SLUB
Wir führen Wissen.

Handreichung Forensische Datenträgerabzüge für digitale Vor- und Nachlässe

SLUB Dresden

Version 1.0.2, 2023-09-20

Inhaltsverzeichnis

Release Note 1.0.2 vom 2023-09-20

- Initiale Veröffentlichung
- Ergänzung Aufruf und Konvertierungsparameter für Kryoflux
- Fehlerkorrektur im Aufruf

Vorwort

Dieses Dokument richtet sich an Produzenten, die digitale Objekte in das SLUBArchiv.digital einliefern und diese langfristig benutzbar erhalten wollen.

Allgemeines

Digitale Vor- und Nachlässe bzw. Archivbestände sind ein wichtiger Teil des Sammlungsgutes der SLUB. Ein Personen-/ Familien- bzw. Körperschaftsarchiv ist die Summe aller Ressourcen, die eine Person oder privatrechtliche Institution geschaffen oder zusammengetragen hat. Bestandteile dieser Ressourcen können auch digitaler Natur sein.

Dabei kann es sich um beliebige Hardware und digitale Daten (üblicherweise nicht Software im engeren Sinne) handeln, die oft bereits ihre geplante Lebensdauer überschritten haben. Aus diesem Grund und weil digitale Daten deutlich anfälliger für Beschädigungen/Zerstörung sind als ihre analogen Gegenstücke ist es wichtig, die Materialien direkt nach dem Eingang archivarisch zu erfassen, nötigenfalls von gefährdeten Datenträgern auf sichere Speicher zu überführen und in archivfähige Formate zu konvertieren, um die dauerhafte Benutzbarkeit sicherzustellen. Dann kann die Tiefenerschließung erfolgen.

Die besondere Herausforderung ist hierbei, dass, wenn überhaupt, der originale Datenträger nur mit spezieller Hardware ausgelesen werden kann und der Datenträgerabzug zur Primärquelle wird.

Aus diesen Gründen ist es erforderlich Datenträgerabzüge so zu sichern, dass sie die Anforderungen an Authentizität, Integrität, Nachvollziehbarkeit und Nachnutzbarkeit gewährleisten.

Als Einstieg in das Thema ist *Practical Forensic Imaging* von Bruce Nikkel (Nikkel, 2016) empfehlenswert.

Vorbehaltlich gesonderter Absprachen mit dem SLUBArchiv sind von dieser Handreichung abweichende Änderungen **nicht** gestattet. Informationspakete, die diese Anforderung nicht erfüllen, sind nicht langzeitarchivfähig und werden vom SLUBArchiv zurückgewiesen.

Abgrenzung

Dieses Dokument beschreibt die Anforderungen des SLUBArchiv an die Sicherung von Datenträgern von digitalen Vor- und Nachlässen.

Diese Datenträger können sein:

- Festplatten
- Speicherkarten (Compactflash, MMC)
- Disketten
- MO-Disks
- Daten-CDROMs und -DVDs

Nicht von diesem Dokument erfasst sind:

- Datenträger-Abbilder von kommerziell hergestellten, an ein breites Publikum adressierten audiovisuellen Medien, zB. Audio-CDs, Video-DVDs
- Datenträger- und Datenspeicher von Spielekonsolen
- forensische Datenträger-Abbilder, die zum Zwecke der Strafverfolgung erstellt wurden

Dieses Dokument wird nicht angewendet in Fällen der Retrodigitalisierung.

Datensicherungsanforderungen an Dienstleister sind im Einklang mit diesem Dokument zu verfassen.

Nutzungsszenarien und signifikante Eigenschaften

Grundlage

Grundlage sind die in https://git.slub-dresden.de/digital-preservation/significantproperties/-/blob/master/sigprops_forensic_images.xml hinterlegten Nutzungsszenarien und signifikante Eigenschaften.

Erhalt des Bitstromes

Ohne tiefere Analyse eines Datenträgers sind nur wenige Informationen zur internen Organisation der Daten bekannt. Die Abbilddateien müssen daher eine Analyse des ursprünglichen Dateiformates, die Extraktion von (Teilen von) Dateien, Interpretation der zugehörigen Metadaten, sowie den Zugriff auf gelöschte Bereiche eines Datenträgers erlauben.

Hinzu kommt, dass Fehlstellen bzw. Lesefehler nachvollziehbar erhalten bleiben.

Dadurch ist die wissenschaftliche Auswertung, zB. des Schaffensprozesses, gewährleistet.

Metadaten Datenträger und Abbild

Es muss eine Zuordnung zwischen Medium und Abbild herstellbar sein. Metadaten, die den Auslesevorgang näher beschreiben (storage metadata) sind für eine spätere Bearbeitung (zB. Tiefenerschliessung) notwendig.

Mounten und Extraktion von Dateien

Die Abbild-Datei muss bei intakter und bekannter Dateisystemstruktur als virtuelles Laufwerk gemountet werden können und die Extraktion von Dateien erlauben.

Anforderungen

Allgemeine Anforderungen

Verpflichtend

- Als Datei- und Verzeichnisnamen sind nur Zeichen aus den Bereichen A-Z, a-z, 0-9 und die Sonderzeichen "-._" zu verwenden. Dies erleichtert den Kopiervorgang über Betriebssystemgrenzen hinweg.
- Die Wahl der Abbildparameter, sofern im Einklang mit diesem Dokument möglich, sind unter den Aspekten der Angemessenheit und Begründetheit vorzunehmen, da diese einen starken Einfluss auf die Kosten der digitalen Langzeitarchivierung haben. Die Anforderung der Begründetheit gilt als erfüllt, wenn wissenschaftlich fundiert auf öffentlich zugängliche Publikationen anerkannter Fachorganisationen, Standardisierungseinrichtungen der Wissenschaft oder Herstellerdokumentationen Bezug genommen wird.

Gute Praxis

- Es hat sich bewährt, je eine Datei pro Originaldatenträger anzulegen.
- Der grundsätzliche Aufbau von Submission Information Packages (SIP) ist in der SIP-Spezifikation beschrieben.
- Sinnvoll ist es, die Dateinamen so zu wählen, dass
  - der Bezug zur Vorlage erkennbar ist
  - die Zuordnungen zueinander erkennbar sind

Expert Witness Format (EWF)

Verpflichtend

- Expert Witness Compression Format (EWF), Pronom-ID fmt/803, in den Versionen 1 und 2 [1]
- Keine Verschlüsselung
- Storage-Metadaten, mit den folgenden Bestandteilen
  - *case number*, von Fachabteilung intern verwendet, bezeichnet kompletten Vor-/Nachlass
  - *evidence number*, von Fachabteilung intern verwendet, bezeichnet das Medium, welches ausgelesen wurde
  - *description*, Angaben zum Hintergrund des Auslesevorgang und des Mediums
  - *examiner*, Welche Organisationseinheit hat das Medium ausgelesen? (SLUBArchiv, Dienstleister) [2]
  - Kompressionsmethode: *deflate* oder *bzip2* [3]
  - Kompressionsstufe: *best*
  - *additional digest*: sha256

    - korrekt gesetzte *media flags*
- bei gesplitteten Datenträgerabzügen muss die Zuordnung durch die ewftools gewährleistet sein

Gute Praxis

- Storage-Metadaten, *notes*: für Notizen, die beim Auslesen angefallen sind, zB. Inhalt von Map-Files von *ddrescue*
- die Splitsize [4] sollte 2GB nicht übersteigen [5]

Es ist sinnvoll, das Kommandozeilen-Werkzeug *ewfacquire* für das Auslesen der Medien zu nutzen, da dieses eine feingranularere Einstellung der Parameter erlaubt.

Beispiel 1. Beispiel Auslesen USB Stick (/dev/sda)

```
ewfacquire -c best -d sha256 -D "Beschreibung" -e "SLUB, Referat 5.1" -E "Nachlassnummer_1_1_2" -t "usb_stick_1_1_2_ewf" /dev/sda
```

Beispiel 2. Beispiel Konvertieren/Exportieren eines EWF Image

```
ewfexport usb_stick_1_1_2_ewf.E01 -t /dev/sda
```

Beispiel 3. Beispiel Anzeigen Metadaten eines EWF Images

```
ewfinfo usb_stick_1_1_2_ewf.E01
```

Sicherung von Disketten mit Kryoflux

Um Disketten auszulesen, die nicht mit einem Standard-Diskettenlaufwerk auf einem PC unter Linux auslesbar sind, kann die Kryoflux Hardware benutzt werden. Für die Sicherung kann dann **abweichend** auf die folgenden Formate zurückgegriffen werden.

Interchangeable Preservation Format

- Interchangeable Preservation Format, Version 1.6

Kryoflux Stream Protocol

- Kryoflux Stream Protocol, Revision 1.1

Dieses Format sollte standardmäßig verwendet werden und entspricht dem Imagetype "i0" des *dtc* -Tools

Beispiel 4. Beispielaufruf Kryoflux für Sicherung flux-streams

```
dtc -fdumpdir/streams -i0
```

Für die spätere Analyse und Konvertierung kann dann *dtc* verwendet werden.

Beispiel 5. Beispielaufruf Kryoflux für Konvertierung flux-streams in ein Diskimage

```
dtc -m1 -fdumpdir/streams -i0 -fimage -i4 -l8
```

Validierung

Aktuell besteht nur die Möglichkeit einer Integritätsprüfung von EWF-Dateien mit dem Tool *ewfverify* der libewf, freie Softwarebibliothek für den Zugriff auf Expert Witness Compression Format, sh. https://github.com/libyal/libewf.

Beispiel 6. Beispiel Überprüfen eines EWF Images

```
ewfverify usb_stick_1_1_2_ewf.E01
```

Hinweise zum Auslesen von beschädigten Medien

Besteht der Anfangsverdacht, dass Medien (insbesondere CDROMs und DVDs) beschädigt sein könnten, so sollte auf das GNU Werkzeug *ddrescue* in Kombination mit *ewfaquirestream* zurückgegriffen werden.

Im Zweifel sollten spezialisierte Dienstleister hinzugezogen werden.

Bibliographie

Nikkel, B. (2016). *Practical Forensic Imaging*. nostarch press.

[1] von der libewf, freie Softwarebibliothek für den Zugriff auf Expert Witness Compression Format, sh. https://github.com/libyal/libewf unterstützt.
[2] Bitte nur Funktionsnamen, keine natürlichen Personen!
[3] *bzip2* nur bei EWF v2 möglich
[4] die Splitsize gibt an, bei welchen Dateigrößen ein Datenträgerabbild in mehrere Dateien aufgeteilt wird. Das kann sinnvoll sein, um Verschnitt bei der Speicherung zu reduzieren.
[5] Es können auch größere Werte verwendet werden, wenn dies für das Medium angemessen und sinnvoll ist, zB. für Festplatten mit Kapazitäten > 100GB.