Jun  1 08:09:14 2022
 Acquisition finished:  Wed Jun  1 08:12:55 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Imation_Test_2/Imation_2.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_Imation_3
Unique description: Udeck_Beagle - Imation Test 3
Examiner: CP
Notes: Hexedit

---------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Imation_Test_3/Imation_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911617
 Source data size: 1909 MB
 Sector count:    3911617
[Computed Hashes]
 MD5 checksum:    2c57db203873a6b4fa4e8b1c786259bf
 SHA1 checksum:   1ee6da20a827f0a7d6d46a95c506f4c7f78ffff8

Image Information:
 Acquisition started:   Wed Jun  1 08:22:38 2022
 Acquisition finished:  Wed Jun  1 08:26:19 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Imation_Test_3/Imation_3.E01
```

Sandisk Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_SanDisk_1
Unique description: Udeck_Beagle - SanDisk Test 1
Examiner: CP
Notes: Dateioperationen

---------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_1/SanDisk_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
```

```
[Drive Geometry]
 Cylinders: 29339
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60086272
 Source data size: 29339 MB
 Sector count:    60086272
[Computed Hashes]
 MD5 checksum:    45e55057aafb67800858d3319bf8b17d
 SHA1 checksum:   c577b649cbfefe185bf35783d46c0850ca6beb54

Image Information:
 Acquisition started:   Wed Jun  1 08:35:13 2022
 Acquisition finished:  Wed Jun  1 09:31:38 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_1/SanDisk_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_1/SanDisk_1.E12
```

Sandisk Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_SanDisk_2
Unique description: Udeck_Beagle - SanDisk Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_2/SanDisk_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29339
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60086272
 Source data size: 29339 MB
 Sector count:    60086272
[Computed Hashes]
 MD5 checksum:    45e55057aafb67800858d3319bf8b17d
 SHA1 checksum:   c577b649cbfefe185bf35783d46c0850ca6beb54

Image Information:
 Acquisition started:   Wed Jun  1 09:53:35 2022
 Acquisition finished:  Wed Jun  1 10:50:01 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_2/SanDisk_2.E01
  ...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_2/SanDisk_2.E12
```

Sandisk Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_SanDisk_3
Unique description: Udeck_Beagle - SanDisk Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_3/SanDisk_3:
```

```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29339
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60086272
 Source data size: 29339 MB
 Sector count:    60086272
[Computed Hashes]
 MD5 checksum:    45e55057aafb67800858d3319bf8b17d
 SHA1 checksum:   c577b649cbfefe185bf35783d46c0850ca6beb54

Image Information:
 Acquisition started:   Wed Jun  1 11:09:19 2022
 Acquisition finished:  Wed Jun  1 12:05:47 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_3/SanDisk_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/SanDisk_Test_3/SanDisk_3.E12
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Udeck_Beagle_Seagate_1
Unique description: Udeck_Beagle - Seagate Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Seagate_Test_1/Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976771072
 Source data size: 476939 MB
 Sector count:    976771072
[Computed Hashes]
 MD5 checksum:    3bdd69fe9d5450e754146446757f45e6
 SHA1 checksum:   16bc79b38ba52f31d94fbfb0b05ba3d70b550439

Image Information:
 Acquisition started:   Wed Jun  1 12:47:39 2022
 Acquisition finished:  Thu Jun  2 02:46:01 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Seagate_Test_1/Seagate_HDD_1.E01
 ...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Udeck_Beagle/Seagate_Test_1/Seagate_HDD_1.E83
```

A.20 Sicherungs-Logs: Magic USB-Hub (4Deck)

Imation Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Imation_1
Unique description: 4Deck - Imation Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Imation_Test_1/Imation_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1018
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3913728
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Mon May 30 18:57:27 2022
 Acquisition finished:  Mon May 30 18:58:59 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Imation_Test_1/Imation_1.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Imation_2
Unique description: 4Deck - Imation Test 2
Examiner: CP
Notes: Partitionierung

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Imation_Test_2/Imation_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1018
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3913728
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    a3e8183e0416388b40fec7851e28b2f4
 SHA1 checksum:   14181de212bc73405697b2fe95f6b9c2b1c6ad7d

Image Information:
 Acquisition started:   Mon May 30 19:07:34 2022
 Acquisition finished:  Mon May 30 19:09:06 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Imation_Test_2/Imation_2.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Imation_3
Unique description: 4Deck - Imation Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Imation_Test_3/Imation_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1018
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3913728
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    74d9dda28e6a1ff0b4b8242e41e3053c
 SHA1 checksum:   05deeb9077145fd00b06db711c3204be748c15f8

Image Information:
 Acquisition started:   Mon May 30 20:41:52 2022
 Acquisition finished:  Mon May 30 20:43:24 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Imation_Test_3/Imation_3.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Emtec_1
Unique description: 4Deck - Emtec Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Emtec_Test_1/Emtec_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Tue May 31 08:40:03 2022
 Acquisition finished:  Tue May 31 08:48:32 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Emtec_Test_1/Emtec_1.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Emtec_2
Unique description: 4Deck - Emtec Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Emtec_Test_2/Emtec_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Tue May 31 09:15:11 2022
 Acquisition finished:  Tue May 31 09:23:40 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Emtec_Test_2/Emtec_2.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Emtec_3
Unique description: 4Deck - Emtec Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Emtec_Test_3/Emtec_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Tue May 31 11:47:44 2022
 Acquisition finished:  Tue May 31 11:56:13 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Emtec_Test_3/Emtec_3.E01
```

Sandisk Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_SanDisk_1
Unique description: 4Deck - SanDisk Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_1/SanDisk_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29340
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60088320
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Mon May 30 21:05:41 2022
 Acquisition finished:  Mon May 30 21:13:54 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_1/SanDisk_1.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_1/SanDisk_1.E12
```

Sandisk Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_SanDisk_2
Unique description: 4Deck - SanDisk Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_2/SanDisk_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29340
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60088320
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Tue May 31 03:28:26 2022
 Acquisition finished:  Tue May 31 03:36:39 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_2/SanDisk_2.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_2/SanDisk_2.E12
```

Sandisk Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_SanDisk_3
Unique description: 4Deck - SanDisk Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_3/SanDisk_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29340
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60088320
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Tue May 31 07:03:21 2022
 Acquisition finished:  Tue May 31 07:11:34 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_3/SanDisk_3.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/SanDisk_Test_3/SanDisk_3.E12
```

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_WD_HDD_1
Unique description: 4Deck - WD_HDD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_1/WD_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue May 31 12:01:01 2022
 Acquisition finished:  Tue May 31 13:49:55 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_1/WD_HDD_1.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_1/WD_HDD_1.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_WD_HDD_2
Unique description: 4Deck - WD_HDD Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_2/WD_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue May 31 14:13:19 2022
 Acquisition finished:  Tue May 31 16:02:13 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_2/WD_HDD_2.E01
…
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_2/WD_HDD_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_WD_HDD_3
Unique description: 4Deck - WD_HDD Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_3/WD_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue May 31 16:05:34 2022
 Acquisition finished:  Tue May 31 17:54:29 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_3/WD_HDD_3.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/WD_Test_3/WD_HDD_3.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Seagate_HDD_1
Unique description: 4Deck - Seagate_HDD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_1/Seagte_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Tue May 31 18:15:34 2022
 Acquisition finished:  Tue May 31 19:35:09 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_1/Seagte_HDD_1.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_1/Seagte_HDD_1.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Seagate_HDD_2
Unique description: 4Deck - Seagate_HDD Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_2/Seagte_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Tue May 31 19:36:34 2022
 Acquisition finished:  Tue May 31 20:56:07 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_2/Seagte_HDD_2.E01
  ...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_2/Seagte_HDD_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: 4Deck_Seagate_HDD_3
Unique description: 4Deck - Seagate_HDD Test 3
Examiner: CP
Notes: Dateioperationen

--------------------------------------------------------------

Information for /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_3/Seagte_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Tue May 31 21:07:58 2022
 Acquisition finished:  Tue May 31 22:27:35 2022
 Segment list:
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_3/Seagte_HDD_3.E01
...
  /media/xubuntu/Daten/Projekt2_Imaging_Tests/4Deck_Hub/Seagate_Test_3/Seagte_HDD_3.E83
```

A.21 Sicherungs-Logs: Sharkoon DriveLink Combo USB 3.0 V2

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Sharkoon_WD_1
Unique description: Sharkoon - WD Test 1
Examiner: CP
Notes: Dateioperationen

--------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_1/WD_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
```

```
 Acquisition started:   Thu Jun  2 11:26:52 2022
 Acquisition finished:  Thu Jun  2 13:16:03 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_1/WD_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_1/WD_HDD_1.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Sharkoon_WD_2
Unique description: Sharkoon - WD Test 2
Examiner: CP
Notes: Partitionierung

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_2/WD_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Thu Jun  2 13:21:02 2022
 Acquisition finished:  Thu Jun  2 15:10:05 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_2/WD_HDD_2.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_2/WD_HDD_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Sharkoon_WD_3
Unique description: Sharkoon - WD Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_3/WD_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
```

```
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Thu Jun  2 17:48:59 2022
 Acquisition finished:  Thu Jun  2 19:38:06 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_3/WD_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/WD_Test_3/WD_HDD_3.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Sharkoon_Seagate_1
Unique description: Sharkoon - Seagate Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_1/Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Thu Jun  2 19:45:58 2022
 Acquisition finished:  Thu Jun  2 21:06:10 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_1/Seagate_HDD_1.E01
  ...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_1/Seagate_HDD_1.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Sharkoon_Seagate_2
Unique description: Sharkoon - Seagate Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_2/Seagate_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
```

```
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Thu Jun  2 21:08:01 2022
 Acquisition finished:  Thu Jun  2 22:28:13 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_2/Seagate_HDD_2.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_2/Seagate_HDD_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Sharkoon_Seagate_3
Unique description: Sharkoon - Seagate Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_3/Seagate_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Thu Jun  2 22:38:49 2022
 Acquisition finished:  Thu Jun  2 23:59:04 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_3/Seagate_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Sharkoon/Seagate_Test_3/Seagate_HDD_3.E83
```

A.22 Sicherungs-Logs: Delock 62652 SATA / USB Converter

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Delock_WD_1
Unique description: Delock - WD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_1/WD_HDD_1:

Physical Evidentiary Item (Source) Information:
```

```
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun  3 10:57:51 2022
 Acquisition finished:  Fri Jun  3 12:56:42 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_1/WD_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_1/WD_HDD_1.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Delock_WD_2
Unique description: Delock - WD Test 2
Examiner: CP
Notes: Partitionierung

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_2/WD_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun  3 13:32:37 2022
 Acquisition finished:  Fri Jun  3 15:21:41 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_2/WD_HDD_2.E01
  ...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_2/WD_HDD_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Delock_WD_3
Unique description: Delock - WD Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------
```

```
Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_3/WD_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun  3 15:26:57 2022
 Acquisition finished:  Fri Jun  3 17:16:03 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_3/WD_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/WD_Test_3/WD_HDD_3.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Delock_Seagate_1
Unique description: Delock - Seagate Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_1/Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Fri Jun  3 18:18:06 2022
 Acquisition finished:  Fri Jun  3 19:38:23 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_1/Seagate_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_1/Seagate_HDD_1.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Delock_Seagate_2
Unique description: Delock - Seagate Test 2
Examiner: CP
Notes: Dateioperationen
```

```
---------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_2/Seagate_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    f8a24a8572294e16d54d85bcb1155bb2
 SHA1 checksum:   e7184f9f0dd2ab8eaac39f746995b533da6249bb

Image Information:
 Acquisition started:   Fri Jun  3 20:17:55 2022
 Acquisition finished:  Fri Jun  3 22:23:17 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_2/Seagate_HDD_2.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_2/Seagate_HDD_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Delock_Seagate_3
Unique description: Delock - Seagate Test 3
Examiner: CP
Notes: Dateioperationen

---------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_3/Seagate_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Sat Jun  4 00:06:55 2022
 Acquisition finished:  Sat Jun  4 01:27:44 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_3/Seagate_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Delock/Seagate_Test_3/Seagate_HDD_3.E83
```

A.23 Sicherungs-Logs: WiebeTech Forensic Ultradock V5

Imation Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Imation_1
Unique description: WiebeTech - Imation Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Imation_Test_1\Imation_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.913.728
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A30A030AA618B3
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Sat Jun 04 14:14:48 2022
 Acquisition finished:  Sat Jun 04 14:16:46 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Imation_Test_1\Imation_1.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Imation_2
Unique description: WiebeTech - Imation Test 2
Examiner: CP
Notes: Partitionierung

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Imation_Test_2\Imation_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.913.728
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A30A030AA618B3
 Drive Interface Type: USB
 Removable drive: True
```

```
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Sat Jun 04 14:22:47 2022
 Acquisition finished:  Sat Jun 04 14:24:44 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Imation_Test_2\Imation_2.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Imation_3
Unique description: WiebeTech - Imation Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Imation_Test_3\Imation_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.913.728
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A30A030AA618B3
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1911 MB
 Sector count:    3913728
[Computed Hashes]
 MD5 checksum:    88746e861790fea1ebd4dcdfc39b4e60
 SHA1 checksum:   28e7672958273cfacf0ca39fa631c6c4276af35f

Image Information:
 Acquisition started:   Sat Jun 04 14:28:42 2022
 Acquisition finished:  Sat Jun 04 14:30:40 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Imation_Test_3\Imation_3.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Emtec_1
Unique description: WiebeTech - Emtec Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Emtec_Test_1\Emtec_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
```

```
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 163601242
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sat Jun 04 18:39:02 2022
 Acquisition finished:  Sat Jun 04 18:51:37 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Emtec_Test_1\Emtec_1.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Emtec_2
Unique description: WiebeTech - Emtec Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Emtec_Test_2\Emtec_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 163601242
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sat Jun 04 20:28:26 2022
 Acquisition finished:  Sat Jun 04 20:40:59 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Emtec_Test_2\Emtec_2.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Emtec_3
Unique description: WiebeTech - Emtec Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------
```

```
Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Emtec_Test_3\Emtec_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 163601242
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sun Jun 05 00:19:00 2022
 Acquisition finished:  Sun Jun 05 00:30:59 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Emtec_Test_3\Emtec_3.E01
```

Sandisk Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Sandisk_1
Unique description: WiebeTech - Sandisk Test 1
Examiner: CP
Notes: Dateioperationen

---------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_1\Sandisk_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101f15ed552cbc7662b
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Sat Jun 04 14:53:56 2022
 Acquisition finished:  Sat Jun 04 15:11:28 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_1\Sandisk_1.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_1\Sandisk_1.E12
```

Sandisk Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Sandisk_2
Unique description: WiebeTech - Sandisk Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_2\Sandisk_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101f15ed552cbc7662b
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Sat Jun 04 15:12:17 2022
 Acquisition finished:  Sat Jun 04 15:29:53 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_2\Sandisk_2.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_2\Sandisk_2.E12
```

Sandisk Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Sandisk_3
Unique description: WiebeTech - Sandisk Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_3\Sandisk_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101f15ed552cbc7662b
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
```

```
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Sat Jun 04 16:45:50 2022
 Acquisition finished:  Sat Jun 04 17:03:27 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_3\Sandisk_3.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Sandisk_Test_3\Sandisk_3.E12
```

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_WD_1
Unique description: WiebeTech - WD HDD Test 1
Examiner: CP
Notes: Dateioperationen

--------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_1\WD_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: WDC WD50 00BPVT-24HXZT3 USB Device
 Drive Serial Number: 20200904
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Sun Jun 05 11:18:44 2022
 Acquisition finished:  Sun Jun 05 13:29:44 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_1\WD_HDD_1.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_1\WD_HDD_1.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_WD_2
Unique description: WiebeTech - WD HDD Test 2
Examiner: CP
Notes: Dateioperationen

--------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_2\WD_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
```

```
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: WDC WD50 00BPVT-24HXZT3 USB Device
 Drive Serial Number: 20200904
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Sun Jun 05 13:35:02 2022
 Acquisition finished:  Sun Jun 05 15:46:05 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_2\WD_HDD_2.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_2\WD_HDD_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_WD_3
Unique description: WiebeTech - WD HDD Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_3\WD_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: WDC WD50 00BPVT-24HXZT3 USB Device
 Drive Serial Number: 20200904
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Sun Jun 05 15:54:07 2022
 Acquisition finished:  Sun Jun 05 18:05:09 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_3\WD_HDD_3.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\WD_Test_3\WD_HDD_3.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Seagate_1
Unique description: WiebeTech - Seagate HDD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_1\Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ST500DM0 02-1BD142 USB Device
 Drive Serial Number: 20200904
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Sun Jun 05 21:17:13 2022
 Acquisition finished:  Sun Jun 05 23:06:47 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_1\Seagate_HDD_1.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_1\Seagate_HDD_1.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Seagate_2
Unique description: WiebeTech - Seagate HDD Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_2\Seagate_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ST500DM0 02-1BD142 USB Device
 Drive Serial Number: 20200904
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
```

```
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Sun Jun 05 23:48:08 2022
 Acquisition finished:  Mon Jun 06 01:37:03 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_2\Seagate_HDD_2.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_2\Seagate_HDD_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Wiebetech_Seagate_3
Unique description: WiebeTech - Seagate HDD Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_3\Seagate_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ST500DM0 02-1BD142 USB Device
 Drive Serial Number: 20200904
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Mon Jun 06 01:39:41 2022
 Acquisition finished:  Mon Jun 06 03:28:30 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_3\Seagate_HDD_3.E01
...
  E:\Projekt2_Imaging_Tests\WiebeTech_USB\Seagate_Test_3\Seagate_HDD_3.E83
```

A.24 Sicherungs-Logs: Tableau T3iu Forensic SATA Imaging Bay

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_WD_1
Unique description: Tableau - WD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_1/WD_HDD_1:

Physical Evidentiary Item (Source) Information:
```

```
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Mon Jun  6 13:19:32 2022
 Acquisition finished:  Mon Jun  6 15:15:39 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_1/WD_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_1/WD_HDD_1.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_WD_2
Unique description: Tableau - WD Test 2
Examiner: CP
Notes: Partitionierung

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_2/WD_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Mon Jun  6 15:29:32 2022
 Acquisition finished:  Mon Jun  6 17:18:38 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_2/WD_HDD_2.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_2/WD_HDD_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_WD_3
Unique description: Tableau - WD Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------
```

```
Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_3/WD_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Mon Jun  6 17:31:39 2022
 Acquisition finished:  Mon Jun  6 19:20:40 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_3/WD_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/WD_Test_3/WD_HDD_3.E83
```

WD Test Windows

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_WD_1
Unique description: Tableau - WD HDD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for E:\Projekt2_Imaging_Tests\Tableau_Drive_Bay\WD_Test_1\WD_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: WDC WD50 00BPVT-2 SCSI Disk Device
 Drive Serial Number:      WD-WX81E81WFC10
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Mon Jun 06 10:53:05 2022
 Acquisition finished:  Mon Jun 06 13:11:42 2022
 Segment list:
  E:\Projekt2_Imaging_Tests\Tableau_Drive_Bay\WD_Test_1\WD_HDD_1.E01
...
  E:\Projekt2_Imaging_Tests\Tableau_Drive_Bay\WD_Test_1\WD_HDD_1.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_Seagate_1
Unique description: Tableau - Seagate Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_1/Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Mon Jun  6 21:46:53 2022
 Acquisition finished:  Mon Jun  6 23:07:05 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_1/Seagate_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_1/Seagate_HDD_1.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_Seagate_2
Unique description: Tableau - Seagate Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_2/Seagate_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Mon Jun  6 23:11:51 2022
 Acquisition finished:  Tue Jun  7 00:32:22 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_2/Seagate_HDD_2.E01
```

```
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_2/Seagate_HDD_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Tableau_Seagate_3
Unique description: Tableau - Seagate Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_3/Seagate_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Tue Jun  7 05:28:47 2022
 Acquisition finished:  Tue Jun  7 06:48:56 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_3/Seagate_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Tableau_Drive_Bay/Seagate_Test_3/Seagate_HDD_3.E83
```

A.25 Sicherungs-Logs: WiebeTech Forensic Ultradock V5

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Ultradock_WD_1
Unique description: Ultradock - WD Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_1/WD_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
```

```
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Wed Jun  8 15:50:40 2022
 Acquisition finished:  Wed Jun  8 17:53:52 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_1/WD_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_1/WD_HDD_1.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Ultradock_WD_2
Unique description: Ultradock - WD Test 2
Examiner: CP
Notes: Formatierung

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_2/WD_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Wed Jun  8 19:19:17 2022
 Acquisition finished:  Wed Jun  8 21:08:36 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_2/WD_HDD_2.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_2/WD_HDD_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Ultradock_WD_3
Unique description: Ultradock - WD Test 3
Examiner: CP
Notes: Hexedit

------------------------------------------------------------

Information for /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_3/WD_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
```

```
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Wed Jun  8 21:50:44 2022
 Acquisition finished:  Wed Jun  8 23:40:00 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_3/WD_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/WD_Test_3/WD_HDD_3.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Ultradock_Seagate_1
Unique description: Ultradock - Seagate Test 1
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_1/Seagate_HDD_1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Wed Jun  8 23:44:35 2022
 Acquisition finished:  Thu Jun  9 01:05:04 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_1/Seagate_HDD_1.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_1/Seagate_HDD_1.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Ultradock_Seagate_2
Unique description: Ultradock - Seagate Test 2
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_2/Seagate_HDD_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
```

```
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Thu Jun  9 01:48:20 2022
 Acquisition finished:  Thu Jun  9 03:08:46 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_2/Seagate_HDD_2.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_2/Seagate_HDD_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: Ultradock_Seagate_3
Unique description: Ultradock - Seagate Test 3
Examiner: CP
Notes: Dateioperationen

------------------------------------------------------------

Information for
/run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_3/Seagate_HDD_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Thu Jun  9 05:32:41 2022
 Acquisition finished:  Thu Jun  9 06:53:10 2022
 Segment list:
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_3/Seagate_HDD_3.E01
...
  /run/media/prosch/Daten/Projekt2_Imaging_Tests/Forensic_Ultradock/Seagate_Test_3/Seagate_HDD_3.E83
```

A.26 Sicherungs-Logs: Windows Registry WriteBlock

Imation Test Dateioperationen

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: imation
Examiner: YS
Notes: Versuch Dateioperationen

------------------------------------------------------------
```

```
Information for C:\Users\Yannick\Desktop\APL\1 WinReg\_Datei-OP\imation_WinReg_Dateioperationen:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Wed Jun  8 15:22:15 2022
 Acquisition finished:  Wed Jun  8 15:24:17 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\_Datei-OP\imation_WinReg_Dateioperationen.E01
```

Imation Test Formatierung

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: imation
Examiner: YS
Notes: Versuch Formatierung

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\_Format\imation_WinReg_Format:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    090cd04df9bbf30d88b925089fa7d1a0
 SHA1 checksum:   6a7fe6aed9c25bc921e118a2ba1707711a8a8010

Image Information:
 Acquisition started:   Wed Jun  8 15:28:57 2022
 Acquisition finished:  Wed Jun  8 15:31:00 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\_Format\imation_WinReg_Format.E01
```

Imation Test Hexedit

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: imation
```

```
Examiner: YS
Notes: Versuch Hex Manipulation

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\_HEX\imation_WinReg_Hex:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    b9b1ea77d493db362edd7451bcb8ac26
 SHA1 checksum:   e6f8c508ca96e0c13b59d050c464c92800f1ae12

Image Information:
 Acquisition started:   Wed Jun  8 15:12:28 2022
 Acquisition finished:  Wed Jun  8 15:14:30 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\_HEX\imation_WinReg_Hex.E01
```

Imation Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: imation
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\1\imation_WinReg_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Tue Jun  7 21:19:19 2022
 Acquisition finished:  Tue Jun  7 21:21:21 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\1\imation_WinReg_Block.E01
```

Imation Test 2

```
Case Information:
```

```
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: imation
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\2\imation_WinReg_Block_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Tue Jun  7 21:24:38 2022
 Acquisition finished:  Tue Jun  7 21:26:39 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\imation_WinReg_Block_2.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: imation
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\3\imation_WinReg_Block_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Tue Jun  7 21:29:53 2022
 Acquisition finished:  Tue Jun  7 21:31:52 2022
```

```
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\imation_WinReg_Block_3.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry WriteBlock
Unique description: EMTEC USB
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 Prod EMTEC\EMTEC_WinReg_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 173506292
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sat May 28 12:15:18 2022
 Acquisition finished:  Sat May 28 12:24:56 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 Prod EMTEC\EMTEC_WinReg_Block.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: EMTEC
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\2\EMTEC_WinReg_Block_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 173506292
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
```

```
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Wed Jun  8 16:32:58 2022
 Acquisition finished:  Wed Jun  8 16:42:33 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\EMTEC_WinReg_Block_2.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Kex
Unique description: EMTEC
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\3\EMTEC_WinReg_Block_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 173506292
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Wed Jun  8 16:46:01 2022
 Acquisition finished:  Wed Jun  8 16:55:36 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\EMTEC_WinReg_Block_3.E01
```

Sandisk Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry WriteBlock
Unique description: SanDisk
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\4 Prod SanDisk\SanDisk_WinReg_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
```

```
 Drive Serial Number: 0101a6356cfde66d7de0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Sat May 28 12:56:07 2022
 Acquisition finished:  Sat May 28 13:03:31 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\4 Prod SanDisk\SanDisk_WinReg_Block.E01
…
  C:\Users\Yannick\Desktop\APL\4 Prod SanDisk\SanDisk_WinReg_Block.E12
```

Sandisk Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: SanDisk
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\2\SanDisk_WinReg_Block_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101a6356cfde66d7de0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Wed Jun  8 17:00:18 2022
 Acquisition finished:  Wed Jun  8 17:07:48 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\SanDisk_WinReg_Block_2.E01
….
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\SanDisk_WinReg_Block_2.E12
```

Sandisk Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: SanDisk
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\3\SanDisk_WinReg_Block_3:

Physical Evidentiary Item (Source) Information:
```

```
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101a6356cfde66d7de0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Wed Jun  8 17:22:34 2022
 Acquisition finished:  Wed Jun  8 17:30:10 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\SanDisk_WinReg_Block_3.E01
…
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\SanDisk_WinReg_Block_3.E12
```

WD Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: WD HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\1\WD_WinReg_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue Jun  7 23:30:08 2022
 Acquisition finished:  Wed Jun  8 01:30:54 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\1\WD_WinReg_Block.E01
…  C:\Users\Yannick\Desktop\APL\1 WinReg\1\WD_WinReg_Block.E80
```

WD Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
```

```
Unique description: WD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\2\WD_WinReg_Block_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Wed Jun  8 08:32:28 2022
 Acquisition finished:  Wed Jun  8 10:33:22 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\WD_WinReg_Block_2.E01
…
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\WD_WinReg_Block_2.E80
```

WD Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: WD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\3\WD_WinReg_Block_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Wed Jun  8 11:31:22 2022
 Acquisition finished:  Wed Jun  8 13:32:17 2022
 Segment list:
```

```
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\WD_WinReg_Block_3.E01
…
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\WD_WinReg_Block_3.E80
```

Seagate Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: Seagate
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\1\Seagate_WinReg_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Wed Jun  8 18:58:55 2022
 Acquisition finished:  Wed Jun  8 20:23:43 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\1\Seagate_WinReg_Block.E01
…
  C:\Users\Yannick\Desktop\APL\1 WinReg\1\Seagate_WinReg_Block.E80
```

Seagate Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: Windows Registry Key
Unique description: Seagate
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\2\Seagate_WinReg_Block_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
```

```
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Wed Jun  8 21:24:40 2022
 Acquisition finished:  Wed Jun  8 22:53:32 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\Seagate_WinReg_Block_2.E01
…
  C:\Users\Yannick\Desktop\APL\1 WinReg\2\Seagate_WinReg_Block_2.E80
```

Seagate Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Forensik II
Evidence Number: Windows Registry Key
Unique description: Seagate
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\1 WinReg\3\Seagate_WinReg_Block_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Thu Jun  9 00:26:15 2022
 Acquisition finished:  Thu Jun  9 01:50:13 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\Seagate_WinReg_Block_3.E01
…
  C:\Users\Yannick\Desktop\APL\1 WinReg\3\Seagate_WinReg_Block_3.E80
```

A.27 Sicherungs-Logs: SAFEBlock

Imation Test Dateiooperationen

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: imation
Examiner: YS
Notes: Versuch Dateioperationen

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\_Datei-OP\imation_SAFEBlock_Dateioperationen:
```

```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Wed Jun  8 14:31:09 2022
 Acquisition finished:  Wed Jun  8 14:33:12 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\_Datei-OP\imation_SAFEBlock_Dateioperationen.E01
```

Imation Test Formatierung

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: imation
Examiner: YS
Notes: Versuch Formatierung

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\_Format\imation_SAFEBlock_Format:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Wed Jun  8 14:50:08 2022
 Acquisition finished:  Wed Jun  8 14:52:10 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\_Format\imation_SAFEBlock_Format.E01
```

Imation Test Hexedit

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: imation
Examiner: YS
```

```
Notes: Versuch Hex Manipulation

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\_HEX\imation_SAFEBlock_Hex:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Wed Jun  8 14:57:37 2022
 Acquisition finished:  Wed Jun  8 14:59:39 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\_HEX\imation_SAFEBlock_Hex.E01
```

Imation Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFE Block
Unique description: imation
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\imation_SAFEBlock_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Sun May 29 17:23:12 2022
 Acquisition finished:  Sun May 29 17:25:11 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\imation_SAFEBlock_Block.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFE Block
Unique description: imation
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\imation_SAFEBlock_Format:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Sun May 29 18:28:45 2022
 Acquisition finished:  Sun May 29 18:30:49 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\imation_SAFEBlock_Format.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: imation
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\imation_SAFEBlock_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 243
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.911.680
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 07A60103EC77210E
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0
```

```
Image Information:
 Acquisition started:   Tue Jun  7 20:45:03 2022
 Acquisition finished:  Tue Jun  7 20:47:04 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\imation_SAFEBlock_3.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFE Block
Unique description: EMTEC USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\EMTEC_SAFEBlock_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 173506292
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sun May 29 10:04:44 2022
 Acquisition finished:  Sun May 29 10:14:17 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\EMTEC_SAFEBlock_Block.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFE Block
Unique description: EMTEC
Examiner: YS
Notes: Formatierungsversuch

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\EMTEC_SAFEBlock_Format:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 173506292
 Drive Interface Type: USB
 Removable drive: True
```

```
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Sun May 29 17:54:49 2022
 Acquisition finished:  Sun May 29 18:04:28 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\EMTEC_SAFEBlock_Format.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: EMTEC
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\EMTEC_SAFEBlock_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.267.839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Serial Number: 173506292
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Tue Jun  7 16:00:00 2022
 Acquisition finished:  Tue Jun  7 16:09:37 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\EMTEC_SAFEBlock_3.E01
```

Sandisk Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFE Block
Unique description: SanDisk
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\SanDisk_SAFEBlock_Block:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
```

```
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101a6356cfde66d7de0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Sun May 29 10:17:46 2022
 Acquisition finished:  Sun May 29 10:25:10 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\SanDisk_SAFEBlock_Block.E01
….
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Datei-OP\SanDisk_SAFEBlock_Block.E12
```

Sandisk Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: SanDisk
Examiner: YS
Notes:

---------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\SanDisk_SAFEBlock_Format:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101a6356cfde66d7de0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Sun May 29 18:08:40 2022
 Acquisition finished:  Sun May 29 18:16:19 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\SanDisk_SAFEBlock_Format.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Formatierung\SanDisk_SAFEBlock_Format.E12
```

Sandisk Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: SanDisk
Examiner: YS
Notes:

---------------------------------------------------------------
```

```
Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\SanDisk_SAFEBlock_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60.088.320
[Physical Drive Information]
 Drive Model:  USB  SanDisk 3.2Gen1 USB Device
 Drive Serial Number: 0101a6356cfde66d7de0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Tue Jun  7 15:45:17 2022
 Acquisition finished:  Tue Jun  7 15:52:52 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\SanDisk_SAFEBlock_3.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\SanDisk_SAFEBlock_3.E12
```

WD Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: WD
Examiner: Ys
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue May 31 21:18:41 2022
 Acquisition finished:  Tue May 31 23:19:32 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK.E01
….
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK.E80
```

WD Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: WD HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue Jun  7 07:03:00 2022
 Acquisition finished:  Tue Jun  7 09:03:44 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK_2.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK_2.E80
```

WD Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: WD HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
```

```
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue Jun  7 10:14:51 2022
 Acquisition finished:  Tue Jun  7 12:16:09 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK_3.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\WD_HDD_SAFEBLOCK_3.E80
```

Seagate Test 1

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: Seagate HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK.E01:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Wed Jun  1 06:11:34 2022
 Acquisition finished:  Wed Jun  1 07:36:13 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK.E01.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK.E01.E80
```

Seagate Test 2

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: Seagate HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
```

```
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Mon Jun  6 21:50:07 2022
 Acquisition finished:  Mon Jun  6 23:14:25 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK_2.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK_2.E80
```

Seagate Test 3

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: Projekt II
Evidence Number: SAFEBlock
Unique description: Seagate HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60.801
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976.773.168
[Physical Drive Information]
 Drive Model: ICY BOX IB-AC704-6G USB Device
 Drive Serial Number: 5A0000015102
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Tue Jun  7 13:13:50 2022
 Acquisition finished:  Tue Jun  7 14:37:44 2022
 Segment list:
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK_3.E01
…
  C:\Users\Yannick\Desktop\APL\2 SAFE Block\Seagate_HDD_SAFEBLOCK_3.E80
```

A.28 Sicherungs-Logs: Tsurugi Linux

Imation Test Dateioperationen

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
```

```
Unique description: Test Dateioperationen
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/_Datei-OP/imation_Tsurugi_Datei-OP:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911680
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Sat Jun 11 10:25:29 2022
 Acquisition finished:  Sat Jun 11 10:27:22 2022
 Segment list:
  /images/_Datei-OP/imation_Tsurugi_Datei-OP.E01
```

Imation Test Formatierung

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: Test Formatierung
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/_Format/imation_Tsurugi_Format:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911680
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    63e6476e3a85cb3667a8c67e2b0099b8
 SHA1 checksum:   45244ef3ed7fc48d6e0c26f29c68ff981f4dbef3

Image Information:
 Acquisition started:   Sat Jun 11 10:33:42 2022
 Acquisition finished:  Sat Jun 11 10:35:36 2022
 Segment list:
  /images/_Format/imation_Tsurugi_Format.E01
```

Imation Test Hexedit

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: Test Hexeditor
Examiner: YS
Notes:
```

```
---------------------------------------------------------------

Information for /images/_Hex/imation_Tsurugi_Hex:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911680
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    9bea2599abda24784c0265b778698e68
 SHA1 checksum:   c19c932549fae83f9b590601ab863564737ee7bd

Image Information:
 Acquisition started:   Sat Jun 11 10:47:26 2022
 Acquisition finished:  Sat Jun 11 10:49:19 2022
 Segment list:
  /images/_Hex/imation_Tsurugi_Hex.E01
```

Imation Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: imation USB
Examiner: YS
Notes:

---------------------------------------------------------------

Information for /images/1/imation_tsurugi_ro:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911680
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Thu Jun  9 14:50:36 2022
 Acquisition finished:  Thu Jun  9 14:52:29 2022
 Segment list:
  /images/1/imation_tsurugi_ro.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: imation USB
Examiner: YS
Notes:

---------------------------------------------------------------

Information for /images/2/imation_tsurugi_ro_2:
```

```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911680
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Thu Jun  9 14:59:26 2022
 Acquisition finished:  Thu Jun  9 15:01:19 2022
 Segment list:
  /images/2/imation_tsurugi_ro_2.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: imation USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/3/imation_tsurugi_ro_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1017
 Heads: 62
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 3911680
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Thu Jun  9 15:02:50 2022
 Acquisition finished:  Thu Jun  9 15:04:43 2022
 Segment list:
  /images/3/imation_tsurugi_ro_3.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: EMTEC USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/1/EMTEC_tsurugi_ro:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
```

```
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Thu Jun  9 15:06:55 2022
 Acquisition finished:  Thu Jun  9 15:15:46 2022
 Segment list:
  /images/1/EMTEC_tsurugi_ro.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: EMTEC USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/2/EMTEC_tsurugi_ro_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Thu Jun  9 15:19:10 2022
 Acquisition finished:  Thu Jun  9 15:28:02 2022
 Segment list:
  /images/2/EMTEC_tsurugi_ro_2.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: EMTEC USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/3/EMTEC_tsurugi_ro_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1021
 Heads: 241
 Sectors per Track: 62
```

```
 Bytes per Sector: 512
 Sector Count: 15267839
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Thu Jun  9 15:36:47 2022
 Acquisition finished:  Thu Jun  9 15:45:38 2022
 Segment list:
  /images/3/EMTEC_tsurugi_ro_3.E01
```

Sandisk Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: SanDisk USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/1/SanDisk_tsurugi_ro:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29340
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60088320
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Fri Jun 10 15:34:03 2022
 Acquisition finished:  Fri Jun 10 15:41:54 2022
 Segment list:
  /images/1/SanDisk_tsurugi_ro.E01
...
  /images/1/SanDisk_tsurugi_ro.E12
```

Sandisk Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: SanDisk USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/2/SanDisk_tsurugi_ro_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29340
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
```

```
 Sector Count: 60088320
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Fri Jun 10 15:48:06 2022
 Acquisition finished:  Fri Jun 10 15:56:00 2022
 Segment list:
  /images/2/SanDisk_tsurugi_ro_2.E01
…
  /images/2/SanDisk_tsurugi_ro_2.E12
```

Sandisk Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: SanDisk USB
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/3/SanDisk_tsurugi_ro_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29340
 Heads: 64
 Sectors per Track: 32
 Bytes per Sector: 512
 Sector Count: 60088320
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Fri Jun 10 16:03:53 2022
 Acquisition finished:  Fri Jun 10 16:11:57 2022
 Segment list:
  /images/3/SanDisk_tsurugi_ro_3.E01
…
  /images/3/SanDisk_tsurugi_ro_3.E11
  /images/3/SanDisk_tsurugi_ro_3.E12
```

WD Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: WD HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/1/WD_tsurugi_ro:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
```

```
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Thu Jun  9 17:13:41 2022
 Acquisition finished:  Thu Jun  9 19:16:55 2022
 Segment list:
  /images/1/WD_tsurugi_ro.E01
…
  /images/1/WD_tsurugi_ro.E83
```

WD Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: WD HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/2/WD_tsurugi_ro_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun 10 08:44:54 2022
 Acquisition finished:  Fri Jun 10 10:48:27 2022
 Segment list:
  /images/2/WD_tsurugi_ro_2.E01
…
  /images/2/WD_tsurugi_ro_2.E83
```

WD Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: WD HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/3/WD_tsurugi_ro_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
```

```
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Fri Jun 10 11:40:30 2022
 Acquisition finished:  Fri Jun 10 13:43:53 2022
 Segment list:
  /images/3/WD_tsurugi_ro_3.E01
….
  /images/3/WD_tsurugi_ro_3.E83
```

Seagate Test 1

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: Seagate HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/1/Seagate_tsurugi_ro:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Fri Jun 10 17:44:18 2022
 Acquisition finished:  Fri Jun 10 19:21:26 2022
 Segment list:
  /images/1/Seagate_tsurugi_ro.E01
…
  /images/1/Seagate_tsurugi_ro.E83
```

Seagate Test 2

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: Seagate HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/2/Seagate_tsurugi_ro_2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
```

```
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Fri Jun 10 20:11:18 2022
 Acquisition finished:  Fri Jun 10 21:46:14 2022
 Segment list:
  /images/2/Seagate_tsurugi_ro_2.E01
…
  /images/2/Seagate_tsurugi_ro_2.E83
```

Seagate Test 3

```
Case Information:
Acquired using: ADI3
Case Number: Projekt II
Evidence Number: TSURUGI Block
Unique description: Seagate HDD
Examiner: YS
Notes:

------------------------------------------------------------

Information for /images/3/Seagate_tsurugi_ro_3:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 60801
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 976773168
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Sat Jun 11 07:58:32 2022
 Acquisition finished:  Sat Jun 11 09:33:17 2022
 Segment list:
  /images/3/Seagate_tsurugi_ro_3.E01
…
  /images/3/Seagate_tsurugi_ro_3.E83
```

A.29 Sicherungs-Logs: Disk Arbitrator (macOS)

Imation Test 1

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „imation2GB“
Unique description: „2GB“
Examiner: CBublies
Notes: „after-data“

------------------------------------------------------------

Information for /Users/topher/img/imation:
```

```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 3911680
[Physical Drive Information]
 Drive Model: Imation Nano Media
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Mon Jun 13 18:39:52 2022
 Acquisition finished:  Mon Jun 13 18:44:41 2022
 Segment list:
  /Users/topher/img/imation.E01
```

Imation Test 2

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „imation2GB“
Unique description: „2GB“
Examiner: CBublies
Notes: „after-hex“

------------------------------------------------------------

Information for /Users/topher/img/imation:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 3911680
[Physical Drive Information]
 Drive Model: Imation Nano Media
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Mon Jun 13 18:51:04 2022
 Acquisition finished:  Mon Jun 13 18:55:52 2022
 Segment list:
  /Users/topher/img/imation.E01
```

Imation Test 3

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „imation2GB“
Unique description: „2GB“
Examiner: CBublies
Notes: „after-part“

------------------------------------------------------------

Information for /Users/topher/img/imation:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 3911680
```

```
[Physical Drive Information]
 Drive Model: Imation Nano Media
 Source data size: 1910 MB
 Sector count:    3911680
[Computed Hashes]
 MD5 checksum:    f4bc5f9fa365c3aa076a11c38514c78f
 SHA1 checksum:   3ab90273e23ec84b994cbf7973a5e4a6071508f0

Image Information:
 Acquisition started:   Mon Jun 13 19:07:03 2022
 Acquisition finished:  Mon Jun 13 19:11:53 2022
 Segment list:
  /Users/topher/img/imation.E01
```

Emtec Test 1

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „Emtec8GB“
Unique description: „8GB“
Examiner: CBublies
Notes: „after-data“

------------------------------------------------------------

Information for /Users/topher/img/emtec:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 15267839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 Media
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Mon Jun 13 19:27:03 2022
 Acquisition finished:  Mon Jun 13 19:54:00 2022
 Segment list:
  /Users/topher/img/emtec.E01
```

Emtec Test 2

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „Emtec8GB“
Unique description: „8GB“
Examiner: CBublies
Notes: „after-hex“

------------------------------------------------------------

Information for /Users/topher/img/emtec:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 15267839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 Media
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
```

```
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Mon Jun 13 19:58:24 2022
 Acquisition finished:  Mon Jun 13 20:25:26 2022
 Segment list:
  /Users/topher/img/emtec.E01
```

Emtec Test 3

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „Emtec8GB“
Unique description: „8GB“
Examiner: CBublies
Notes: „after-part“

------------------------------------------------------------

Information for /Users/topher/img/emtec:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 15267839
[Physical Drive Information]
 Drive Model: USB DISK 2.0 Media
 Source data size: 7454 MB
 Sector count:    15267839
[Computed Hashes]
 MD5 checksum:    eba107b6e7f98d667da7b6292b1c4b0e
 SHA1 checksum:   f087f3dbb45cc6c5dcce237c0c1e94d0b9d7ab41

Image Information:
 Acquisition started:   Mon Jun 13 20:28:50 2022
 Acquisition finished:  Mon Jun 13 20:55:44 2022
 Segment list:
  /Users/topher/img/emtec.E01
```

Sandisk Test 1 (gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „sandisk32GB“
Unique description: „32GB“
Examiner: CBublies
Notes: „after-data“

------------------------------------------------------------

Information for /Users/topher/img/sandisk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 60088320
[Physical Drive Information]
 Drive Model: USB SanDisk 3.2Gen1 Media
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Mon Jun 13 21:01:45 2022
 Acquisition finished:  Mon Jun 13 21:41:04 2022
```

```
 Segment list:
  /Users/topher/img/sandisk.E01
  …
  /Users/topher/img/sandisk.E12
```

Sandisk Test 2 (gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „sandisk32GB“
Unique description: „32GB“
Examiner: CBublies
Notes: „after-hex“

--------------------------------------------------------------

Information for /Users/topher/img/sandisk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 60088320
[Physical Drive Information]
 Drive Model: USB SanDisk 3.2Gen1 Media
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Mon Jun 13 21:42:55 2022
 Acquisition finished:  Mon Jun 13 22:22:18 2022
 Segment list:
  /Users/topher/img/sandisk.E01
  …
  /Users/topher/img/sandisk.E12
```

Sandisk Test 3 (gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „sandisk32GB“
Unique description: „32GB“
Examiner: CBublies
Notes: „after-part“

--------------------------------------------------------------

Information for /Users/topher/img/sandisk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 60088320
[Physical Drive Information]
 Drive Model: USB SanDisk 3.2Gen1 Media
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    3a36a973c1470c47dc0d9b34619d36f5
 SHA1 checksum:   c54fd47a20c811b79ec9c9d5d9b0525641d8cfd1

Image Information:
 Acquisition started:   Mon Jun 13 22:23:52 2022
 Acquisition finished:  Mon Jun 13 23:03:27 2022
 Segment list:
  /Users/topher/img/sandisk.E01
```

```
  …
  /Users/topher/img/sandisk.E12
```

WD Test 1 (gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „wd500GB“
Unique description: „500GB“
Examiner: CBublies
Notes: „after-data“

---------------------------------------------------------------

Information for //Volumes/TS-BCK-TMP/wd:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 976773168
[Physical Drive Information]
 Drive Model: WDC WD50 00BPVT-22HXZT3 Media
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    a62ea7f89c14c7f921124c598893a99f
 SHA1 checksum:   82198285ffe1226f1db9333e557a8ac1a63ad99e

Image Information:
 Acquisition started:   Tue Jun 14 11:52:02 2022
 Acquisition finished:  Wed Jun 15 02:08:06 2022
 Segment list:
  //Volumes/TS-BCK-TMP/wd.E01
  …
  //Volumes/TS-BCK-TMP/wd.E83
```

Seagate Test 1 (gekürzt)

```
Case Information:
Acquired using: ADI3
Case Number: „Fachprojekt2“
Evidence Number: „sg500GB“
Unique description: „500GB“
Examiner: CBublies
Notes: „after-data“

---------------------------------------------------------------

Information for /Users/topher/img/sg:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 976773168
[Physical Drive Information]
 Drive Model: TOSHIBA USB 3.5"-HDD Media
 Source data size: 476940 MB
 Sector count:    976773168
[Computed Hashes]
 MD5 checksum:    ca6f055db13bbff662be29a91859538e
 SHA1 checksum:   6a33457f3dd24eb0a6ac8a256af183c15e23a39a

Image Information:
 Acquisition started:   Wed Jun 15 16:37:28 2022
 Acquisition finished:  Thu Jun 16 04:21:14 2022
 Segment list:
  /Users/topher/img/sg.E01
...
  /Users/topher/img/sg.E83
```