

MoNA Nutzerhandbuch

Version 1.1 zu MoNA v3.6.1

FoSIL

Inhaltsverzeichnis

1. Einführung	1
2. Grundlagen	2
2.1. Einrichtung	3
2.1.1. Installation MoNA	4
2.1.2. Konfiguration Arbeitsspeicher	5
2.1.3. Änderung der Arbeitsspeicherkonfiguration	6
2.1.4. Windows Defender Ausnahme einrichten	7
2.1.5. Docker einrichten	9
2.1.6. PhotoDNA einrichten.	17
2.1.7. Modelle für Nachrichtenmarkierung importieren	18
2.2. Erste Schritte	20
2.2.1. Startdialog	22
2.2.2. Untersuchung anlegen	22
2.2.3. Untersuchung öffnen	23
2.2.4. Mobiles Endgerät anlegen	24
2.2.5. Backup erstellen	25
2.3. Daten einlesen	25
2.3.1. UFDR Report Daten einlesen	27
2.3.2. WhatsApp Daten einlesen (Android)	28
2.3.3. WhatsApp Daten einlesen (iOS)	31
2.3.4. Telegram Daten einlesen (Android)	33
2.3.5. Telegram Daten einlesen (iOS)	36
2.3.6. Facebook Messenger Daten einlesen (Android)	38
2.3.7. Facebook Messenger Daten einlesen (iOS)	41
2.3.8. Operationen zur Nachverarbeitung	43
2.4. Analyse	45
2.4.1. Chat Nachbearbeitung	45
2.4.1.1. Chats zusammenführen	45
2.4.1.2. Semantische Analyse	46
2.4.1.3. Sprache detektieren	46
2.4.1.4. Offensive Speech	46
2.4.1.5. Videoframes extrahieren	46
2.4.1.6. Lokale und globale Nutzerkonten gruppieren	47
2.4.2. Themenextraktion	47
2.4.2.1. Themenextraktion	47
2.4.2.2. Extrahiere alle Arten von Themen	47
2.4.3. Begriffsbaum	47
2.4.3.1. Begriffsbaum erstellen	48
2.4.3.2. Begriffsbaum manuel initialisieren	48
2.4.3.3. Begriffsbaum Erstellung mit Themenextraktion	49

2.4.3.4. Themenextraktion Optionen	49
2.4.3.5. Synonyme und Übersetzungen automatisch finden.	49
2.4.3.6. Begriffsbaum exportieren	49
2.4.3.7. Begriffsbaum importieren	49
2.4.4. Suche	50
2.4.4.1. Termsuche	50
2.4.4.2. Suchoptionen	51
2.4.4.3. Tags	51
2.4.4.4. Suchergebnisse verstehen	52
2.4.5. Zeitdiagramm	52
2.4.5.1. Zeitdiagramm öffnen	52
2.4.5.2. Zeitdiagramm bearbeiten	53
2.4.5.3. Zeitdiagramm filtern	53
2.4.5.4. Zeitdiagramm exportieren	53
2.4.6. Nutzerprofile	54
2.4.6.1. Nutzerprofile verknüpfen	54
2.4.6.2. Nutzerprofile vergleichen	54
2.4.7. Netzwerkstatistiken	54
2.4.8. Netzwerkdetails	54
2.4.8.1. Netzwerkdetail Sortierung Suche	54
2.4.9. Nachrichtentabelle	55
2.4.9.1. manuelle Markierung von Nachrichten/Chats	55
2.4.9.1.1. Als relevant/Verdächtig markieren	55
2.4.9.1.2. Als irrelevant markieren	55
2.4.9.2. Übersetzung	56
2.4.10. Medien	56
2.4.10.1. Medieninformationen anzeigen	56
2.4.10.2. Medien gegen Hashdatenbank prüfen	56
2.4.10.3. Medien gegen Hashdatenbank und Treffer auf Ähnlichkeit überprüfen	56
2.4.10.4. Bilder auf Ähnlichkeit überprüfen	56
2.4.11. Auswertung	57
2.4.11.1. Report erstellen	57
2.4.11.2. Berichtsoptionen	57
3. Troubleshooting	57
3.1. Ungültige Lizenz	57
3.2. Anlegen der Untersuchung	58
3.3. Keine Rückmeldung/Lange Ladedauer	59
3.4. Import	59
3.5. Fehlermeldung	59

1. Einführung

Der Mobile Network Analyzer (MoNA) ist eine Plattform zur Analyse mobiler Kommunikation. Das Konzept basiert auf der Erkenntnis, dass, aufgrund der Einzigartigkeit jedes einzelnen Falles, nur eine interaktive Lösung, unter Einbeziehung der Erfahrung und des Fallwissens eines Ermittlers, erfolgreich sein kann. Das Herzstück bildet dabei ein semantisches Wörterbuch in Form eines Begriffsgraphen. Dieser verknüpft einzelne Schlüsselbegriffe und Muster zu komplexen semantischen Ketten. Jeder Begriff wird dabei nicht als einfache Erscheinungsform eines Wortes, sondern als Vektor möglicher Erscheinungsformen inkl. Synonyme und fremdsprachlicher Varianten repräsentiert. Die Analyse des individuellen Gesprächsverhaltens einzelner Teilnehmer ermöglicht darüber hinaus die Gruppierung von Nachrichten zu Gesprächen, wodurch nicht mehr nur eine Nachricht, sondern ein ganzes Gespräch als Suchtreffer an den Ermittler zurückgeliefert werden kann. Der dadurch erzielte Kontexterhalt erleichtert die Interpretation der Ergebnisse erheblich.

Finanzierung

Von diesem Lösungsansatz konnten zwischenzeitlich verschiedene Landeskriminalämter, Polizeidirektionen und Generalstaatsanwaltschaften überzeugt werden, welche mittlerweile MoNA im Praxistest erproben.

Das LKA Baden-Württemberg finanziert darüber hinaus die Weiterentwicklung bis 2023 und ermöglicht damit die langfristige Implementierung weiterer intelligenter Services, welche die Software zu einer international konkurrenzfähigen Analyselösung für mobile Endgeräte machen.

Aktuell plant die Firma NUIX, einer der weltweiten Marktführer im Bereich forensischer Softwarelösungen und Services, parallel die Integration von MoNA in Ihre Systemlandschaft.

Dieser Erfolg sichert nicht nur die Nachhaltigkeit der Software, sondern zementiert die Bedeutung der Hochschule Mittweida als Standort exzellenter Anwendungsforschung.

Hintergrund

In den letzten neun Jahren schaffte es die **AG FoSIL (Forensic Science Investigation Lab)** an der Hochschule Mittweida Kooperationen mit zahlreichen Strafverfolgungsbehörden zu etablieren. Im Rahmen dieser Zusammenarbeit erhielt die Arbeitsgruppe eines Tages den Auftrag eine automatisierte Lösung zur Analyse von Kurznachrichten zu entwickeln. Schnell stellte sich heraus, dass dieses simple anmutende Problem tatsächlich außerordentlich schwer zu lösen ist.

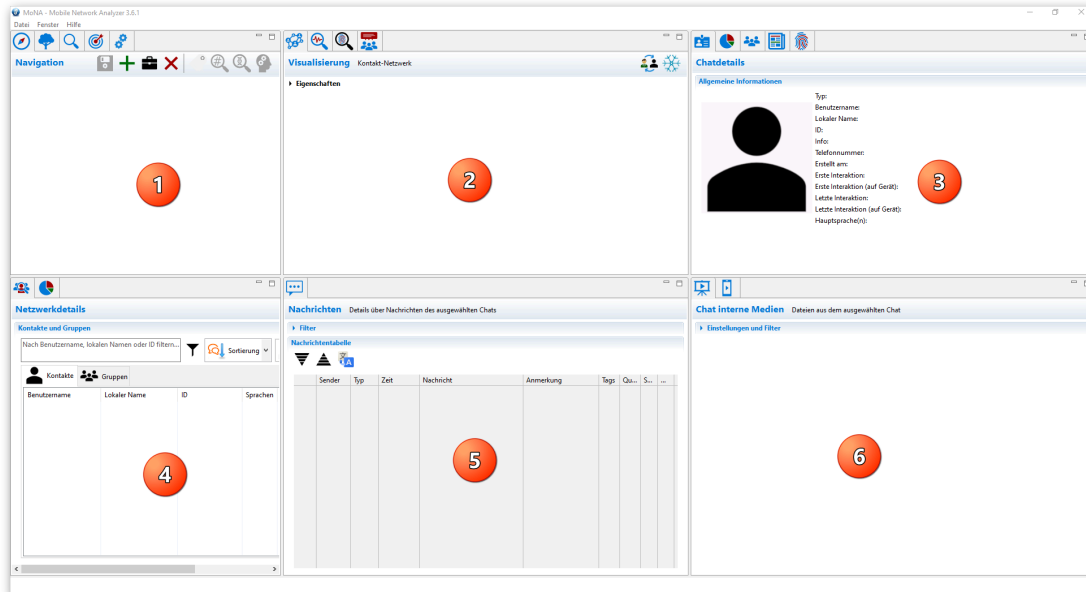
Die Gründe hierfür liegen vor allem in der Kombination der grundlegenden Charakteristik forensischer Texte (strukturelle und inhaltliche Heterogenität, Anreicherung mit nicht textbasierten Daten, sozio-kulturelle Schreibvarianten, etc.) und einer hohen Informationsdichte, die sich zum einen aus der Beschränkung der zur Verfügung stehenden Anzahl von 160 Zeichen, andererseits aus der Art ihrer Verwendung ableitet. Insbesondere werden derartige Nachrichten oft als eine Art „Nebenbei-Nachricht“ versendet, weshalb ihr Kontext für Außenstehende vielfach im Dunkeln bleibt.

Prinzipiell stehen Ermittler vor der Herausforderung alle Nachrichten vollständig lesen, bewerten und ggf. fallrelevante Informationen extrahieren zu müssen. In vielen Fällen befinden sich auf mobilen Endgeräten mehrere Tausend Nachrichten, welche oftmals von Subsprache dominiert werden, was es selbst für Ermittler mit jahrelanger Erfahrung schwer macht, diese Texte zu lesen. Darüber hinaus ist der reine Zeitaufwand zur manuellen Bewältigung dieser Aufgabe so enorm, dass er sich oft nur in Fällen mittlerer oder schwerer Kriminalität (hierzu zählen insbesondere gewerbsmäßige oder Bandenriminalität) mit hohem öffentlichem Interesse rechtfertigen lässt.

2. Grundlagen

Dieses Kapitel bietet einen allgemeinen Überblick über MoNA und seinen Anwendungsfunktionen sowie Informationen zu Einleseoperationen, Nachverarbeitung, Datenanalyse und Konfigurationseinstellungen. Außerdem werden häufige Nutzungsszenarios im Detail erläutert. Diese Betriebsanleitung bietet in der aktuellen Version keinen Quick Start, da MoNA für eine solche Verwendung noch nicht geeignet ist. Eine weitergehende Einarbeitung in die Software ist für die vollständige Nutzung von MoNA notwendig. In den Ersten Schritten wird unter anderem das Anlegen von Untersuchungen und Mobilten Endgeräten erläutert darauf folgt der erste Datenimport. Hiernach kann mit den ersten Analyseoperationen gestartet werden.

Das User Interface (Benutzerschnittstelle) ist wie folgt aufgebaut.



Nummerierung siehe Abbild	Funktionen (Reihenfolge entspricht Layout)
1	Navigationsbereich, Begriffsbaum Editor, Globale Suche, Suchergebnisse und laufenden Operationen. Standardmäßig wird der Navigationsbereich angezeigt.
2	Visualisierung der Chatteilnehmer, Zeitdiagramm, Liste der Nutzerprofile und Chat-übergreifende Themen. Standardmäßig wird die Liste der Nutzerprofile angezeigt.
3	Chatdetails, Chatstatistik, Chatmitglieder, Chat interne Themen und das Nutzerprofil. Standardmäßig werden die Chatdetails angezeigt.
4	Netzwerkdetails und Netzwerkstatistiken. Standardmäßig werden die Netzwerkdetails angezeigt.
5	Nachrichtentabelle.
6	Chat interne Medien und die Mediengalerie. Standardmäßig werden Chat interne Medien angezeigt.

Bemerkung

Die einzelnen Bereiche können mit ☐ minimiert und mit ☐ maximiert werden.

2.1. Einrichtung

Im Folgenden werden alle notwendigen Schritte beschrieben, welche einmalig vor der Benutzung von MoNA durchgeführt werden müssen. MoNA wird etwa alle 4 Monate aktualisiert. Über den [Moodle Kurs](#) können Sie sich über die neusten Änderungen auf dem Laufenden halten. MoNA ist in seiner aktuellen Version für Windows mit Java-Umgebung ausgelegt. Wobei MoNA bereits mit einer funktionierenden Java Umgebung ausgeliefert wird, hierfür ist eine separate Installation nicht nötig! Stellen Sie vor der Einrichtung sicher, dass alle [Mindestanforderungen](#) erfüllt sind. Um sich einen ersten Überblick zu verschaffen, empfehlen wir das [Anlegen einer Untersuchung](#), eines [Mobilen Endgeräts](#) und dem Import eines beliebigen Messengers. Um MoNA erfolgreich in Ihre Ermittlungsarbeit zu integrieren werden in diesem User Guide die verfügbaren Funktionen genau beschreiben, sodass Sie die verschiedenen Funktionen adäquat anwenden können. Wie die Daten interpretiert werden können, wird in einem weiteren Kapitel erläutert. Ein leistungsstarker Computer mit mehr als 16 GB Arbeitsspeicher wird empfohlen, insbesondere wenn Sie Chatverläufe mit mehreren Millionen Nachrichten analysieren. Für die Anwendung komplexer KI-Modelle beispielsweise für eine semantische Analyse, wird eine leistungsstarke Grafikkarte empfohlen, hierfür bietet es sich an MoNA auf einer modernen Workstation zu installieren. Die Leistung des Hostsystems von MoNA spielt eine fundamentale Rolle bei der Einlesezeit der Daten. Der Anleitung zur Einrichtung muss Schritt für Schritt folge geleistet werden, um einen reibungslosen Ablauf zu garantieren.

Achtung

Wenn die Mindestanforderungen nicht gegeben sind kann dies zu erheblich längeren Ladezeiten führen.

2.1.1. Installation MoNA

Im Folgenden wird die Installation von MoNA schrittweise erläutert. In der aktuellen Version wird MoNA als vorkonfiguriertes **gepacktes ZIP-Archiv** zur Verfügung gestellt. Für die Installation ist **kein Installer erforderlich**. Bezogen wird MoNA über die Bildungsplattform Moodle in dem [MoNA Kurs](#). Extrahieren Sie die Dateien aus dem MoNA-Download unter Berücksichtigung der [Anforderungen](#) in ein Verzeichnis Ihrer Wahl. Nach der Extraktion ist MoNA einsatzbereit. Folgende Anforderungen müssen von dem System gegeben sein.

Vorbereitungen

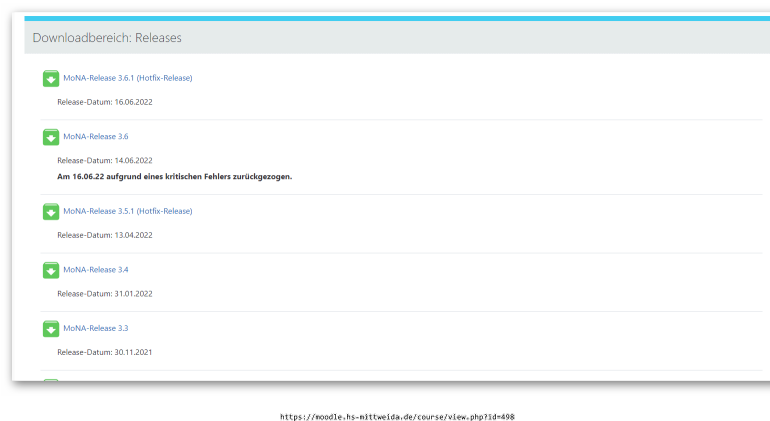
Anforderungen an das System:

- Betriebssystem: Windows 10+
- Mindestens 16 GB Arbeitsspeicher (Empfohlen 32 GB)
- Für bestimmte KI-Anwendungen wird eine Grafikkarte mit mindestens 11 GB VRAM benötigt.

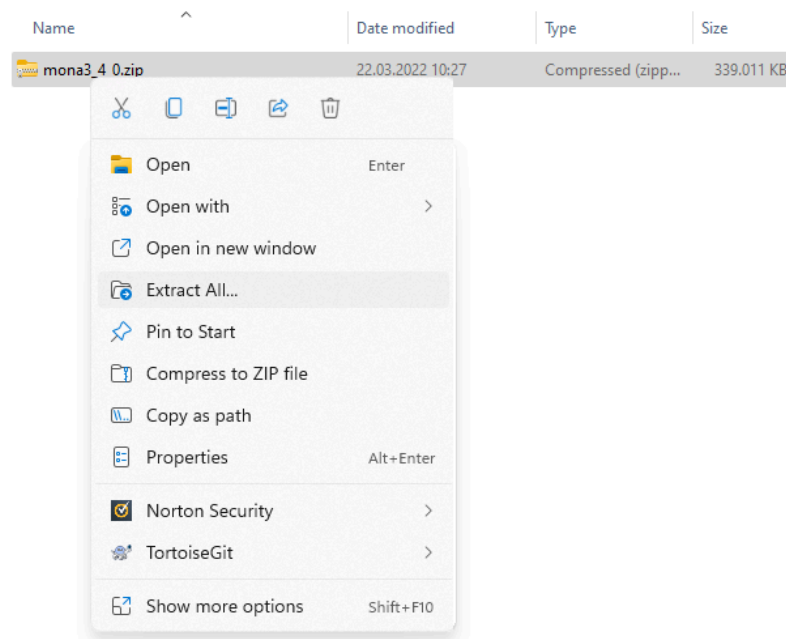
Referenz Nvidia Gefore RTX 2080TI

Prozedur

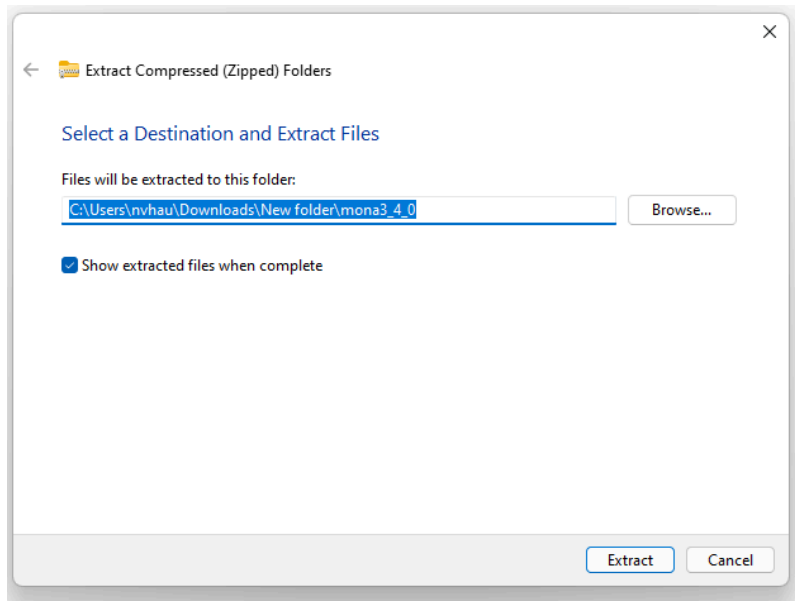
1. Herunterladen der aktuellen Version von MoNA (aus Moodle, aktuell v3.6.1).



2. Entpacken des heruntergeladenen Archivs, hierfür Rechtsklick -> Alle extrahieren...



3. Extraktionsort wählen -> Extrahieren



4. Verschieben des Installationsverzeichnis auf ein Laufwerk ohne rechtliche Einschränkungen.
5. Hinzufügen des MoNA-Installationsverzeichnis zu den [Ausnahmen im Windows Defender](#).
6. Kopieren der Lizenzdatei in das Unterverzeichnis `./configurations` (In dem mona3_5_1 Ordner).

Name	Date modified	Type	Size
configuration	22.03.2022 10:59	File folder	
features	14.03.2022 11:46	File folder	
jre	14.03.2022 11:46	File folder	
plugins	14.03.2022 11:46	File folder	
workspace	14.03.2022 11:49	File folder	
.eclipseproduct	24.02.2022 12:55	ECLIPSEPRODUCT...	1 KB
hidden	22.03.2022 10:59	File	2 KB
LIZENZ.lic	22.03.2022 11:03	VisualStudio.Lic.51...	0 KB
mona.exe	24.02.2022 12:55	Application	415 KB
mona.ini	13.03.2022 11:25	Configuration sett...	1 KB

7. Start mit Doppelklick auf mona.exe 

2.1.2. Konfiguration Arbeitsspeicher

Um größere Datenmengen verarbeiten zu können, muss die Konfigurationsdatei `mona.ini` im MoNA-Installationsverzeichnis angepasst werden. Dies ist gerade bei der Verwendung von Modellen zur Nachrichtenmarkierung notwendig, da diese in den Arbeitsspeicher geladen werden und einen durchschnittlichen Umfang von ca. 5 GB pro Sprache haben.

Vorbereitungen

In dieser Konfigurationsdatei kann der maximal von MoNA verwendbare Arbeitsspeicher (RAM) von standardmäßig 8 GB auf einen höheren Wert eingestellt werden. Abhängig ist die Konfiguration von dem Arbeitsspeicher, welcher auf dem Gerät verfügbar ist, auf dem MoNA betrieben wird.

Die entsprechende Zeile in der Konfigurationsdatei lautet in der Ursprungsform:

-Xmx8g

Dieser Wert kann entsprechend für 16 GB folgendermaßen geändert werden:

-Xmx16g

Wichtig

Als Empfehlung sollte hier nicht der gesamte Arbeitsspeicher eines Gerätes angegeben werden, je nach den zusätzlich zu MoNA verwendeten Programmen sollte $\frac{1}{4}$ des Arbeitsspeichers für andere Programme übrigbleiben.

Empfohlene maximal Belegung des Arbeitsspeichers:

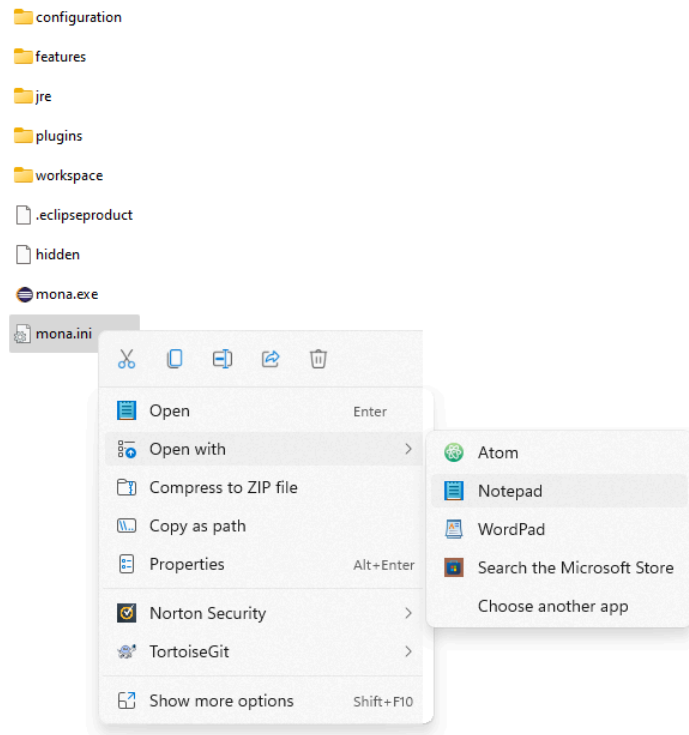
Verfügbarer RAM	Einstellung MoNA
16 GB	-Xmx12g
32 GB	-Xmx24g
64 GB	-Xmx48g
128 GB	-Xmx96g

Die in der Konfigurationsdatei angegebene Menge an Arbeitsspeicher für MoNA wird zudem dynamisch und erst bei Bedarf auch tatsächlich in Anspruch genommen.

2.1.3. Änderung der Arbeitsspeicherkonfiguration

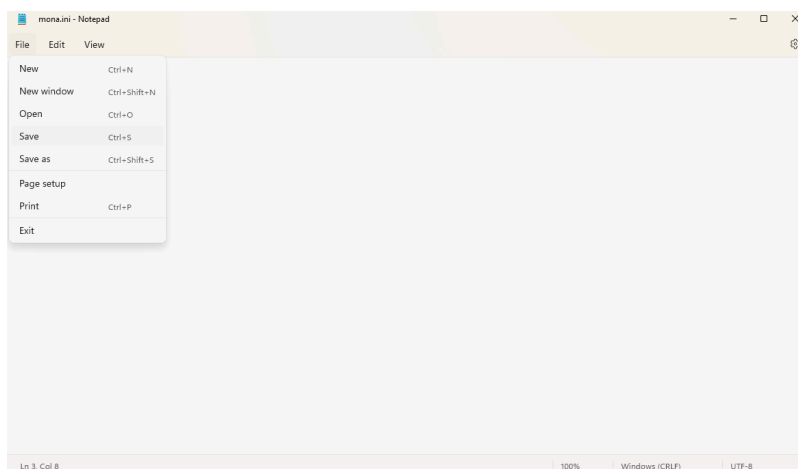
Prozedur

1. Im MoNA Programmordner die `mona.ini` Datei anwählen
2. Rechtsklick -> Öffnen mit -> Editor



3. Konfiguration wie beschrieben bearbeiten.

4. Datei -> Speichern oder Strg + S



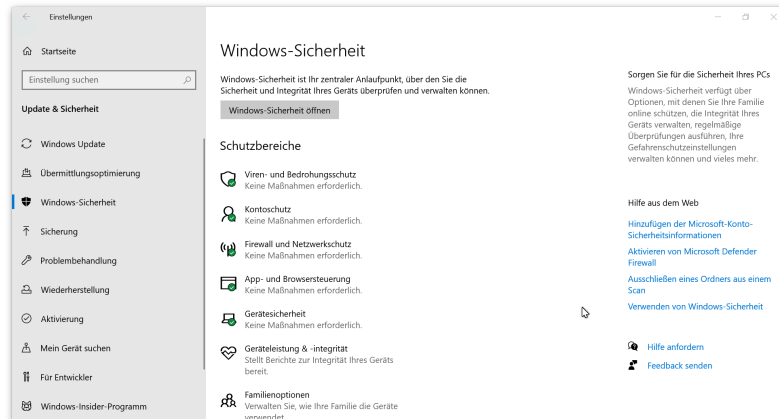
5. Datei schließen

2.1.4. Windows Defender Ausnahme einrichten

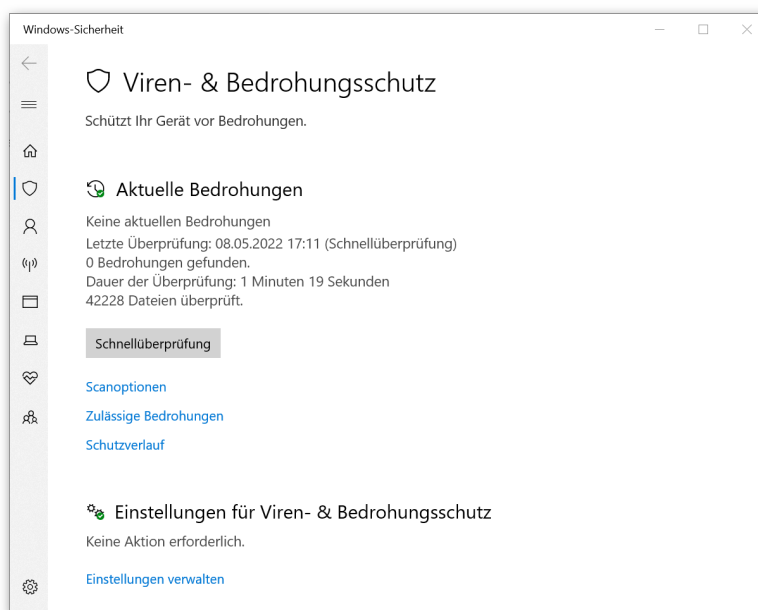
Um ein gegebenenfalls stark verlangsamtes Einlesen von Falldaten unter Microsoft Windows zu verhindern, muss das MoNA-Installationsverzeichnis als Ausnahme zum Windows Defender hinzugefügt werden.

Prozedur

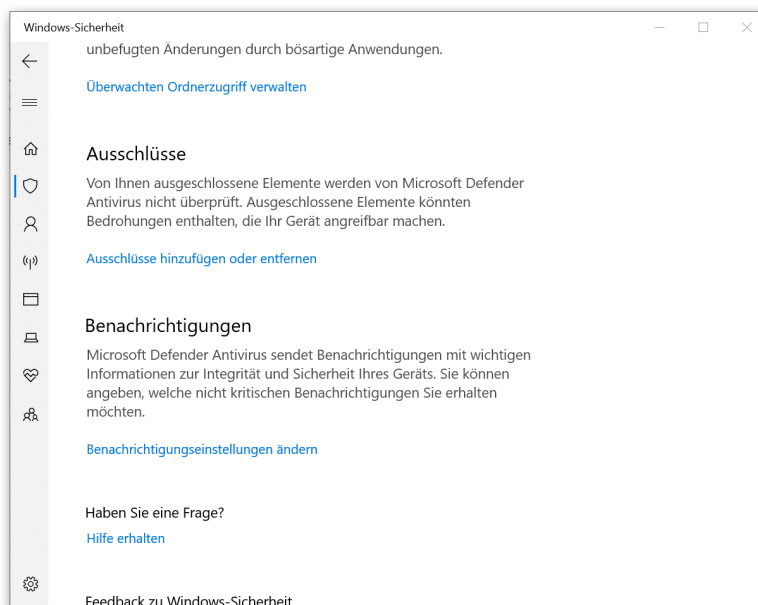
1. Öffnen der Einstellungsseite "Viren - und Bedrohungsschutz" in den Systemeinstellungen (Start -> Einstellungen -> Update und Sicherheit -> Windows Sicherheit -> Viren - und Bedrohungsschutz).



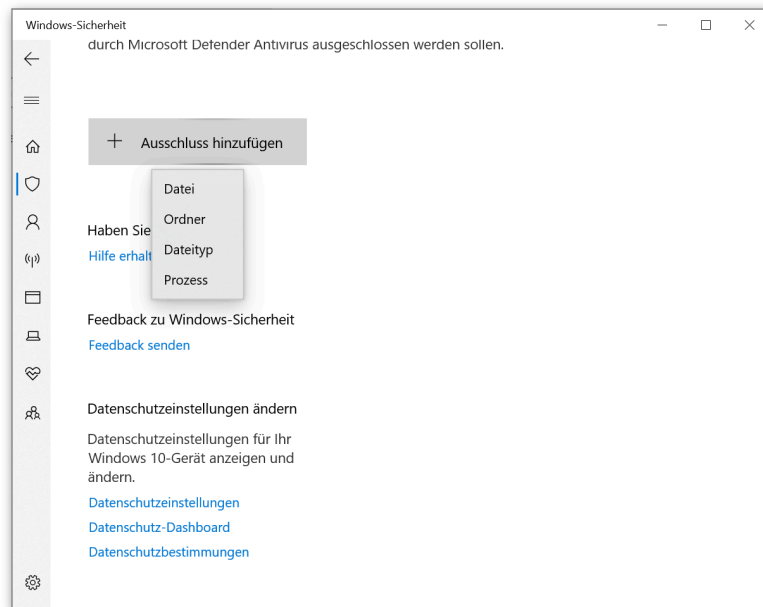
2. Öffnen der Einstellungen für Viren- & Bedrohungsschutz über **Einstellungen** verwalten.



3. Im Unterpunkt **Ausschlüsse** den Eintrag **Ausschlüsse** hinzufügen oder entfernen auswählen.



4. Hier über den Punkt **+ Ausschluss** hinzufügen das **MoNA-Installationsverzeichnis** auswählen und damit als Ausnahme hinzufügen.



2.1.5. Docker einrichten

Um die Semantische Analyse nutzen zu können, muss zuerst ein Docker Container auf ihrem Windows System eingerichtet werden. Mit dieser lässt sich für Bilder, Videos und Audiodateien eine textuelle Beschreibung generieren. Dafür sollten folgende Mindestanforderungen vom System gegeben sein.

Gerät	Empfohlene Anforderungen
Grafikkarte	1 x NVIDIA GPU mit mindestens 5GB GPU memory
CPU	64-bit Prozessor mit Second Level Address Translation (SLAT)
RAM	Mindestens 16 GB
BIOS	Die Unterstützung der Hardware-Virtualisierung auf BIOS-Ebene muss in den BIOS-Einstellungen aktiviert werden. Weitere Informationen finden Sie unter Virtualisierung und Aktivieren der virtuellen Visualisierung .
Internet	Eine Internetverbindung wird vorausgesetzt.

Bemerkung

Diese Anforderungen müssen mindestens für die Docker-Applikation verfügbar sein und nicht durch MoNA verwendet werden. Wenn von 16GB installiertem RAM in MoNA 12GB (~Xmx12g) konfiguriert sind kann Docker nur noch ca. 4 GB verwenden. Daher sollten Mindestens 32GB Arbeitsspeicher zur Verfügung stehen.

Außerdem setzt die Docker Anwendung folgende **Software** voraus:

Windows:

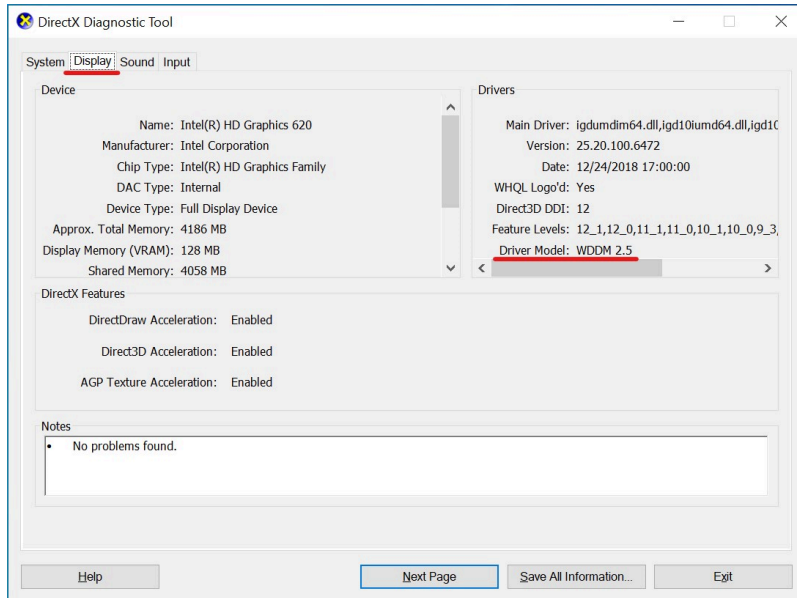
- Für x64-Systeme: mit Build 18362 oder höher.

- Für ARM64-Systeme: mit Build 19041 oder höher.

Um Ihre Windows-Version und Build-Nummer zu überprüfen, betätigen Sie die Windows -Taste + R, und geben `winver` ein und wählen **OK**. Sie können auf die neueste Windows-Version aktualisieren, indem Sie **Start > Einstellungen > Windows Update > Nach Updates suchen** wählen.

DirectX:

Für den Container wird mindestens eine Display Treiber Version WDDM 2.5 oder höher benötigt.



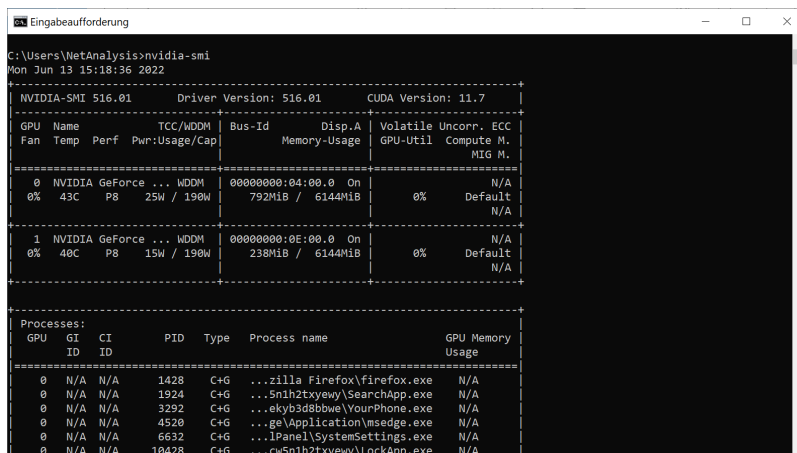
Um Ihre DirectX-Version zu überprüfen, betätigen Sie die Windows -Taste + R, und geben `dxdiag` ein und wählen **OK**. Danach wählen Sie eine Anzeige aus und suchen wie im Bild zu sehen nach der Treiber Version.

NVIDIA Treiber:

Aktualisieren Sie die Treiber der vorausgesetzten NVIDIA Grafikkarte. Nachdem Sie die Treiber installiert haben, müssen Sie den Erfolg der Installation überprüfen, indem Sie den folgenden Befehl in der PowerShell oder Windows-Eingabeaufforderung eingeben.

Powershell Befehl: `nvidia-smi.exe`

Wenn der Treiber erfolgreich installiert wurde, wird eine Liste der an das System angeschlossenen GPUs angezeigt, wie in der nachfolgenden Abbildung dargestellt.



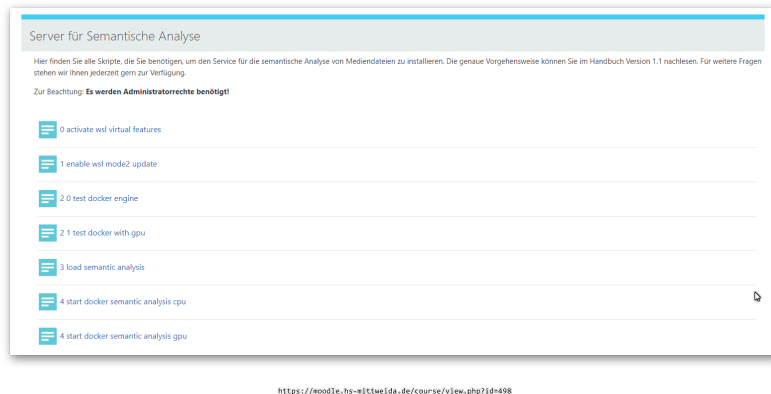
WSL 2 backend:

Außerdem wird für das später benötigte Windows Subsystem for Linux 2 die vorherige Aktivierung vorausgesetzt. Falls dies nicht bereits der Fall ist folgen Sie bitte dieser [Anleitung](#).

Docker:

Auf dem Container-Host muss Docker Engine Version 19.03 oder neuer installiert sein. Detaillierte Anweisungen finden Sie im Abschnitt [Docker Desktop installieren](#).

Wenn alle Voraussetzungen gegeben sind, können sie mit der Konfiguration der Programme fortfahren. Hierfür werden 7 Skripts zur Verfügung gestellt, welche diese Schritte für Sie übernehmen. Diese Skripts können Sie über die [Bildungsplattform Moodle](#) beziehen.



1. Windows Feature aktivieren:

Bevor Sie mit Docker arbeiten, müssen die Funktionen des Windows Subsystems für Linux (WSL) und der Virtual Machine Platform aktiviert werden. Dies kann durch Ausführen des Skripts `0_activate_wsl_virtual_features` erreicht werden. Nach dem Ausführen dieser Skriptdatei **ist ein Neustart** des Betriebssystems **erforderlich**.

2. WSL Einrichtung:

Sobald das WSL und die Virtual Machine Platform-Funktion aktiviert sind, muss das WSL aktualisiert werden. Dies kann durch Ausführen des Skripts `1_enable_wsl_mode2_update` erfolgen.

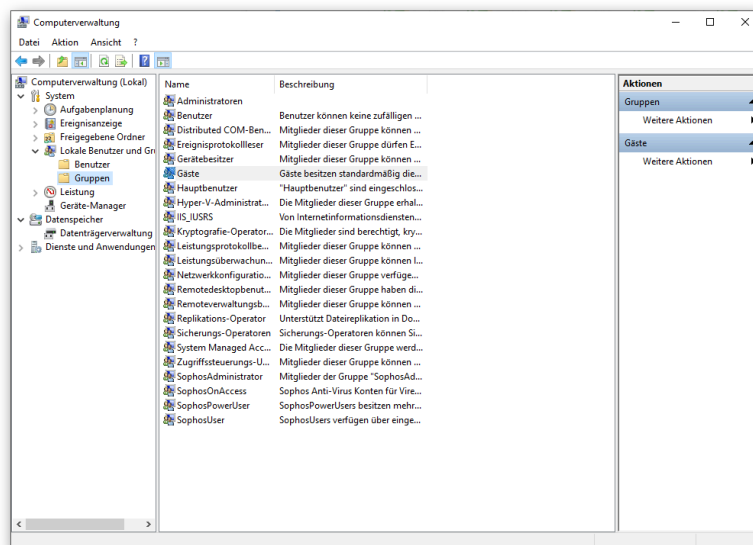
3. Docker-Arbeitsplatz einrichten:

Installation:

- Gehen Sie zu [Docker für Windows](#) und laden Sie das Docker Desktop-Installationsprogramm herunter.
- Mit einem Doppelklick auf Docker Desktop Installer.exe können Sie Docker starten, um das Installationsprogramm auszuführen. Wenn Sie das Installationsprogramm (Docker Desktop Installer.exe) noch nicht heruntergeladen haben, können Sie es von Docker Hub herunterladen. Es wird in der Regel in Ihren Download-Ordner heruntergeladen, oder Sie können es über die Leiste der letzten Downloads unten in Ihrem Webbrowser ausführen.

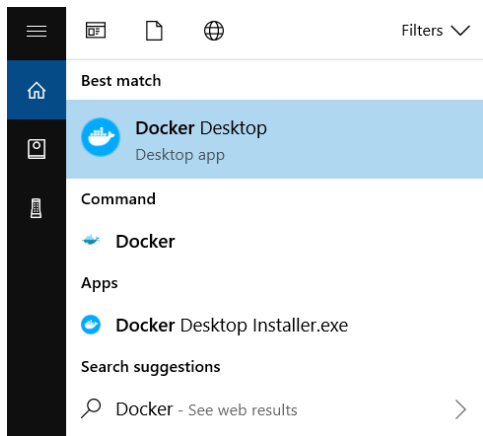


- c. Wenn Sie dazu aufgefordert werden stellen Sie sicher, dass die Option **WSL 2** anstelle von Hyper-V auf der Konfigurationsseite ausgewählt ist.
- d. Folgen Sie den Anweisungen des Installationsassistenten, um das Installationsprogramm zu autorisieren und mit der Installation fortzufahren.
- e. Wenn die Installation erfolgreich ist, klicken Sie auf Schließen, um den Installationsvorgang abzuschließen.
- f. Wenn Ihr Administratorkonto nicht mit Ihrem Benutzerkonto identisch ist, müssen Sie den Benutzer zur Gruppe docker-users hinzufügen. Starten Sie die **Computerverwaltung** als Administrator und navigieren Sie zu **Lokale Benutzer und Gruppen > Gruppen > Gruppen > docker-users**. Klicken Sie mit der rechten Maustaste, um den Benutzer zu der Gruppe hinzuzufügen. Melden Sie sich ab und wieder an, damit die Änderungen wirksam werden.

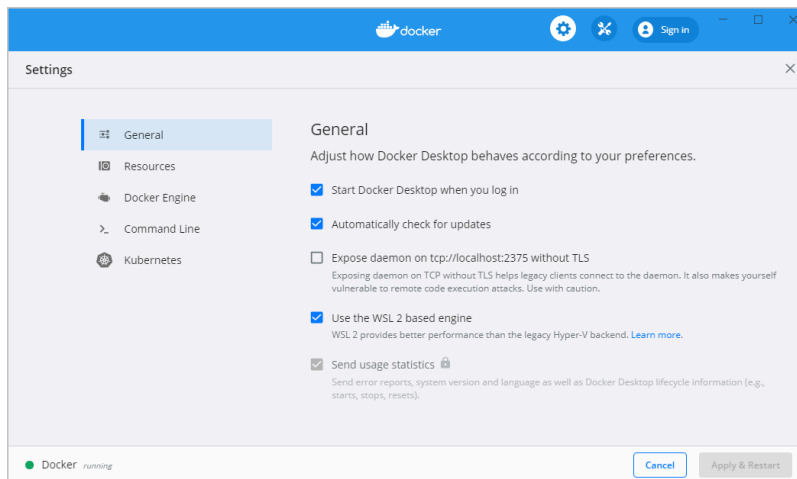


4. Aktivieren der WSL-basierten Engine:

- a. Starten Sie Docker Desktop über das Windows-Startmenü.

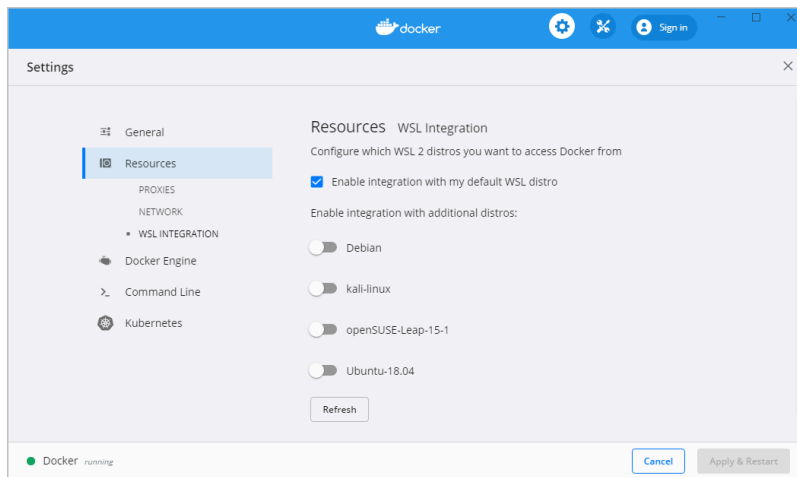


- b. Wählen Sie im Docker-Menü **Einstellungen** > **Allgemein**.
- c. Vergewissern Sie sich, dass die Option WSL 2-basierte Engine ausgewählt ist, wie in der folgenden Abbildung dargestellt.
- d. Betätige **Apply & Restart**.



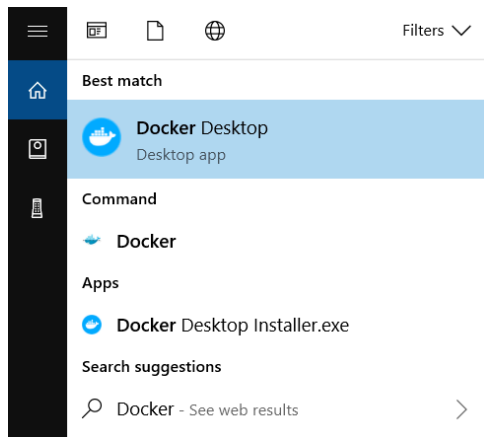
5. Aktivieren der Docker-Unterstützung in WSL 2-Distributionen

- a. Docker benötigt WSL 2 im Hintergrund.
- b. Stellen Sie sicher, dass die Anwendung im WSL 2-Modus läuft.
- c. **Powershell:** `wsl -l -v`
- d. Sie werden die aktuellen Distributionen und deren WSL-Modus sehen. Wenn Ihre Zieldistribution nicht mit v2 läuft, können Sie mit folgendem Befehl Ihre bestehende Linux-Distribution auf v2 aktualisieren
- e. **Powershell:** `wsl --set-version 2`
- f. Starten Sie Docker Desktop und gehen Sie zu **Einstellungen** > **Ressourcen** > **WSL-Integration**. Die Docker-WSL-Integration wird für Ihre Standard-WSL-Distribution aktiviert, wie in der Abbildung dargestellt.



6. Test der Docker-Installation.

Zur Durchführung der folgenden Schritte muss Die Docker-Desktop Applikation gestartet werden.



7. Informationen zur Docker-Engine

- a. Sie können den Befehl `docker version` in die PowerShell oder die Windows-Eingabeaufforderung eingeben. Alle Informationen über den Docker-Desktop werden wie in Abbild gezeigt, angezeigt.

```

C:\Users\NetAnalysis>docker version
Client:
 Cloud integration: v1.0.24
 Version:          20.10.14
 API version:      1.41
 Go version:       go1.16.15
 Git commit:       a224086
 Built:            Thu Mar 24 01:53:11 2022
 OS/Arch:          windows/amd64
 Context:          default
 Experimental:     true

Server: Docker Desktop 4.8.2 (79419)
Engine:
 Version:          20.10.14
 API version:      1.41 (minimum version 1.12)
 Go version:       go1.16.15
 Git commit:       87a90dc
 Built:            Thu Mar 24 01:46:14 2022
 OS/Arch:          linux/amd64
 Experimental:     false
 containerd:

```

- b. Sobald Sie die Docker-Versioneninformationen überprüft haben, ist es notwendig, die Docker-Engine mit einem Hello-World-Docker-Image zu testen. Durch Ausführen des `2_0_test_docker_engine` können Sie überprüfen, ob Ihr Docker-Daemon und -Client funktionieren. Wenn die Installation erfolgreich war, werden Sie die folgenden Informationen sehen.

```

C:\WINDOWS\system32\cmd.exe
Testing Docker Engine...
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29718123e: Pull complete
Digest: sha256:11337d1a85359f42d637adf6da428f76d75dc9afeb3c21faea0d976f5c651
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

Drücken Sie eine beliebige Taste . . .

```

8. Docker mit GPU-Computing

- a. Falls Sie die Möglichkeit haben ein GPU-Computing-Gerät zu verwenden, kann es auch in einem Docker-Container genutzt werden. Daher müssen wir die Integrationsfähigkeit von GPU-Gerät und Docker-Engine prüfen. Wenn **kein GPU-Computing-Gerät** vorhanden ist, können Sie den fließenden **Abschnitt überspringen** und zu Docker ohne CPU-Computing übergehen.
- b. Durch ausführen des Skripts `2_0_test_docker_with_gpu` können Sie die Funktion testen. Sie werden das GPU-Gerät im aktuellen Betriebssystem sehen, wie im folgenden Diagramm dargestellt. *Wir gehen davon aus, dass Sie den GPU-Treiber bereits erfolgreich installiert haben, wie im Abschnitt [NVIDIA-Treiber](#) erläutert.*

```

Eingabeaufforderung
C:\Users\NetAnalysis>docker run --rm --gpus all nvcr.io/nvidia/k8s/cuda-sample:nbody 282 nbody -gpu -benchmark
Unable to find image 'nvcr.io/nvidia/k8s/cuda-sample:nbody' locally
nbody: Pulling from nvidia/k8s/cuda-sample
11323ed2c653: Pull complete
b6166589502e: Pull complete
4f6da51da82: Pull complete
a65da20ce53d: Pull complete
f02d6169d353: Pull complete
56e9fab00773: Pull complete
af3342639518: Pull complete
95e5f8cb48e9: Pull complete
ba0cb6713727: Pull complete
Digest: sha256:fa0c8b471d223df44b82795dee54a7bc36d372fc5a2c7197f8df89e30f2abf48
Status: Download newer image for nvcr.io/nvidia/k8s/cuda-sample:nbody
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
    -fullscreen          (run n-body simulation in fullscreen mode)
    -fp64                (use double precision floating point values for simulation)
    -hostmem             (stores simulation data in host memory)
    -benchmark          (run benchmark to measure performance)
    -numbodies=<N>       (number of bodies (>= 1) to run in simulation)
    -device=<id>         (where id=0,1,2,... for the CUDA device to use)
    -numdevices=<i>       (where i=(number of CUDA devices > 0) to use for simulation)
    -compare             (compares simulation results running once on the default GPU and once on the CPU)
    -cpu                 (run n-body simulation on the CPU)
    -tipsy=<file.bin>     (load a tipsy model file for simulation)

NOTE: The CUDA Samples are not meant for performance measurements. Results may vary when GPU Boost is enabled.

```

9. Semantische Analyse Docker-Image laden:

Während Docker Desktop noch läuft, laden Sie das Docker-Image `docker_image.7z` über den [FTP-Server](#) herunter. Mit Ihren Authentifizierungsdaten können Sie das Docker-Image für die semantische Analyse beziehen. Sobald die Daten erfolgreich heruntergeladen wurden, können sie durch Ausführen des Skripts `3_load_semantic_analysis` geladen werden. Bis das Image in der Docker-Engine geladen ist, kann es eine Weile dauern. Siehe Abbildung.

```

C:\WINDOWS\system32\cmd.exe
Loading MoNA Docker image...
ff4af3169fbd: Loading layer [=====] 570.8MB/570.8MB
c7e7a0e41e0a: Loading layer [=====] 6.048MB/6.048MB
dee42ed298ec: Loading layer [=====] 56.26MB/56.26MB
809c5348e680: Loading layer [=====] 5.891MB/5.891MB
c53575ac1eaf: Loading layer [=====] 7.68kB/7.68kB
279ded52a83a: Loading layer [=====] 2.048kB/2.048kB
90d1d654d643: Loading layer [=====] 2.56kB/2.56kB
19f7f6de07eb: Loading layer [=====] 2.56kB/2.56kB
7b3185ef6560: Loading layer [=====] 2.56kB/2.56kB
87f95e499f29: Loading layer [=====] 6.777GB/6.777GB
e544fa32e5f4: Loading layer [=====] 4.608kB/4.608kB
af5105b2cd26: Loading layer [=====] 18.6MB/18.6MB
3d1be351b1c0: Loading layer [=====] 2.675GB/2.675GB
fb8a3007e1c9: Loading layer [=====] 321.1MB/321.1MB
f14972032fda: Loading layer [=====] 10.24kB/10.24kB
f3699d8362b8: Loading layer [=====] 8.192kB/8.192kB
b020904d4363: Loading layer [=====] 60.51MB/60.51MB
Loaded image: mona_semantic_analysis:1.0
REPOSITORY          TAG          IMAGE ID          CREATED          SIZE
mona_semantic_analysis 1.0          a693bd14387a     2 days ago      10.6GB

```

10. Starte Docker Image:

Nachdem Sie das Docker-Image geladen haben, können Sie nun die semantische Analyse in Docker verwenden. Je nach Gerät können Sie das Docker-Image entweder auf der GPU oder CPU ausführen, indem Sie `4_start_docker_semantic_analysis_gpu` ausführen oder indem Sie `4_start_docker_semantic_analysis_cpu` ausführen. Hier gehen wir davon aus, dass Sie das semantische Analyse-Docker-Image mit GPU verwenden werden. Nach der Ausführung von `4_start_docker_semantic_analysis_gpu` sehen Sie die folgenden Informationen.

```

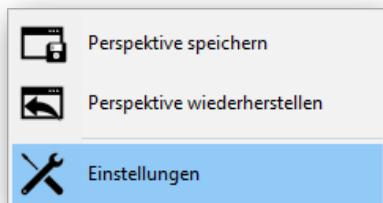
Eingabeaufforderung - E:\JoSemA_Docker\start_docker_semantic_analysis.bat
E:\JoSemA_Docker>E:\JoSemA_Docker\start_docker_semantic_analysis.bat
E:\JoSemA_Docker>docker run --rm -it --gpus=all -p 61527:8086 mona_semantic_analysis:1.0
#supp: appending output to 'nohub.out'
2022-06-13 14:20:00 INFO | summarizer:preprocessing_cleaner | 'pattern' package not found; tag filters are not available for English
2022-06-13 14:20:00 INFO | summarizer:preprocessing_cleaner | 'pattern' package not found; tag filters are not available for English
/usr/local/lib/python3.8/site-packages/past/builtins/misc.py:45: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's
documentation for alternative uses
  from imp import reload
/usr/local/lib/python3.8/site-packages/past/builtins/misc.py:45: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's
documentation for alternative uses
  from imp import reload
2022-06-13 14:20:00 INFO | numexpr.utils | Note: NumExpr detected 16 cores but "NUMEXPR_MAX_THREADS" not set, so enforcing safe limit of 8.
2022-06-13 14:20:00 INFO | numexpr.utils | NumExpr defaulting to 8 threads.
2022-06-13 14:20:00 INFO | numexpr.utils | Note: NumExpr detected 16 cores but "NUMEXPR_MAX_THREADS" not set, so enforcing safe limit of 8.
2022-06-13 14:20:00 INFO | numexpr.utils | NumExpr defaulting to 8 threads.
2022-06-13 14:20:01 INFO | JoSemA | APPLICATION_ROOT /app
2022-06-13 14:20:01 INFO | waitress | Serving on http://0.0.0.0:8086
2022-06-13 14:20:01 INFO | matplotlib.font_manager | generated new fontManager
2022-06-13 14:20:02 INFO | JoSemA | JoSemA common.py Creating semantic annotation models...
2022-06-13 14:20:02 INFO | JoSemA | annotator.py:756:Initializing models on device:cuda
2022-06-13 14:20:02 INFO | JoSemA | cuda device count:2
2022-06-13 14:20:02 INFO | JoSemA | device id:0 name=NVIDIA GeForce RTX 2060
2022-06-13 14:20:02 INFO | JoSemA | device id:1 name=NVIDIA GeForce RTX 2060
2022-06-13 14:20:07 INFO | JoSemA | annotator.py:194:cuda
2022-06-13 14:20:08 INFO | fairseq.tasks.speech_to_text | dictionary size (spm_unigram_10000.txt): 10,000
2022-06-13 14:20:13 INFO | fairseq.tasks.speech_to_text | pre-tokenizer: ('tokenizer': None)
2022-06-13 14:20:13 INFO | fairseq.tasks.speech_to_text | tokenizer: ('bpe': 'sentencepiece', 'sentencepiece_model': '/app/flaskapp/fairseq/checkpoints/e
n_unigram_10000.model')
2022-06-13 14:20:14 INFO | JoSemA | annotator.py:71:Loaded DomainClassifier from/app/flaskapp/resnet/checkpoint/resnet152_1002.pth
2022-06-13 14:20:16 INFO | JoSemA | Loading feature backbone from /app/flaskapp/boa/checkpoint/boa-caffe-frcn-r101_with_attributes.pth
load captioning model from /app/flaskapp/ingv/captioning/checkpoint/common_domain/en/emt.pth
2022-06-13 14:20:17 INFO | JoSemA | annotator.py:619:cuda

```

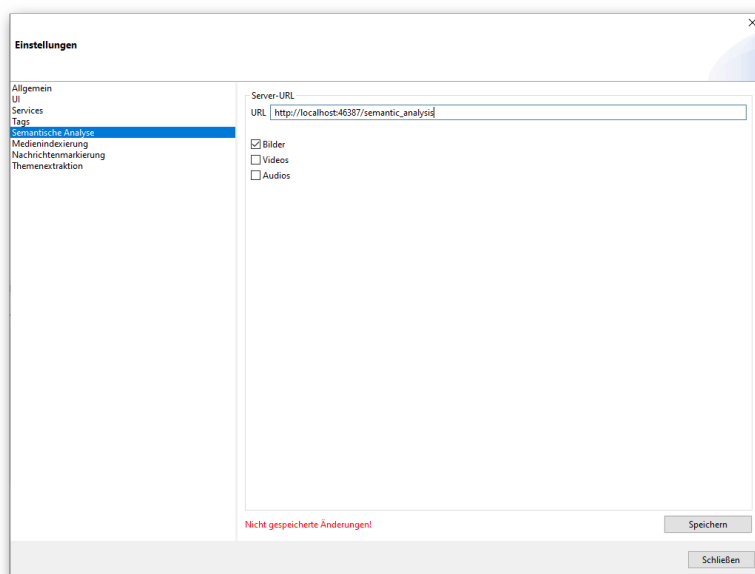
Der einzige Unterschied besteht darin, dass das Docker-Image auf der CPU gestartet wird, wenn Sie den Befehl `4_start_docker_semantic_analysis_cpu` ausführen.

11. MoNA Einstellungen anpassen

- a. Öffnen Sie über die Navigationsleiste Ansicht -> Einstellungen -> Semantische Analyse.



- b. Folgende URL `http://localhost:46387/semantic_analysis` einfügen. Die Port-Nummer kann sich an Ihrem System unterscheiden.



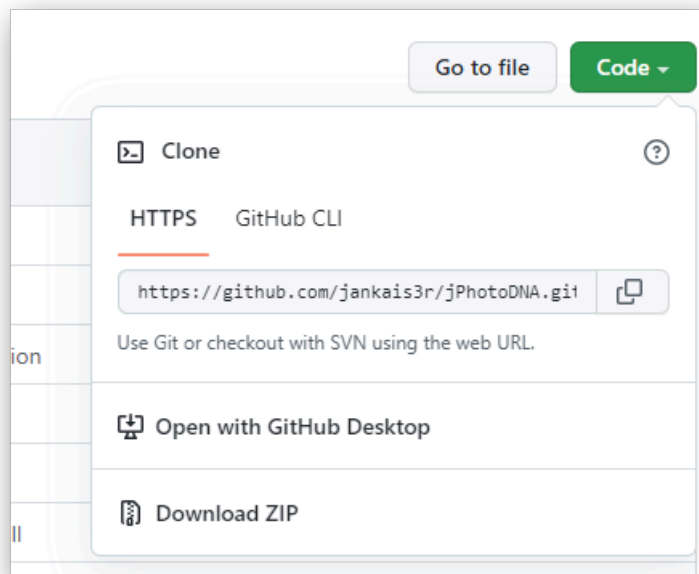
- c. Auswahl der Medientypen für die Semantische Analyse (Bilder, Videos, Audios). Dabei ist die Leistung des Systems zu beachten.
- d. Speichern betätigen
- e. Links Unten auf die Bestätigung warten, dass der Server in Funktion ist.

2.1.6. PhotoDNA einrichten.

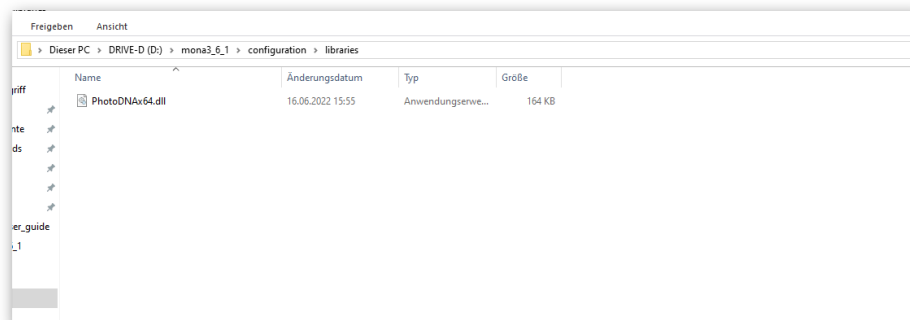
Für die Verwendung der externen Software und ihren Funktionen in MoNA werden folgende Schritte vorausgesetzt. PhotoDNA ist ein von Jan Kaiser (Digitaler Forensiker bei Alvarez & Marsal) programmiertes Open Source Projekt, welches über [GitHub](#) bereitgestellt wird. Mit folgenden Schritten wird PhotoDNA in MoNA implementiert:

Prozedur

1. PhotoDNA Projektdateien von GitHub herunterladen (Code -> Download ZIP)



2. ZIP entpacken
3. install.bat ausführen.
4. PhotoDNA.dll in ./configuration/libraries verschieben.

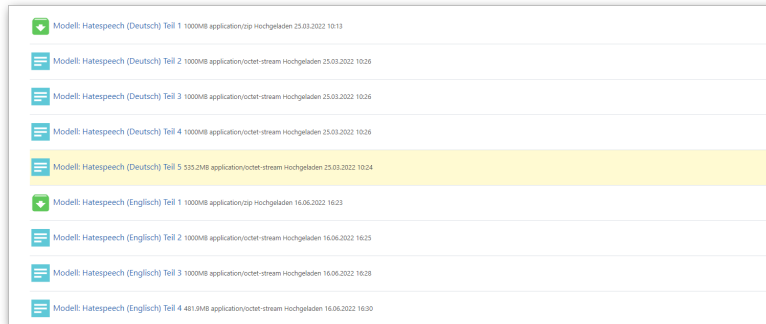


2.1.7. Modelle für Nachrichtenmarkierung importieren

MoNA bietet die Möglichkeit mit Sprachmodellen Chats automatisch auf Hassrede zu untersuchen. Dabei gibt es in der aktuellen Version ein deutschsprachiges und englischsprachiges Modell. Die Modelle werden über [Moodle](#) zur Verfügung gestellt.

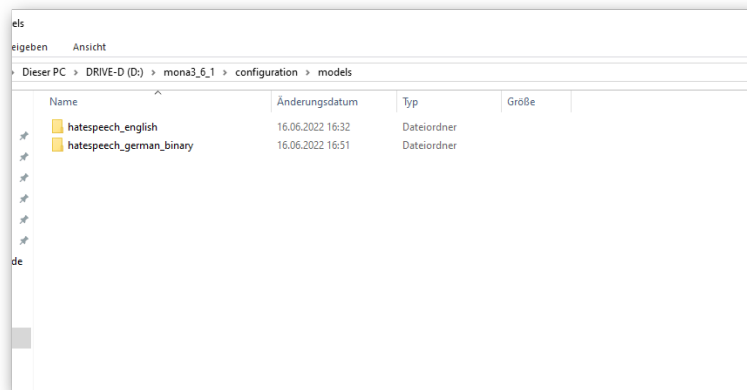
Prozedur

1. Die Sprachmodelle von [Moodle](#) herunterladen. Dabei müssen alle Teile einer Sprache heruntergeladen werden.

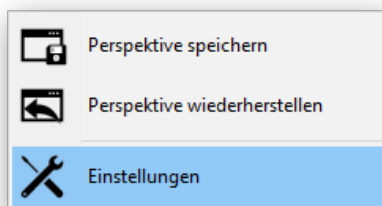


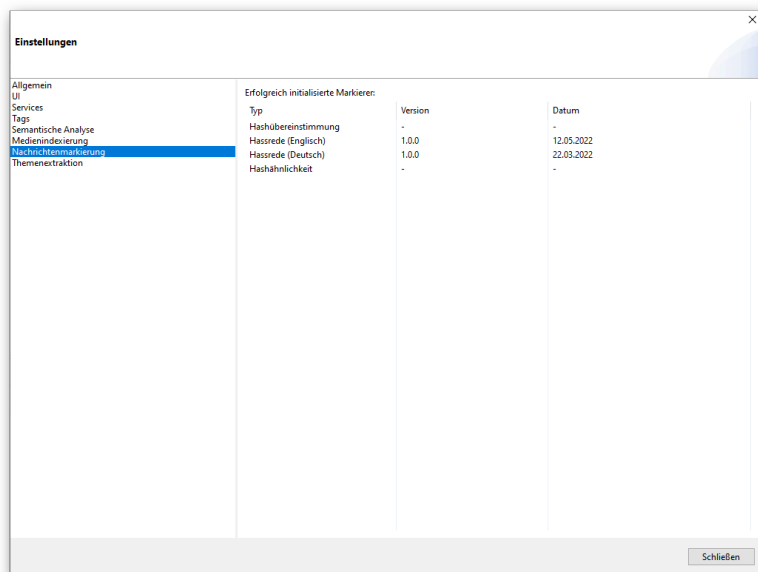
<https://moodle.hs-mittweida.de/course/view.php?id=498>

2. Teil 1 ZIP entpacken. Die restlichen werden danach automatisch mitentpackt. **Achtung erst beginnen, wenn alle Dateien vollständig heruntergeladen sind.**
3. In den Ordner `.configurations/models` verschieben.



4. In MoNA unter Ansicht -> Einstellungen -> Nachrichtenmarkierung überprüfen ob das Sprachmodell geladen wurde (siehe 2. Abbildung).





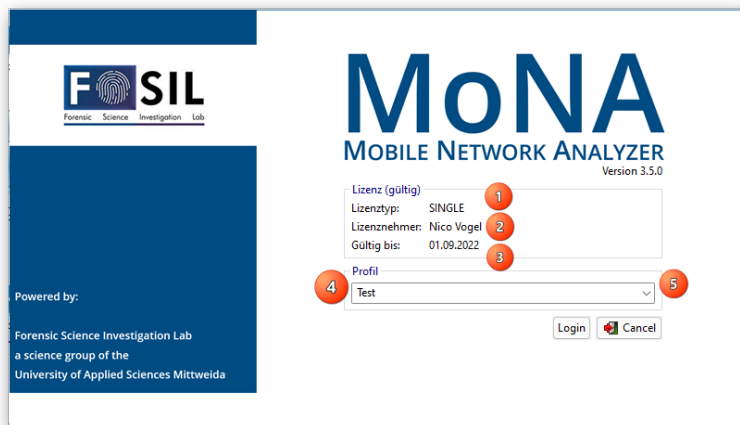
2.2. Erste Schritte

Im Folgenden werden alle grundlegenden Funktionen erläutert. Das Anlegen von Untersuchungen und Mobilien Endgeräten bilden die Voraussetzung für die Arbeit mit MoNA und können nur in dieser Reihenfolge durchgeführt werden. Die Untersuchung bildet als logische Entität den Kern der Arbeit mit MoNA. In ihr werden alle wichtigen Rahmenbedingungen und Daten gespeichert. Hierdurch können Fälle sortiert und getrennt gehalten werden. Innerhalb der Untersuchung können mehrere Mobile Endgeräte initialisiert werden. Diese sollen die physischen Asservate widerspiegeln, um eine eindeutige Zuordnung der Daten zu gewährleisten. Die zuletzt erläuterten Backups sind nur für einen Versionswechsel relevant und spielen im Normalbetrieb keine Rolle.

2.2.1. Startdialog

Der Startdialog beinhaltet wichtige Informationen über das verwendete Profil und der Lizenz. Zusätzlich bietet er außerdem Informationen über die Version und Entwickler von MoNA.


Das Profil ermöglicht es unter einer Lizenz mehrere Benutzer zu trennen.



Ein neues Profil wird wie folgt angelegt

1. Name des gewünschten Profils in Leiste angeben (siehe 4).
2. Login betätigen.

Bemerkung

Bereits bestehende Profile können durch  (siehe 5) aufgelistet werden. Und wie oben ausgewählt und geöffnet werden.

Zur Lizenz bietet MoNA 3 Informationen:

- Lizenztyp (siehe 1)
- Lizenznehmer (siehe 2)
- Gültigkeitsdauer (siehe 3)



Bemerkung

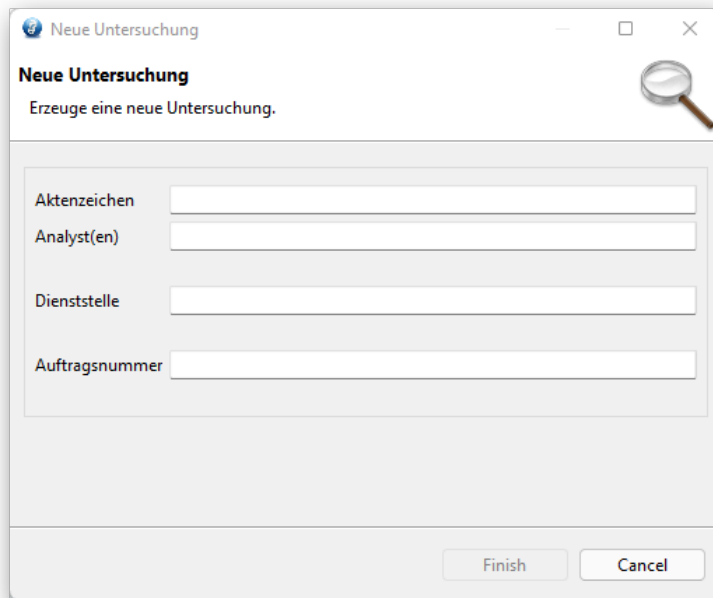
Eine Verlängerung der Lizenz können Sie unter siewerts@hs-mittweida.de beantragen.

2.2.2. Untersuchung anlegen

Jede Arbeit in MoNA beginnt mit einer Untersuchung. Diese fungiert als Projekt, dass heißt sie umfasst alle Daten und Analysen. Untersuchungen können geschlossen und wieder geöffnet werden, um ein datenkonsistentes Arbeiten zu ermöglichen. Zusätzlich ermöglicht es Arbeitsschritte zwischenspeichern. Außerdem speichert sie die Rahmenbedingungen der Ermittlung wie: Aktennummer, Namen der Ermittler/Analysten etc, welche für einen späteren [Report](#) verwendet werden können.

Prozedur

1. Navigationsbereich anwählen 
2. Das grüne Plus in der Navigationsleiste anwählen 
3. Rahmeninformationen der Untersuchung eintragen. (Aktennummer wird benötigt, alle weiteren Informationen sind optional)





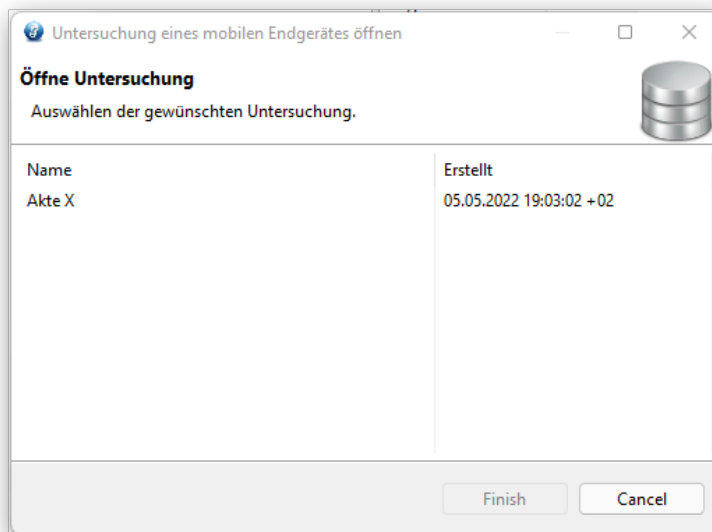
4. Finish bestätigen.

2.2.3. Untersuchung öffnen

Eine zuvor angelegte Untersuchung kann nach erfolgreichem Speichern wieder geöffnet werden.

Prozedur

1. Navigationsbereich anwählen 
2. Das Koffer Symbol in der Navigationsleiste anwählen 
3. gewünschte Untersuchung auswählen



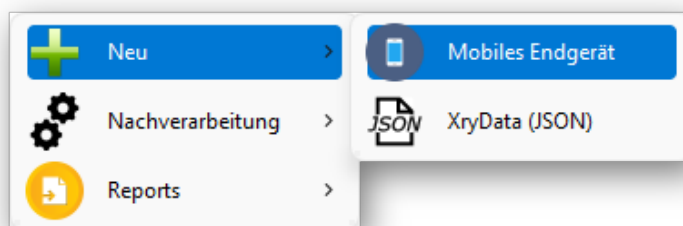
4. Finish betätigen.

2.2.4. Mobiles Endgerät anlegen

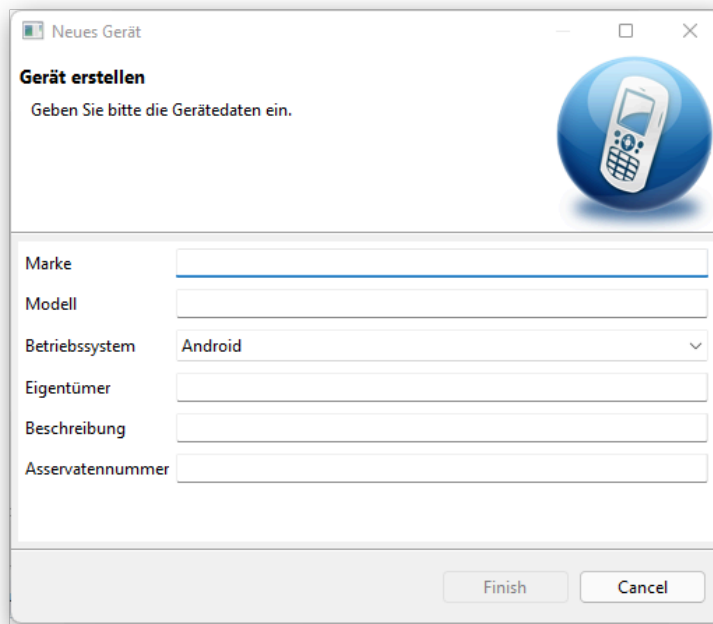
Jede Analyse eines Chats beginnt mit dem Anlegen des Mobilen Endgerätes, von welchem der Chat stammt. Das Mobile Endgerät soll den physischen Datenträger in die digitale Welt überführen. Dies ermöglicht eine genaue Zuordnung von relevanten Daten zu den Eigentümer der Beweismittel. In dieser Instanz werden Information über das Beweismittel, wie: den Eigentümern, Asservatenummer, usw. gespeichert.

Prozedur

1. Navigationsbereich anwählen
2. Rechtsklick in die leere Fläche der Untersuchung.
3. Neu anwählen und Mobiles Endgerätanwählen.



4. Informationen zu Beweismittel angeben.



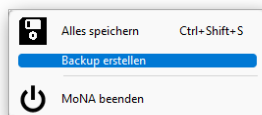
5. Finish betätigen.

2.2.5. Backup erstellen

Durch das Backup werden alle Untersuchungen und Konfigurationen gespeichert. Dies ermöglicht den Austausch von Daten zwischen Geräten. Für die versionsübergreifende Arbeit ist die Speicherung als Backup auch nötig.

Prozedur

1. Navigationsleiste -> Datei -> Backup erstellen



2. Speicherort wählen
3. Speichern betätigen

2.3. Daten einlesen

In der aktuellen MoNA Version können **WhatsApp-, Telegram-, Facebook Messenger- Chats und Emails von Android und iOS Geräten**, welche gemeinsam von 97,28% der Nutzer verwendet werden ⁽¹⁾, importiert werden. Zusätzlich können **UFDR Reports direkt von Cellebrite UFED** (aktuell nur bei Android möglich) importiert werden. Das Importverfahren unterscheidet sich zwischen den Messengern und Betriebssystemen. MoNA bietet ausschließlich die Funktionalität der Analyse der Daten, das heißt **alle Daten müssen zuvor extrahiert und entschlüsselt werden**. In der aktuellen Version bietet MoNA für die extrahierten Messenger Daten 3 Arten von Importverfahren. Der intelligente Datenimport sucht die relevanten rekursiv in dem angegebenen Ordner. Für den Anwender ist dies die einfachste Variante, da hier keine Datenbankenstrukturen beachtet werden müssen. Diese Funktion ist momentan nur für den Import von Facebook Messenger Daten aus iOS und UFDR Daten für Android implementiert. Die Funktion soll in Zukunft auf alle Messenger ausgeweitet werden. Bereits für alle Messenger ist der vereinfachte Datenimport möglich. Hierbei muss der Root Ordner des Messengers ausgewählt werden, wobei die Ordnerstruktur relevant ist. Zuletzt hat der Anwender die Möglichkeit eines manuellen Imports. Dabei müssen alle relevanten Daten einzeln ausgewählt werden z.B. die Datenbankdatei der Nachrichten und Kontakte. Alle Importverfahren werden in gegebener Reihenfolge beim Import von MoNA angeboten (Intelligenter-, vereinfachter- und manueller Datenimport).

⁽¹⁾StatCounter (2022, März). Marktanteile der führenden mobilen Betriebssysteme an der Internetnutzung mit Mobiltelefonen in Deutschland von Januar 2009 bis März 2022. [Online]. Available: <https://de.statista.com/statistik/daten/studie/184332/umfrage/marktanteil-der-mobilen-betriebssysteme-in-deutschland-seit-2009/#professional>.

2.3.1. UFDR Report Daten einlesen

MoNA bietet für den Import von UFDR Report Daten einen intelligenten Datenimport, welcher ein vereinfachtes Importverfahren ermöglicht. Der Importprozess unterscheidet sich bei UFDR-Daten nicht bezüglich des Betriebssystems. **Die Qualität der Daten hängt hierbei maßgeblich von der Vorselektion in Celebrite UFED ab.** MoNA kann nur mit Daten arbeiten die auch in der Reportdatei vorhanden sind.

Warum und wann dieser Vorgang ausgeführt wird

Um UFDR Report Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von UFDR Daten von einem Android oder iOS Gerät gibt es folgende


Voraussetzungen:

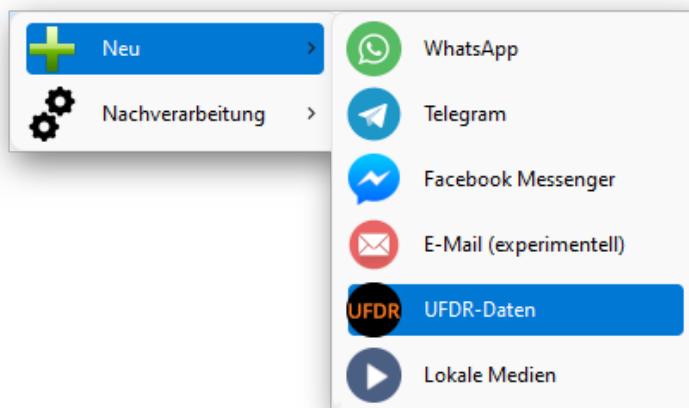
- Alle Fallrelevanten Daten wurden in UFED ausgewählt und in die Report Datei exportiert.
- Aktuelle Celebrite UFED Physical Analyzer Version. *Referenz Version: 7.52.0.36*

Wichtig

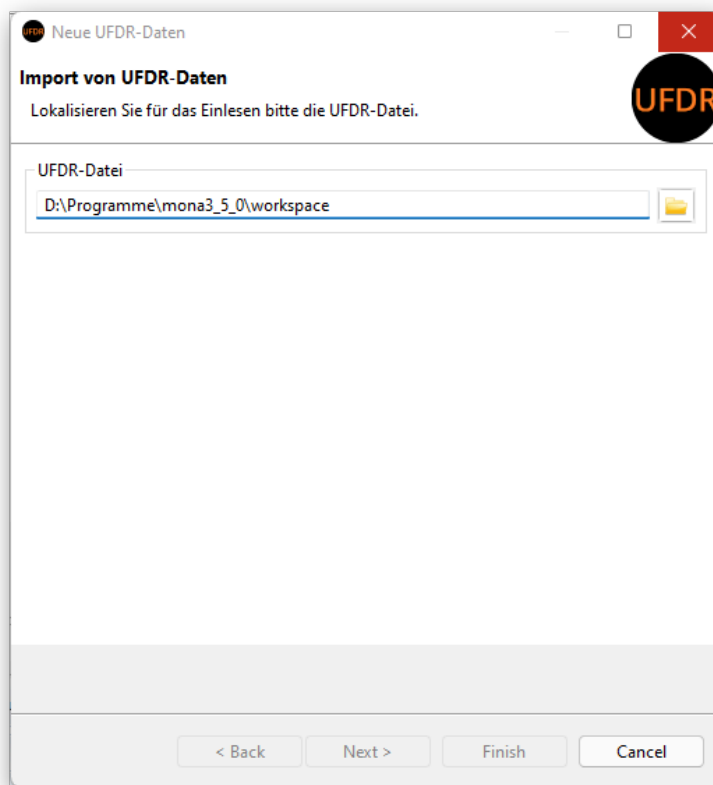
Aktuell nur mit Android Daten möglich.

Prozedur

1. Navigationsbereich anwählen. 
2. Das zuvor angelegte mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> UFDR-Daten



4. Die UFDR Report Datei auswählen.  -> Datei auswählen -> Öffnen.



5. Next betätigen.
6. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
7. Finish betätigen.

2.3.2. WhatsApp Daten einlesen (Android)

MoNA bietet für WhatsApp Daten aus Android einen vereinfachten Datenimport, welcher ein schnelles Importverfahren ermöglicht. Dabei erwartet MoNA eine bestimmte Ordnerstruktur, welche beachtet werden muss.

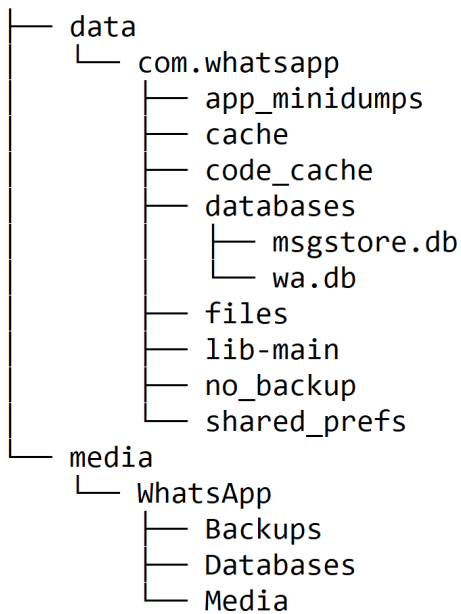
Warum und wann dieser Vorgang ausgeführt wird

Um WhatsApp Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von WhatsApp Daten von einem Android Gerät gibt es folgende

Voraussetzungen:

Für den vereinfachten Datenimport	Für den manuellen Import:
Root/ data Ordner	com.whatsapp Ordner
-	WhatsApp Ordner mit Medien
(optional) externer Media Ordner	(optional) externer Media Ordner

Die Daten sollten im folgenden Format vorliegen:



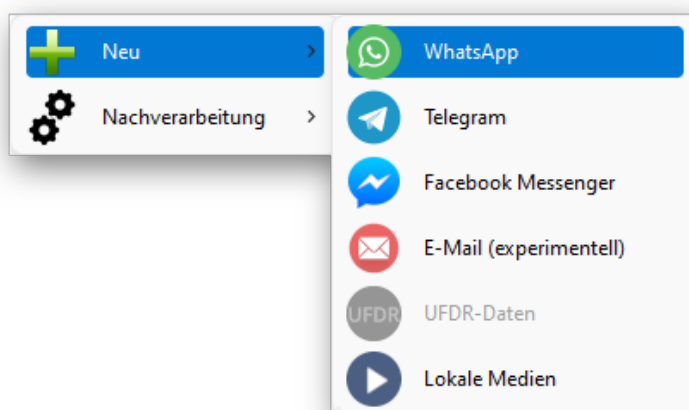
Wenn die Daten dem entsprechend vorliegen kann mit dem Import begonnen werden.

Achtung

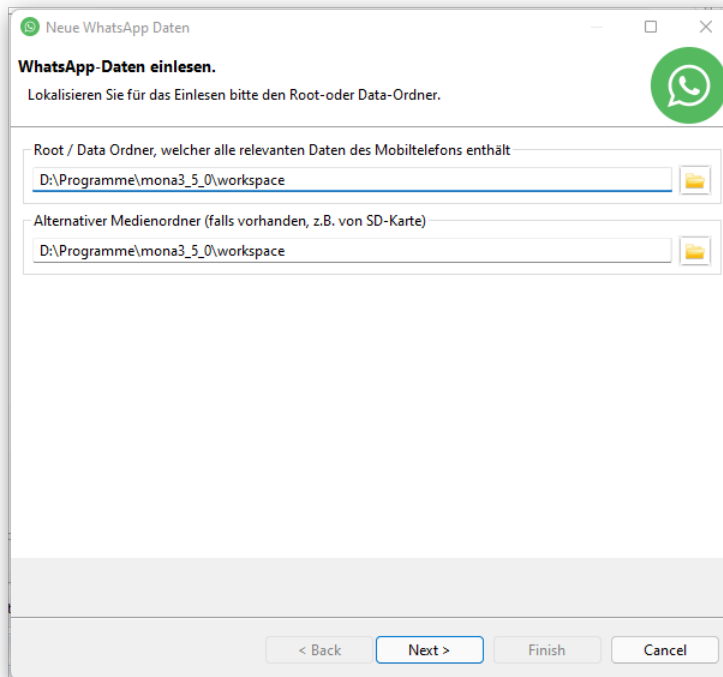
Ist die gegebene Ordnerstruktur nicht gegeben muss anstatt Schritt 4, Schritt 5 befolgt werden.

Prozedur

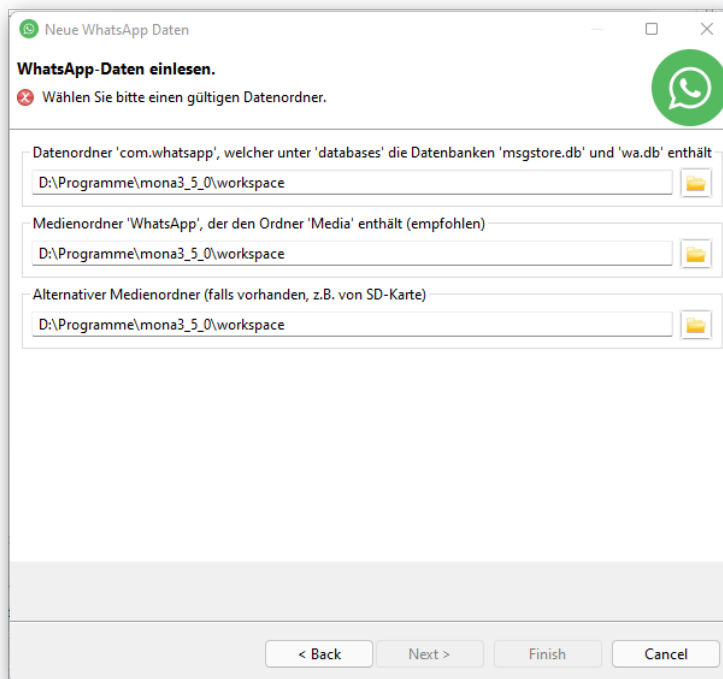
1. Navigationsbereich anwählen. [🔗](#)
2. Das zuvor angelegte und dem Chat zugehörigen Mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> WhatsApp



4. Für den vereinfachten Import: Im ersten Feld den Root/ data Ordner und (optional) im zweiten Feld den externen Medienordner auswählen. 📁 -> Datei auswählen -> Öffnen.



5. Bei nicht erfolgreichen Import durch den vereinfachten Import kann der manuellen Import durchgeführt werden. Next -> com.whatsapp Ordner auswählen -> WhatsApp Ordner auswählen -> (optional) Medien Order auswählen com.whatsapp muss unter databases, msgstore.db und wa.db enthalten (siehe [Struktur oben](#)).



6. Next > betätigen.
 7. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
 8. Finish betätigen.

2.3.3. WhatsApp Daten einlesen (iOS)

MoNA bietet für WhatsApp Daten aus iOS einen vereinfachten Datenimport, welcher ein schnelles Importverfahren ermöglicht. Dabei erwartet MoNA eine bestimmte Ordner Struktur, welche beachtet werden muss.

Warum und wann dieser Vorgang ausgeführt wird

Um WhatsApp Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von WhatsApp Daten von einem iOS Gerät gibt es folgende

Voraussetzungen:

Für den vereinfachten Datenimport	Für den manuellen Import:
Root/ data Ordner	ChatStorage.sqliteS Datei
(optional) externer Media Ordner	(optional) externer Media Ordner

Die Daten sollten im folgenden Format vorliegen:


```
group.net.whatsapp.WhatsApp.shared
├── BackedUpKeyValue.sqlite
├── Biz
├── CallHistory.sqlite
├── ChatStorage.sqlite
├── consumer_version
├── ContactsV2.sqlite
├── current_wallpaper_dark.jpg
├── current_wallpaper.jpg
├── emoji.sqlite
├── FieldStats2
├── Library
├── Logs
├── Message
├── mona
├── Ranking.sqlite
├── stickers
└── Sticker.sqlite
```

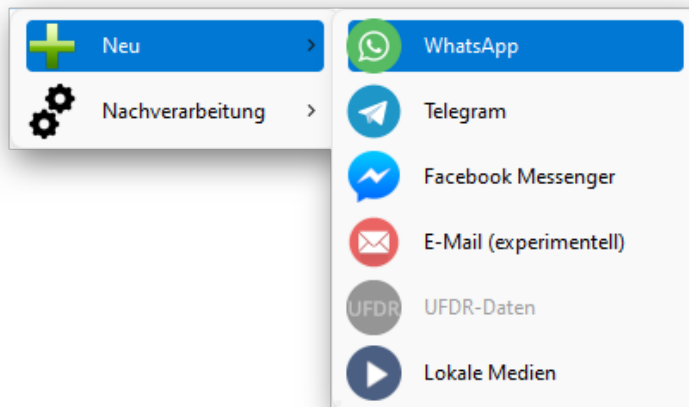
Wenn die Daten dem entsprechend vorliegen kann mit dem Import begonnen werden.

Achtung

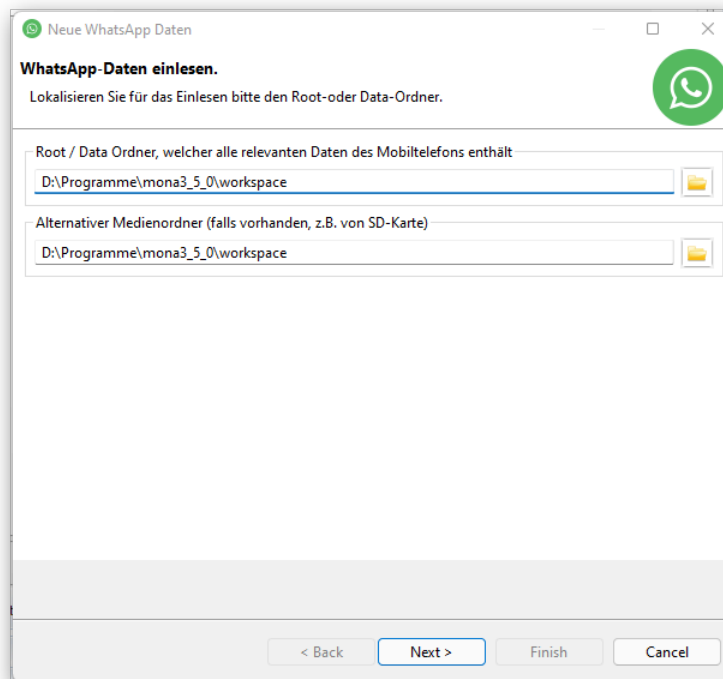
Ist die gegebene Ordnerstruktur nicht gegeben muss anstatt Schritt 4, Schritt 5 befolgt werden.

Prozedur

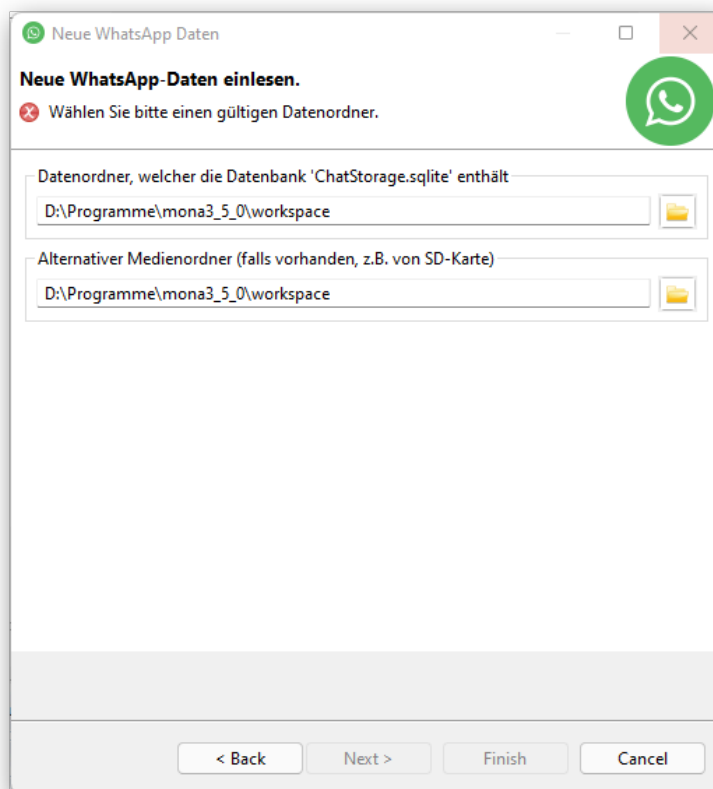
1. [Navigationsbereich](#) anwählen. 
2. Das zuvor angelegte und dem Chat zugehörigen Mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> WhatsApp



4. Für den vereinfachten Import: Im ersten Feld den Root/ data Ordner und (optional) externer Medien Order auswählen. 📁 -> Datei auswählen -> Öffnen.



5. Bei nicht erfolgreichen Import durch den vereinfachten Import kann der manuellen Import durchgeführt werden. Next -> Datenbank Ordner auswählen -> (optional) Medien Order auswählen Datenbank Ordner muss ChatStorage.sqlite enthalten (siehe [Struktur oben](#)).



6. Next > betätigen.
7. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
8. Finish betätigen.

2.3.4. Telegram Daten einlesen (Android)

MoNA bietet für Telegram Daten aus Android einen vereinfachten Datenimport, welcher ein schnelles Importverfahren ermöglicht. Dabei erwartet MoNA eine bestimmte Ordner Struktur, welche beachtet werden muss.

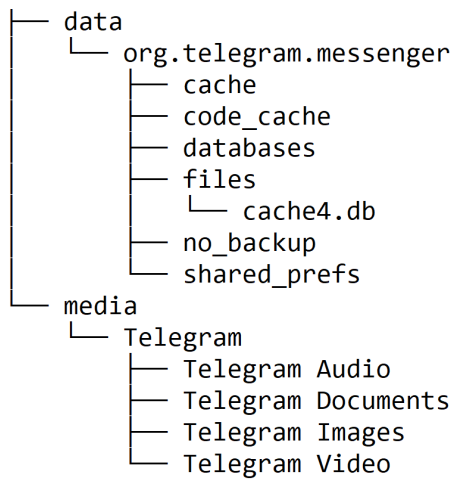
Warum und wann dieser Vorgang ausgeführt wird

Um Telegram Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von Telegram Daten von einem Android Gerät gibt es folgende

Voraussetzungen:

Für den intelligenten Datenimport	Für den manuellen Import:
Root/ data Ordner mit allen Daten	org.telegram.messenger Ordner
-	Telegram Ordner mit Medien
-	(optional) cache Ordner
(optional) externer Media Ordner	(optional) externer Media Ordner

Daten sollten im folgenden Format vorliegen:



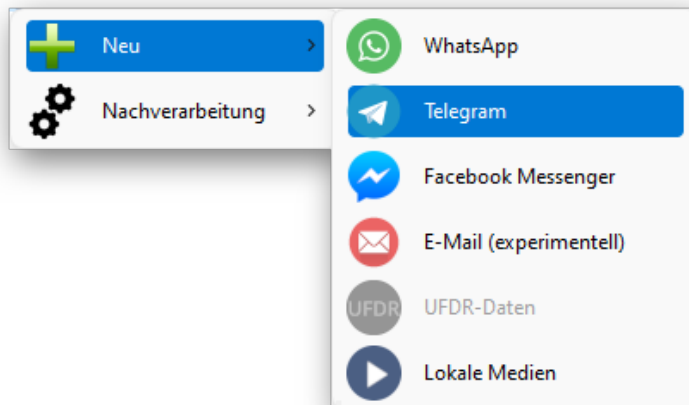
Wenn die Daten dem entsprechend vorliegen kann mit dem Import begonnen werden.

Achtung

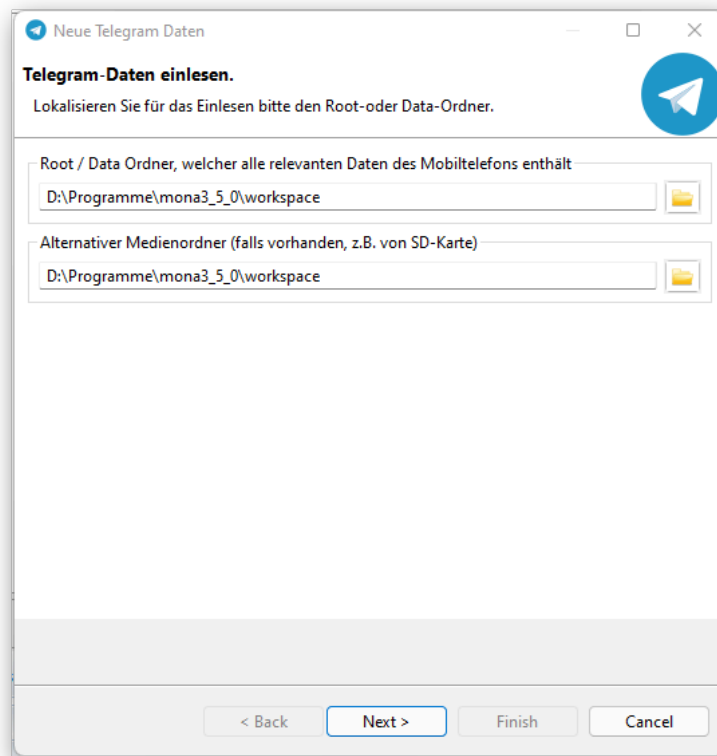
Ist die gegebene Ordnerstruktur nicht gegeben muss anstatt Schritt 4, Schritt 5 befolgt werden.

Prozedur

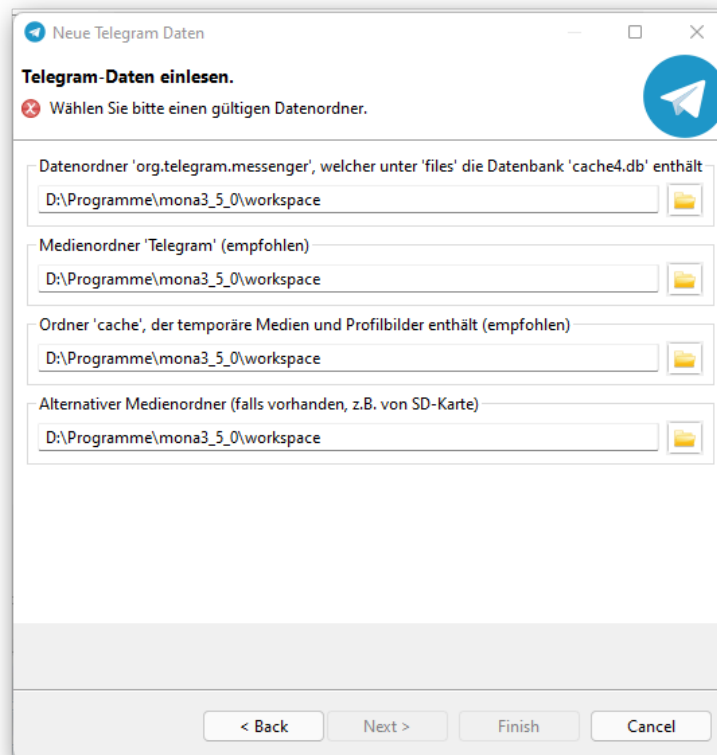
1. Navigationsbereich anwählen. [🔗](#)
2. Das zuvor angelegte und dem Chat zugehörigen Mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> Telegram



4. Für den vereinfachte Import: Im ersten Feld den Root/ data Ordner und (optional) externer Medien Order auswählen. 📁 -> Datei auswählen -> Öffnen.



5. Bei nicht erfolgreichen Import durch den vereinfachten Import kann der manuellen Import durchgeführt werden. Next -> org.telegram.messenger Ordner auswählen -> Telegram Ordner auswählen -> (optional) cache Ordner auswählen -> (optional) externer Medien Order auswählen
org.telegram.messenger muss unter files, cache4.db enthalten (siehe [Struktur oben](#)).



6. Next > betätigen.
7. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
8. Finish betätigen.

2.3.5. Telegram Daten einlesen (iOS)

MoNA bietet für Telegram Daten aus iOS einen vereinfachten Datenimport, welcher ein schnelles Importverfahren ermöglicht. Dabei erwartet MoNA eine bestimmte Ordner Struktur, welche beachtet werden muss.

Warum und wann dieser Vorgang ausgeführt wird

Um Telegram Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von Telegram Daten von einem iOS Gerät gibt es folgende

Voraussetzungen:

Für den intelligenten Datenimport	Für den manuellen Import:
Root/ data Ordner mit allen Daten	telegram-data Ordner
(optional) externer Media Ordner	(optional) externer Media Ordner

Daten sollten im folgenden Format vorliegen:

```

telegram-data
├── account-14064689701717446085
│   ├── calls
│   ├── network-stats
│   ├── notificationsKey
│   └── mailbox
│       ├── db
│       │   └── db_sqlite
│       └── media


```

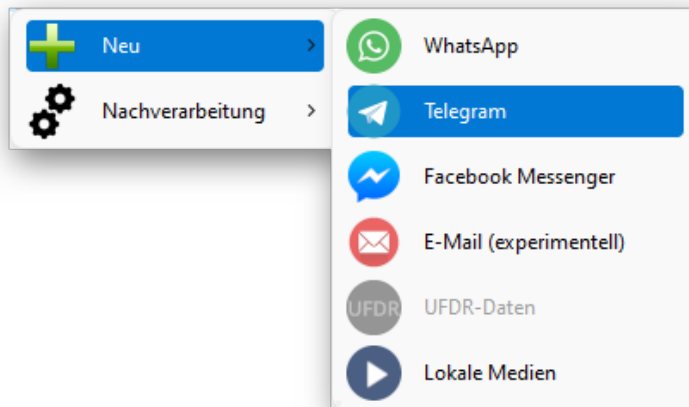
Wenn die Daten dem entsprechend vorliegen kann mit dem Import begonnen werden.

Achtung

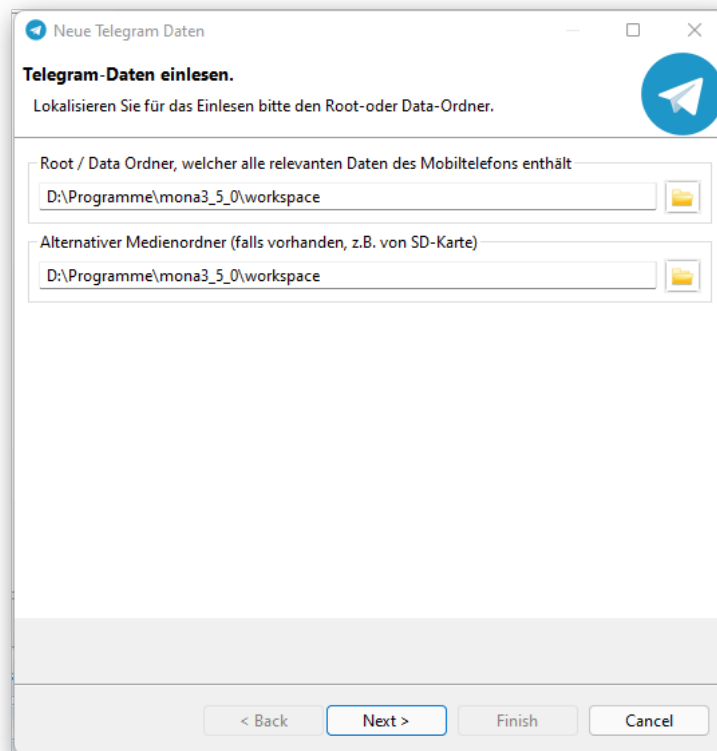
Ist die gegebene Ordnerstruktur nicht gegeben muss anstatt Schritt 4, Schritt 5 befolgt werden.

Prozedur

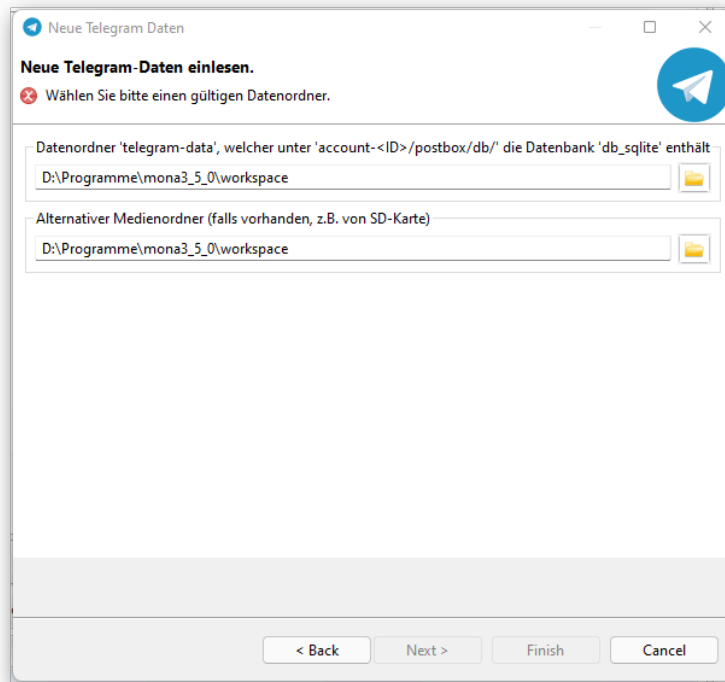
1. [Navigationsbereich](#) anwählen. 
2. Das zuvor angelegte und dem Chat zugehörigen Mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> Telegram



4. Für den vereinfachte Import: Im ersten Feld den Root / data Ordner und (optional) externer Medien Order auswählen. 📁 -> Datei auswählen -> Öffnen.



5. Bei nicht erfolgreichen Import durch den vereinfachten Import kann der manuellen Import durchgeführt werden. Next -> telegram-data Ordner auswählen -> (optional) cache Ordner auswählen -> (optional) externer Medien Order auswählen telegram-date muss unter account-<ID>/postbox/db,db_sqlite (<ID> wird durch Account ID des Nutzers ersetzt) enthalten (siehe Struktur oben).



6. Next > betätigen.
7. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
8. Finish betätigen.

2.3.6. Facebook Messenger Daten einlesen (Android)

MoNA bietet für Facebook Messenger Daten aus Android einen intelligenten Datenimport, welcher ein schnelles Importverfahren ermöglicht. Dabei muss keine Ordnerstruktur beachtet werden, wie bei dem vereinfachten Import. MoNA durchsucht den angegebenen Ordner rekursiv nach allen relevanten Daten.

Warum und wann dieser Vorgang ausgeführt wird

Um Facebook Messenger Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von Facebook Messenger Daten von einem Android Gerät gibt es folgende

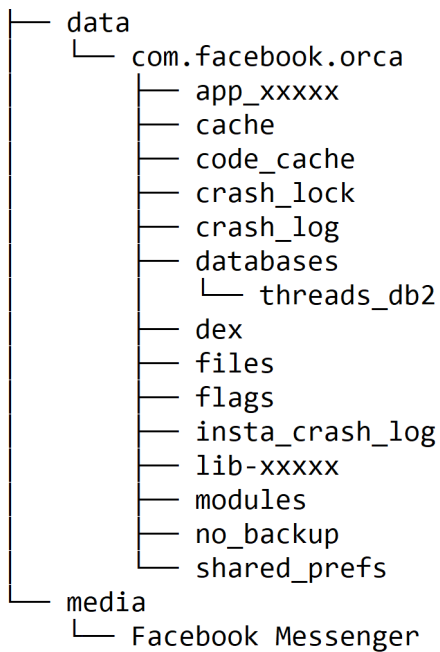
Voraussetzungen:

Für den intelligenten Import	Für den vereinfachten Import	Für den manuellen Import:
Ordner mit allen relevanten Daten	Root / data Ordner	databases Ordner
-	-	Facebook Messenger Ordner mit Medien
-	(optional) externer Media Ordner	(optional) externer Media Ordner

Wichtig

Aktuell intelligenter Datenimport nur mit iOS Daten möglich.

Daten sollten im folgenden Format vorliegen (**nur für vereinfachten Datenimport relevant**):




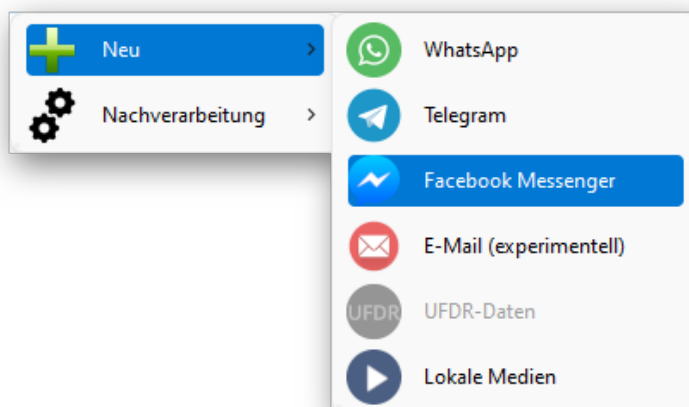
Wenn die Daten dem entsprechend vorliegen kann mit dem Import begonnen werden.


Achtung

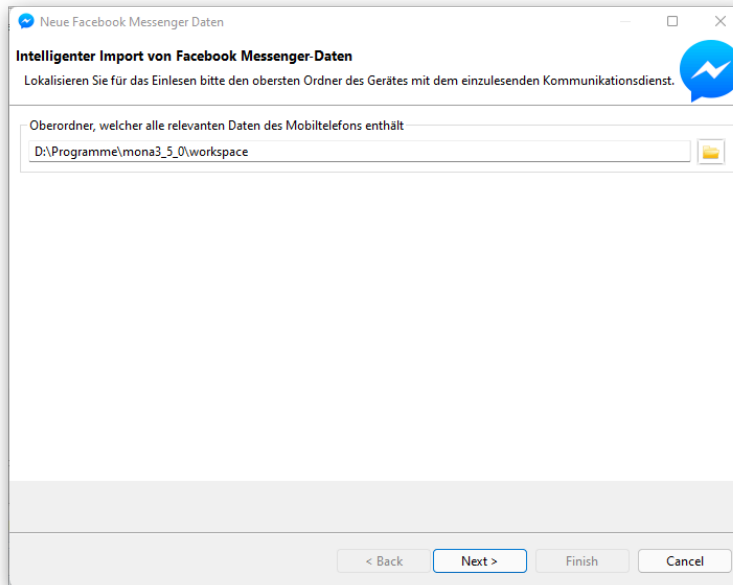
Ist die gegebene Ordnerstruktur nicht gegeben muss anstatt Schritt 5, Schritt 6 befolgt werden.

Prozedur

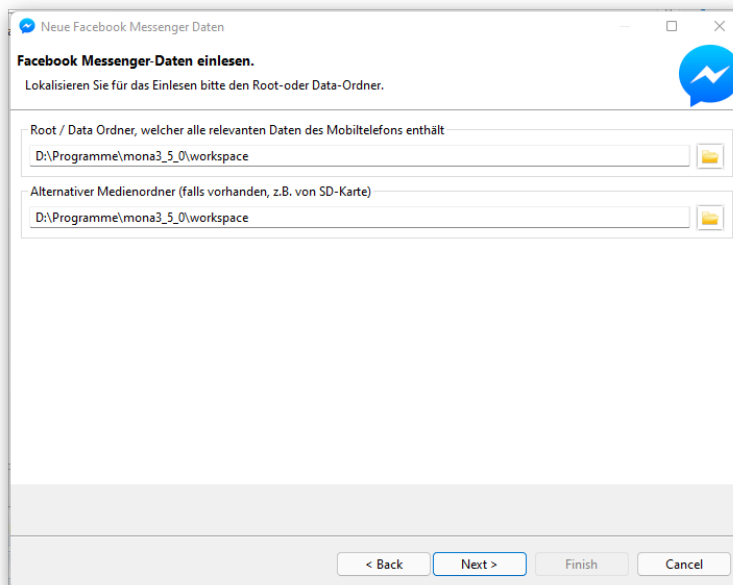
1. Navigationsbereich anwählen. 
2. Das zuvor angelegte und dem Chat zugehörigen Mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> Facebook Messenger



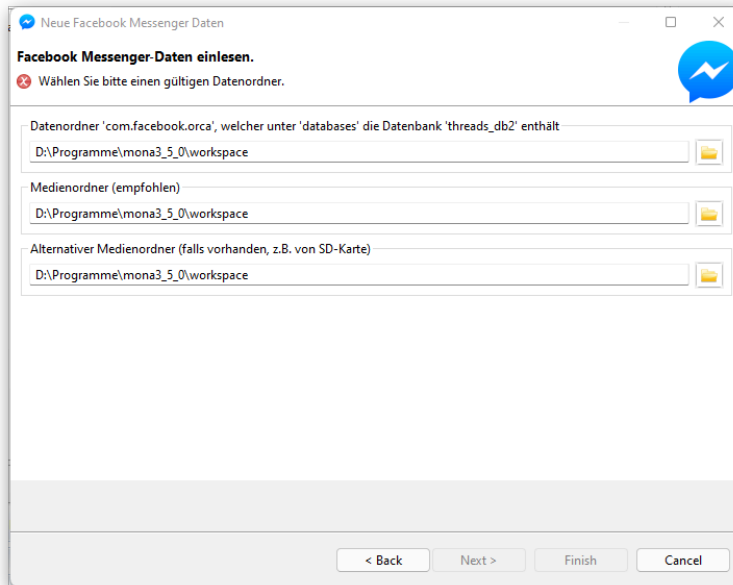
4. Für den intelligenten Import: Ordner mit allen relevanten Daten auswählen.  -> Datei auswählen -> Öffnen.



5. Für den vereinfachte Import: Im ersten Feld den Root/ data Ordner und (optional) externer Medien Ordner auswählen. 📁 -> Datei auswählen -> Öffnen.



6. Bei nicht erfolgreichen Import durch den vereinfachten Import kann der manuellen Import durchgeführt werden. Next -> databases Ordner auswählen-> Facebook Messenger Ordner auswählen -> (optional) externer Medien Ordner auswählen. databases Ordner muss unter databases , threads_db2 enthalten (siehe [Struktur oben](#)).



7. Next > betätigen.
8. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
9. Finish betätigen.

2.3.7. Facebook Messenger Daten einlesen (iOS)

MoNA bietet für Facebook Messenger Daten aus iOS einen intelligenten Datenimport, welcher ein schnelles Importverfahren ermöglicht. Dabei muss keine Ordnerstruktur beachtet werden, wie bei dem vereinfachten Import. MoNA durchsucht den angegebenen Ordner rekursiv nach allen relevanten Daten.

Warum und wann dieser Vorgang ausgeführt wird

Um Facebook Messenger Daten analysieren zu können müssen sie zuerst importiert werden. Für den Import von Facebook Messenger Daten von einem iOS Gerät gibt es folgende

Voraussetzungen:

Für den intelligenten Import	Für den vereinfachten Import	Für den manuellen Import:
Ordner mit allen relevanten Daten	Root / data Ordner	Datenbank Ordner mit lightspeed- <ID>.db
-	(optional) externer Media Ordner	(optional) externer Media Ordner

Daten sollten im folgenden Format vorliegen (**nur für vereinfachten Datenimport relevant**):

```

└─ 37C2DD9E-6326-4E24-81F5-7CED0310B801
   └─ 100052831449889
      └─ Library
         └─ lightspeed-100052831449889.db
            └─ lightspeed-FNFRRangeCache
               └─ lightspeed-imageCache
                  └─ lightspeed-sessionless.db
                     └─ SharedAppGroupLogs


```

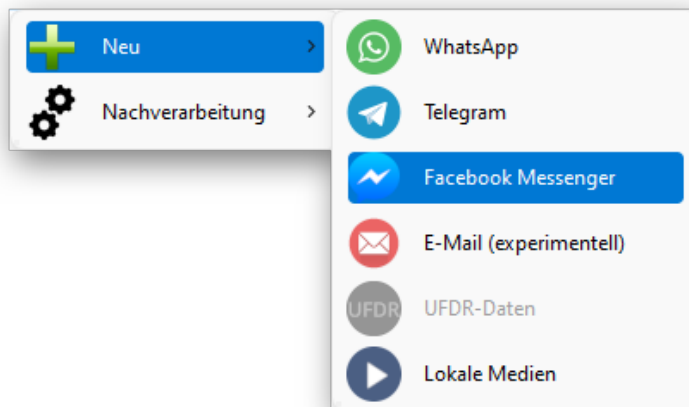
Wenn die Daten dem entsprechend vorliegen kann mit dem Import begonnen werden.


Achtung

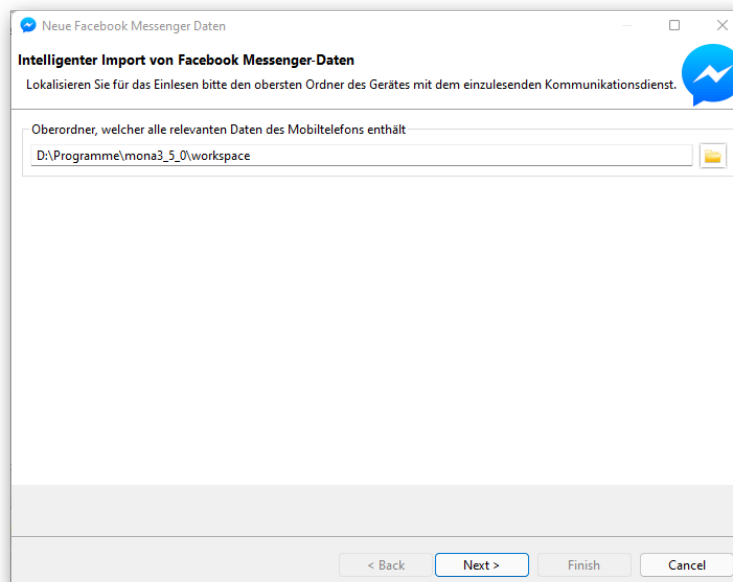
Ist die gegebene Ordnerstruktur nicht gegeben muss anstatt Schritt 5, Schritt 6 befolgt werden.


Prozedur

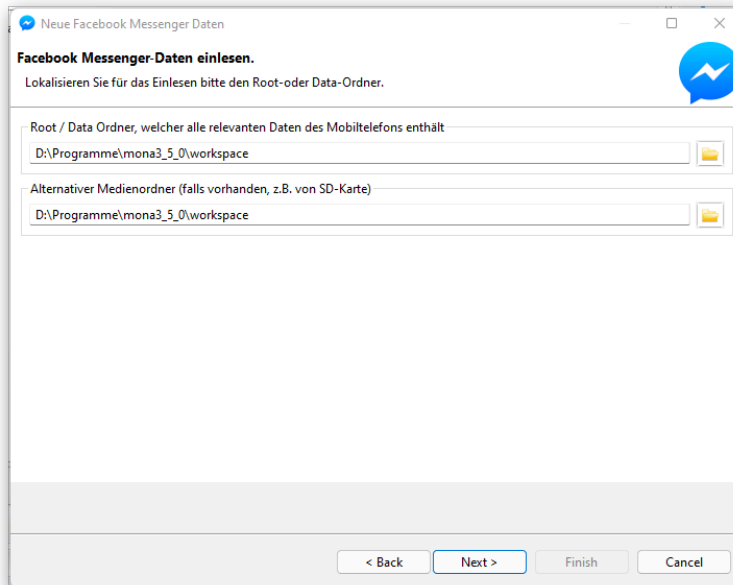
1. Navigationsbereich anwählen. 
2. Das zuvor angelegte und dem Chat zugehörigen Mobile Endgerät anwählen.
3. Rechtsklick -> Neu -> Facebook Messenger



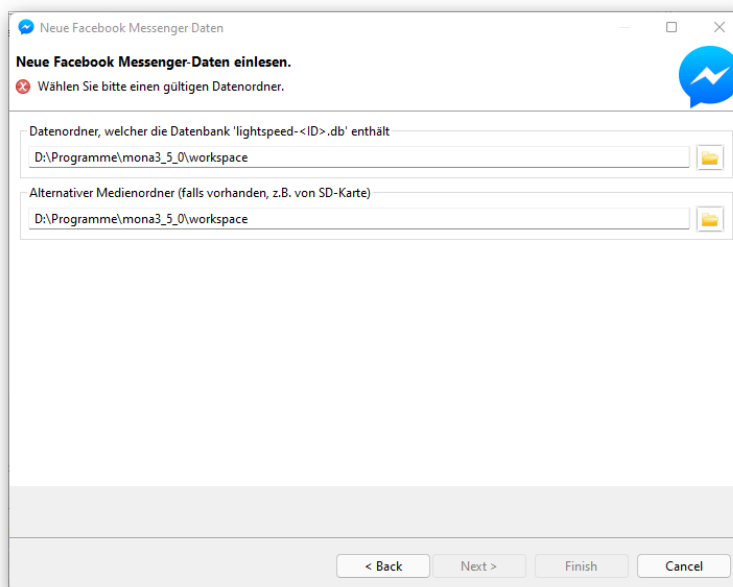
4. Für den intelligenten Import: Ordner mit allen relevanten Daten auswählen.  -> Datei auswählen -> Öffnen.



5. Für den vereinfachte Import: Im ersten Feld den Root/ data Ordner und (optional) externer Medien Order auswählen.  -> Datei auswählen -> Öffnen.



6. Bei nicht erfolgreichen Import durch den vereinfachten Import kann der manuellen Import durchgeführt werden. Next -> Datenbank Ordner auswählen -> (optional) externer Medien Order auswählen. Datenbank Ordner muss lightspeed-<ID>.db enthalten (siehe [Struktur oben](#)).



7. Next > betätigen.
 8. Vorverarbeitung wählen, siehe [Operationen zur Nachverarbeitung](#)
 9. Finish betätigen.

2.3.8. Operationen zur Nachverarbeitung

Bereits beim Importprozess ermöglicht MoNA die Vorbereitung der Daten für eine spätere Analyse. Dies ermöglicht dem Ermittler schneller in die Analyse zu starten. Gerade bei größeren Datensätzen ist diese Option besonders sinnvoll so kann die möglicherweise lange Import und Nachverarbeitungszeit kombiniert werden und danach direkt in die Auswertung gestartet werden.

Auszug der Nachverarbeitungsschritte nach einem WhatsApp Import. Folgende Optionen sind universell und für alle Datenimporte gleich.

Neue WhatsApp Daten

Operationen zur Nachverarbeitung

Bitte wählen Sie Operationen, die nach dem Einlesen der Daten ausgeführt werden sollen.

Detektion

- ☒ Konversationsdetektion
- ☐ Sprachenerkennung
- ☐ Chats zusammenführen
- ☐ Semantische Analyse
- ☐ Extraktion von Videoframes
- ☐ Themenextraktion
- ☐ Markierung von Chatnachrichten (z.B. Hassrede)
- ☐ Generierung von Nutzerprofilen

Begriffsbaum

- ☐ Existierenden Begriffsbaum anwenden

Speichern

- ☐ Speichere alle Änderungen nach Nachverarbeitung

Ergebnisberichte

- ☐ Zeige Bericht über den Datenimport und die Nachverarbeitung an

< Back Next > Finish Cancel

Folgende Nachverarbeitungsoptionen bietet MoNA an.

Optionen	Erläuterung
Konversationsdetektion	Gruppieren des Chatverlaufs zu Gesprächen.
Sprachenerkennung	Erkennt verwendete Hauptsprache im Chat.
Chats zusammenführen	Chats, welche auf mehrer Geräte verteilt sind, werden verknüpft. <i>Option ist ausgegraut, wenn bisher kein weiteres Gerät eingelesen wurde.</i>
Semantische Analyse	Generiert für Bilder, Videos und Audiodateien eine textuelle Beschreibung.
Extraktion von Videoframes	Extrahiert Einzelbilder aus Videodateien.
Themenextraktion	Erzeugt Repräsentation der in den Chats diskutierten Hauptgedanken.
Markierung von Chatnachrichten (z.B. Hassrede)	Markierung von Chatnachrichten mit Hilfe von KI-Modellen.
Generierung von Nutzerprofilen	Berechnung von Interaktionsprofilen für Chatteilnehmer.
Existierenden Begriffsbaum anwenden	Auswahl eines bestehenden Begriffsbaums und Anwendung auf den einzulesenden Datensatz.
Speicher alle Änderungen nach Nachverarbeitung	Übernimmt alle Nachverarbeitungsschritte persistent und übernimmt sie in Log Datei.

Optionen	Erläuterung
Zeige Bericht über den Datenimport und die Nachverarbeitung an	Die im Hintergrund erstellten Log-Einträge werden ausgegeben.

1. Die gewünschten Optionen können durch anklicken der Häkchenboxen ausgewählt werden.
2. Mit **Next** > bestätigen

Direktaufruf

Empfohlene Optionen sind bereits ausgewählt und können übernommen werden.

2.4. Analyse

MoNA bietet die Möglichkeit die importierten Chats interaktiv zu analysieren. Hierfür Nutzt MoNA moderne Methoden aus dem Text Mining, ein interdisziplinäres Feld, welches sich Methoden aus Informationsrückgewinnung, Verarbeitung natürlicher Sprache, Statistik, maschinellen Lernverfahren, Mustererkennung, Datenbanktechnologien, Netzwerkforschung, wissensbasierten Systemen, künstlichen Intelligenz, High-Performance-Computing und Datenvisualisierung nutzbar macht, um große Mengen von Texten zu strukturieren, mit dem Ziel Muster und Trends zu erkennen, welche die Entwicklung und Vorhersage von Straftaten ermöglichen (Predictive Policing) sowie inkriminierte Texte zu finden und daraus Informationen zu extrahieren, welche zur vollständigen Aufklärung aller Tatumstände einer Straftat beitragen.

2.4.1. Chat Nachbearbeitung

Wurde die Nachverarbeitung nicht bereits beim **Import** durchgeführt kann diese nachträglich angewandt werden. Nachträglich können die folgenden Optionen durchgeführt werden.

2.4.1.1. Chats zusammenführen

Um die Arbeit mit mehreren Mobilten Endgeräten zu erleichtern, können Chats von mehreren Geräten zusammengeführt werden.

Warum und wann dieser Vorgang ausgeführt wird


Wenn über die beiden Geräte miteinander kommuniziert wurde, werden Nachrichten nicht doppelt angezeigt.

Für die Zusammenführung gelten folgende **Voraussetzungen**:

Es müssen mehrere Mobilendgeräte (*min* 2) mit Chats aus dem selben Messenger importiert werden.

Wenn die Chats vorliegen, kann wie folgt vorgegangen werden:

Prozedur

1. **Navigationsbereich** anwählen 
2. Rechtsklick auf einen der beiden (*zufällig*) Chats.
3. Nachbereitung -> Chats zusammenführen

Nach der Zusammenführung können zusammengeführte Chats an folgendem Symbol erkannt werden.

Nachrichten die nur auf einem Gerät vorliegen werden mit folgendem Symbol gekennzeichnet.

2.4.1.2. Semantische Analyse

Die Semantische Analyse ermöglicht es die im Chat verwendeten Medien in Text umzuwandeln. Hierdurch ist es möglich die [Globale Suche](#) und den Termbaum auch auf diese Medien anzuwenden.

Prozedur

1. Chat auswählen
2. Rechtsklick -> Nachbearbeitung -> Semantische Analyse
3. (optional) Mediendatei in Nachrichtentabelle oder Chat interne Medien auswählen
4. (optional) Rechtsklick -> Ergebnisse der semantischen Analyse anzeigen

Rechenzeit kann entsprechend der Menge der Medien im Chat sehr lange dauern.

2.4.1.3. Sprache detektieren

Befinden sich in der Nachrichtentabelle Einträge mit einer unbekannten Sprache oder der Ermittler ist sich nicht sicher mit seiner Vermutung kann diese Funktion es dem Ermittler ermöglichen unbekannte Sprachen schnell zu klassifizieren. Zusätzlich kann mit dieser Information der [Begriffsbaum automatisch an die verwendete Sprache angepasst werden](#).

Prozedur

1. Chat im Navigationsbereich auswählen.
2. Rechtsklick -> Sprache detektieren
3. Info schließen

Ergebnis kann in den Chatdetails gefunden werden.

2.4.1.4. Offensive Speech

Diese Funktion ermöglicht es in der aktuellen Version Hassrede in Deutsch und Englischer Sprache automatisch als verdächtig zu markieren. Hierdurch ist eine zeiteffiziente Arbeit für die schnelle Identifizierung potentiell strafbarer Inhalte möglich. Nur unter der Voraussetzung der vorherigen [Einrichtung](#) möglich.

Prozedur

1. Chat im Navigationsbereich auswählen.
2. Rechtsklick -> Markiere Nachrichten -> Offensive Speech
3. Info schließen

Als verdächtig markierte Nachrichten können der Nachrichtentabelle entnommen werden. Infos über die markierten Nachrichten sind in den Chatstatistiken zu finden.

2.4.1.5. Videoframes extrahieren

Diese Funktion ermöglicht es alle Einzelbilder aus einem Video zu extrahieren

Prozedur

1. Chat im Navigationsbereich auswählen.
2. Rechtsklick -> Videoframes extrahieren.

Unter laufende Operationen  kann der Status der Extraktion entnommen werden.

3. Das Ergebnis befindet sich in der Medien Galerie.

2.4.1.6. Lokale und globale Nutzerkonten gruppieren

Prozedur

2.4.2. Themenextraktion

2.4.2.1. Themenextraktion

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

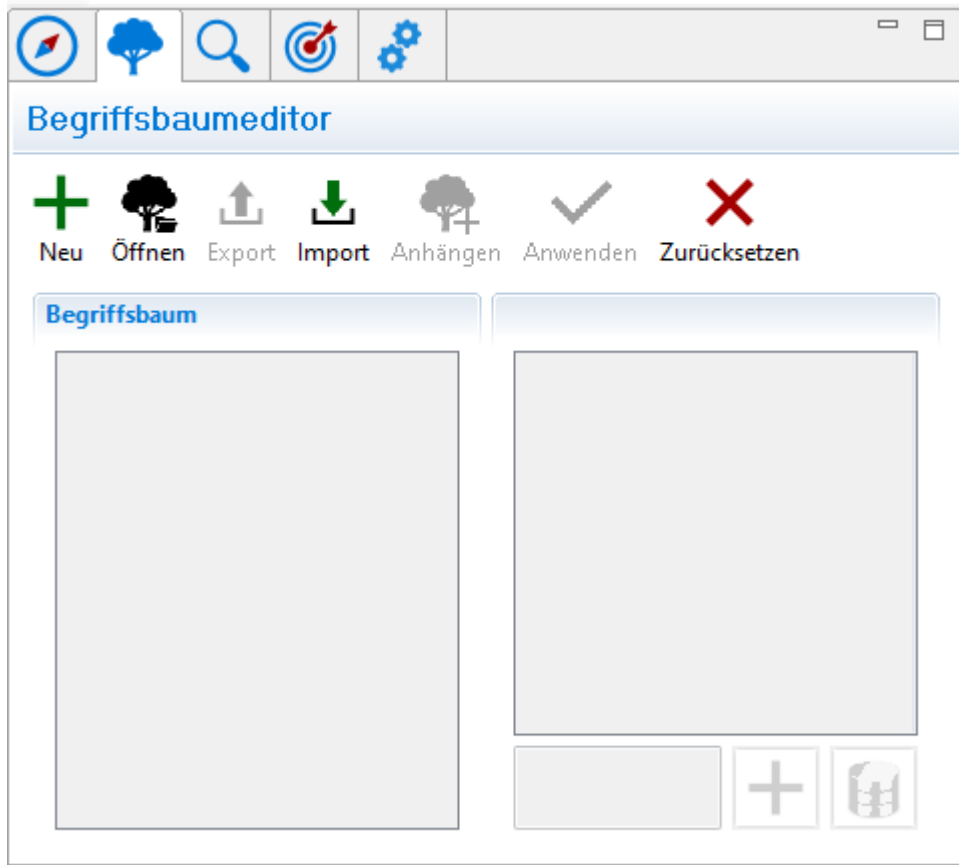
- 1.

2.4.2.2. Extrahiere alle Arten von Themen

Prozedur

2.4.3. Begriffsbaum

Mit dem Begriffsbaum können schnell und einfach verdächtige Nachrichten identifiziert werden. Der Termbaum kann für jeden Fall individuell erstellt oder angepasst werden. Das Herzstück bildet hierbei ein semantisches Wörterbuch in Form eines Begriffsgraphen. Dieser verknüpft einzelne Schlüsselbegriffe und Muster zu komplexen semantischen Ketten. Jeder Begriff wird dabei nicht als einfache Erscheinungsform eines Wortes, sondern als Vektor möglicher Erscheinungsformen inkl. Synonyme und fremdsprachlicher Varianten repräsentiert. Der Termbaum kann manuell oder durch die Themenextraktion gefüllt werden. Bereits bestehende Begriffsbäume können gespeichert und wiederverwendet werden können.



2.4.3.1. Begriffsbaum erstellen

Bei der manuellen Initialisierung des Termbaumes muss jeder Begriff per Hand eingegeben werden, dies ermöglicht eine individuelle und exakte Suche.

Warum und wann dieser Vorgang ausgeführt wird

Für die manuelle Erstellung wird wie folgt vorgegangen:

Prozedur

1. Den Begriffsbaumeditor öffnen 🌳
2. In der Navigationsleiste das grüne Plus anwählen.
3. Name und Sprache wählen.
4. Mit `Finish` bestätigen

2.4.3.2. Begriffsbaum manuell initialisieren

Bei der manuellen Initialisierung des Termbaumes muss jeder Begriff per Hand eingegeben werden, dies ermöglicht eine individuelle und exakte Suche.

Warum und wann dieser Vorgang ausgeführt wird

Für die manuelle Erstellung wird wie folgt vorgegangen:

Prozedur

1. Den Begriffsbaumeditor öffnen 🌳
2. In der Navigationsleiste den Baum auswählen.

3. Mit dem Grünen Plus einen Begriff hinzufügen.
4. So viele Begriffe einfügen wie nötig.

2.4.3.3. Begriffsbaum Erstellung mit Themenextraktion

Die automatische Erstellung des Termbaums durch die Themenextraktion ermöglicht es schnell und einfach inhaltlich verwandte Begriffe zu finden.

Prozedur

1. Begriffsbaumeditor öffnen 
2. Rechtsklick in den Begriffsbaum (weiße Fläche) # Empfehlungen berechnen für Begriffsbaum (ohne Kontext)
3. [Kantenextraktion Optionen auswählen](#)
4. Thema auswählen
5. Begriffe auswählen durch Hakensetzung
6. Mit Finish bestätigen

2.4.3.4. Themenextraktion Optionen


2.4.3.5. Synonyme und Übersetzungen automatisch finden.

Diese Funktion ermöglicht es dem Nutzer schnell Synonyme in 7 Sprachen zum Begriffsbaum hinzuzufügen.

Warum und wann dieser Vorgang ausgeführt wird

Vorgehensweise:

Prozedur

1. Begriffsbaumeditor öffnen 
2. Begriff aus Begriffsbaum auswählen
3. Im Bereich "[Wortvektor](#)" Das Datenbank Symbol anwählen
4. gewünschte Sprache(n) auswählen # Next
5. Die gewünschten Begriffe einzelnen durch Hakensetzung auswählen, Alle Begriffe einer Sprache Auswählen durch Haken vor der Sprache oder Alle auswählen anwählen
6. mit Finish bestätigen


2.4.3.6. Begriffsbaum exportieren

Begriffsbäume können für erneute Verwendung exportiert werden. Diese werden im xml Format gespeichert

Warum und wann dieser Vorgang ausgeführt wird

Vorgehensweise:

Prozedur

1. Begriffsbaumeditor öffnen 
2. Export anwählen
3. Speicherort und Name wählen
4. Speichern betätigen


2.4.3.7. Begriffsbaum importieren

Zuvor exportierte Begriffsbäume können wieder importiert werden.

Warum und wann dieser Vorgang ausgeführt wird

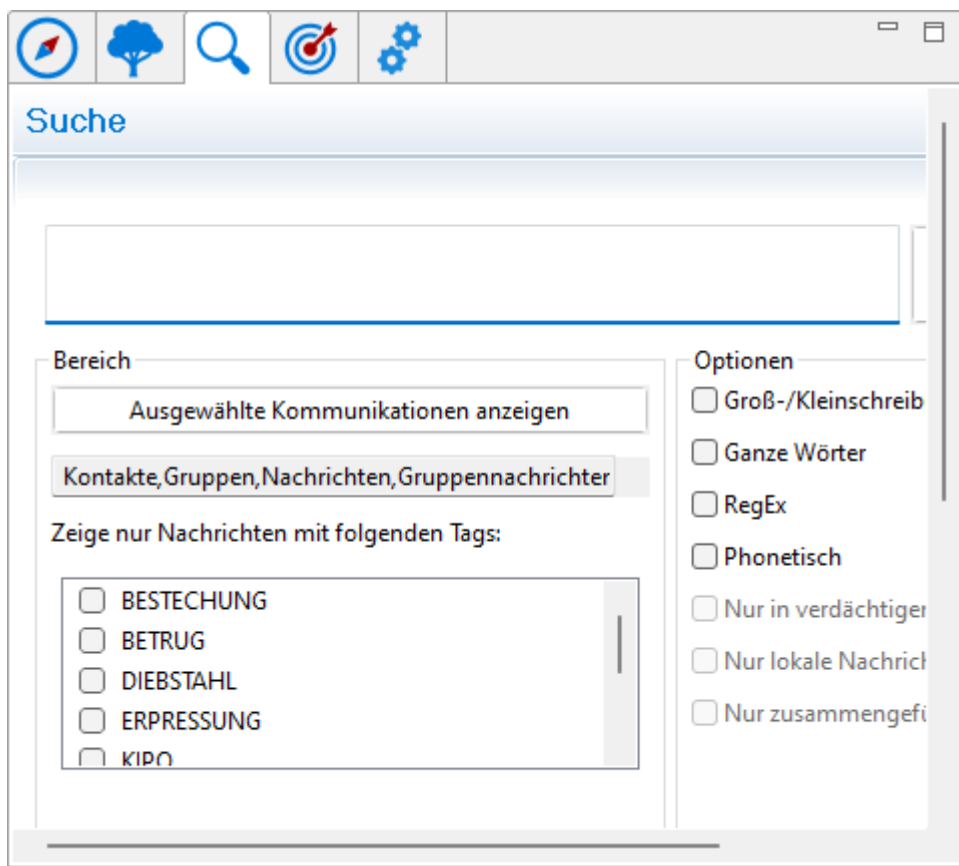
Vorgehensweise:

Prozedur

1. Begriffsbaumeditor öffnen 
2. Import anwählen
3. gewünschte Datei lokalisieren und anwählen
4. Öffnen betätigen

2.4.4. Suche

Die Suchfunktion ermöglicht es dem Ermittler alle Nachrichten und Medien nach bestimmten Begriffen zu durchsuchen. Außerdem können durch Tags Suchergebnisse nach bestimmten Tatbeständen gefiltert werden und auf eine Zeitspanne begrenzt werden.




2.4.4.1. Termsuche

Mit der Termsuche lässt sich einfach in der ganzen Untersuchung nach einem Term/Begriff gesucht werden.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Im Navigationsbereich die Lupe  auswählen
2. Zu suchenden Term eingeben (hierbei werden von MoNA Vorschläge mit vorhandenen Begriffen gemacht)
3. [Suchoptionen](#) wählen
4. (optional) gewünschte Tags durch anklicken der Box auswählen.

5. Suchen betätigen.

2.4.4.2. Suchoptionen

Mit den Suchoptionen wird dem Ermittler ermöglicht seine Suche an bestimmte Gegebenheiten anzupassen, um fallrelevante Informationen schneller zu finden.

MoNA bietet folgende Suchoptionen:

Suchoptionen	Funktionen (Reihenfolge entspricht Layout)
Groß-/Keinschreibung beachten	Standardmäßig beachtet MoNA bei der globalen Suche keine Groß- und Kleinschreibung
Ganze Wörter	Nur Ergebnisse in welchen der gesuchte Term vollständig vorkommt.
RegEx	Sucht nach zuvor ausgewählten Regulären Ausdrücken (deaktiviert alle anderen Funktionen)
Phonetisch	Auch Ergebnisse anzeigen, welche phonetisch (der Aussprache ähnelnd) dem Suchterm entsprechen.
Nur in verdächtigen Objekten	Nur in zuvor als verdächtig markierten Nachrichten suchen. Link auf Verdächtig nicht vergessen (Ausgegraut wenn es keine verdächtigen Nachrichten gibt)
Nur lokale Nachrichten vom Gerät	Sucht bei zusammengeführten Chats nur in den lokalen Nachrichten des ausgewählten Geräts. (Ausgegraut wenn keine Chats zusammengeführt wurden)
Nur zusammengeführte Nachrichten	Sucht bei zusammengeführten Chats nur in den zusammengeführten Nachrichten des ausgewählten Chats. (Ausgegraut wenn keine Chats zusammengeführt wurden)




2.4.4.3. Tags

Mit Tags können Nachrichten bestimmten Kategorien zugeordnet werden. Durch die Auswahl der Tags bei der Suche können die Suchergebnisse auf diese Kategorie eingeschränkt werden. Wie man Nachrichten bestimmten Tags zuordnen finden sie hier. **Link einfügen** MoNA bietet standard mäßig diese Tags an, welchen deutschen Straftatbeständen entsprechen.

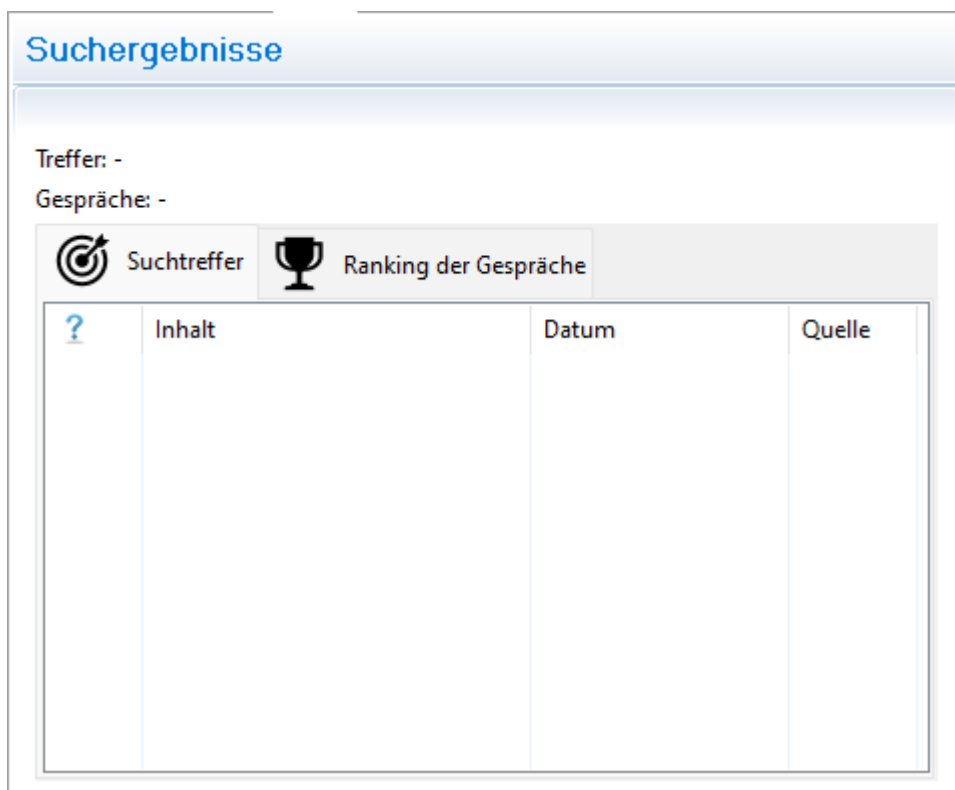
- Bestechung
- Betrug
- Diebstahl
- Erpressung
- KiPo
- Linksextremismus
- Rechtsextremismus
- Nötigung

Die Liste der Tags kann wie folgt bearbeitet werden:

1. Fenster in der oberen Navigationsleiste anwählen.
2. Einstellung anklicken Screenshot einfügen

3. Tags anklicken.
4. Um einen Tag hinzuzufügen: Name des neuen Tags in das Feld neben das  einfügen und das  anklicken.
5. Um einen Tag zu löschen Tag in der Liste auswählen und mit dem  löschen.

2.4.4.4. Suchergebnisse verstehen



MoNA führt nach der Suche ein automatisches Ranking der Suchergebnisse durch. Diese ist unter Ranking der Gespräche zu finden



2.4.5. Zeitdiagramm

Durch das Zeitdiagramm lässt sich der Chat auf einer Zeitachse betrachten. Die X-Achse stellt hierbei die Zeit und die Y-Achse die Anzahl der Nachrichten dar. Dies bietet z.B. die Möglichkeit, die Chat Frequenz mit bestimmten Tatrelevanten Ereignissen zu vergleichen.

2.4.5.1. Zeitdiagramm öffnen

Durch das Zeitdiagramm lässt sich der Chat auf einer Zeitachse betrachten. Dies bietet z.B. die Möglichkeit, die Chat Frequenz mit bestimmten Tatrelevanten Ereignissen zu vergleichen.

Prozedur

1. Zeitdiagramm öffnen 
2. Chat im Navigationsbereich  auswählen
3. Das Zeitdiagramm kann jetzt mit anderen Zeitdiagrammen verglichen werden.

2.4.5.2. Zeitdiagramm bearbeiten

Zeitdiagramme können durch verschiedene Optionen graphisch aufgearbeitet werden.

Mona bietet dabei folgende Optionen:

- Grafik Einstellungen

Graph: Screenshot

1.

2.

Axes: Screenshot

1.

2.

Traces: Screenshot

1.

2.

- Legende Ein/Ausblenden
- Annotationen hinzufügen/löschen
- Autoskalierung
- Dynamischer/Rubberband Zoom
- Vertical/Horizontal Zoom
- Zoom In/out
- Verschieben
- Letzte Operation Rückgängig machen und Wiederherstellen

2.4.5.3. Zeitdiagramm filtern

Durch die Funktion Einstellungen und Filter lässt sich der Chat, welcher visualisiert werden soll auswählen, sowie die Einheit der Zeit in welcher die Grafik aufgelöst werden soll.

1.

2.

2.4.5.4. Zeitdiagramm exportieren

Zeitdiagramm zur weiteren Verwendung (z.B. Drucken) exportieren.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. gewünschtes [Zeitdiagramm öffnen](#)
2. Kamera Symbol anwählen
3. Speicherort wählen

4. Speichern betätigen

2.4.6. Nutzerprofile

MoNA extrahiert automatisch, falls bei der Nachverarbeitung ausgewählt, aus den Chats Nutzerprofile. Über diese Nutzerprofile werden Statistiken erstellt.

Folgende Statistiken werden erstellt:

2.4.6.1. Nutzerprofile verknüpfen

Prozedur

2.4.6.2. Nutzerprofile vergleichen

Prozedur

2.4.7. Netzwerkstatistiken

2.4.8. Netzwerkdetails

2.4.8.1. Netzwerkdetail Sortierung Suche

- 1.

Prozedur

1. Irrelevante Nachricht in der Nachrichtentabelle identifizieren
2. Rechtsklick -> als irrelevant markieren

2.4.9.2. Übersetzung

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

- 1.

2.4.10. Medien

2.4.10.1. Medieninformationen anzeigen

Informationen zu Mediendateien wie Speicherort, EXIF-Informationen, usw. können von MoNA angezeigt werden.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Mediendatei auswählen
2. Rechtsklick ->?

2.4.10.2. Medien gegen Hashdatenbank prüfen

Medien aus dem Chat als Vergleichsobjekt genommen werden

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Dieses Verfahren kann je nach Größe der Chats mehrere Minuten dauern.

2.4.10.3. Medien gegen Hashdatenbank und Treffer auf Ähnlichkeit überprüfen

Der Vergleich von Hashwerten von Mediendateien ermöglicht es dem Ermittler in kürzester Zeit illegale oder verdächtige Inhalte zu identifizieren, ohne die Datei betrachten zu müssen.

Warum und wann dieser Vorgang ausgeführt wird

Hierfür können entweder Hashwerte wie folgt importiert werden.

Prozedur

1. Dieses Verfahren kann je nach Größe der Chats mehrere Minuten dauern.

2.4.10.4. Bilder auf Ähnlichkeit überprüfen

Prozedur

2.4.11. Auswertung

2.4.11.1. Report erstellen

Für die Aktenarbeit ermöglicht MoNA den Export in verschiedenen Formaten.

Prozedur

1. Chat im Navigationsbereich auswählen.
2. Rechtsklick -> Reports -> Bericht erstellen.
3. [Bericht optionen angeben](#).
4. Erzeugen bestätigen.

2.4.11.2. Berichtsoptionen

3. Troubleshooting

Im Nachfolgenden werden alle bekannten Probleme und ihre Ursachen erläutert. MoNA befindet sich noch in der Entwicklung, daher bitten wir um Ihr Verständnis. Das Importverfahren ist noch nicht einheitlich optimiert und kann daher wiederholt zu Problemen führen. Außerdem ist die Analyse von großen Daten mit Hilfe von KI ein sehr rechenintensiver Prozess und kann daher bei leistungsschwächeren Systemen zu Problemen führen.

Falls es für ihr Problem keine Lösung gibt [melden Sie es bitte per E-Mail](#).

3.1. Ungültige Lizenz

Für die Verwendung von MoNA wird eine gültige Lizenz vorausgesetzt. Lizenzdateien können zeitlich begrenzt sein und auf Geräte beschränkt sein.

Ursache:

- Lizenz wurde für ein anderes Gerät erstellt.
- Lizenz wurde mehrmals verwendet (wenn es sich um eine SINGLE Lizenz handelt).

- Lizenz ist abgelaufen.

Lösungen:

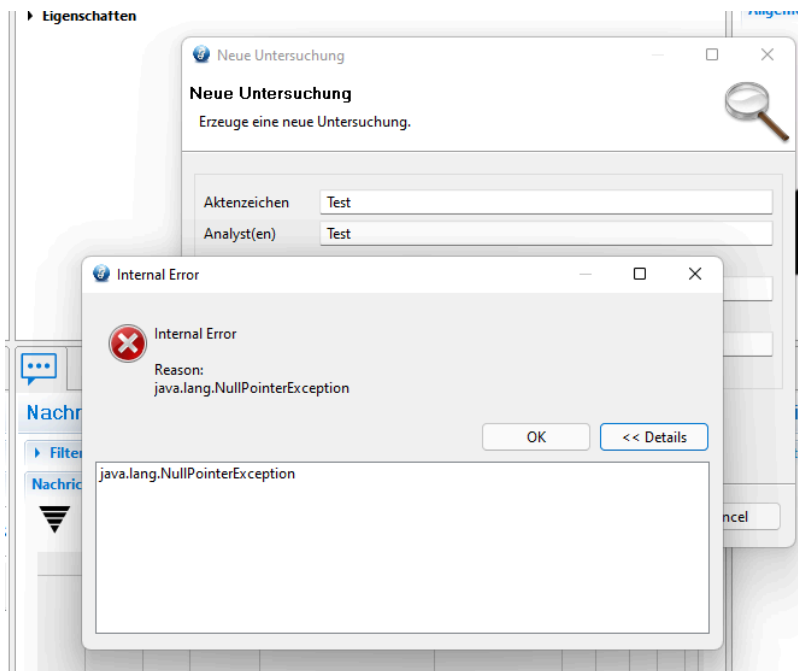
- MoNA auf Gerät verwenden für das die Lizenz erstellt wurde.
- .emfstore löschen
- Neue Lizenz ausstellen lassen

Bemerkung

Neue Lizenzen können unter siewerts@hs-mittweida.de beantragt werden.

3.2. Anlegen der Untersuchung

Folgende Fehlermeldung weist auf Probleme bei Schreib- und Leseberechtigungen hin. **Internal Error**
Reason: java.lang.NullPointerException



Ursache:

- MoNA wurde auf einem Laufwerk mit rechtlichen Beschränkungen installiert.
- MoNA wurde auf einem Netzlaufwerk installiert.
- MoNA wurde in einem Ordner, welcher vom Betriebssystem bereitgestellt wurde, installiert.
- MoNA wurde auf der Betriebssystem Partition (meistens C:) installiert.
- Der Installationspfad enthält ein Leerzeichen oder Sonderzeichen.
- MoNA wurde bei aktiviertem Windows Defender nicht zu den Ausnahmen hinzugefügt.

Lösungen:

1. Verzeichnis verschieben
2. .emfstore Ordner in mona_3_5_1/workspace löschen

3. Neustart

3.3. Keine Rückmeldung/Lange Ladedauer

Beim Einleseprozess kann es je nach Importdateien und Hostsystem zu längeren Ladedauern kommen.

Ursache:

- Host System entspricht nicht Mindestanforderungen.
- Sehr großer Dateiiimport (100GB+).

Lösungen:

- Auf leistungstärkeres System wechseln
- [Fehlende Windows Defender Ausnahme](#)
- Bei UFED Import Daten in Cellebrite vorselektieren, um eine kleinere Reportdatei zu erzeugen. Z.b. Abwahl von MoNA nicht unterstützten Diensten wie Signal.

Bemerkung

Wenn MoNA über eine längere Zeit nicht reagiert, kann es mit dem Task Manager geschlossen werden. (Strg + Shift + Esc)

3.4. Import

Die Messenger Dienste verändern stetig ihre Datenstrukturen. Kommt es daher beim Import trotz korrekter Daten und unter genauer Befolgung der Anleitung zu einem Fehler beim Import, liegt es wahrscheinlich an einer veränderten Datenstruktur der Chatdateien.

Achtung

Veränderungen der Datenstrukturen fallen vorallem im praktischen Betrieb auf. Hierbei sind wir auf Ihre Mitarbeit angewiesen. [Bitte melden Sie den Fehler!](#)

3.5. Fehlermeldung

Trotz sorgfältiger Überprüfung können uns unbekannte Fehler auftreten. Falls Fehler auftreten bitten wir Sie darum diese zu melden, um diese in der weiteren Entwicklung berücksichtigen zu können. Einige Fehler treten unter unseren Testbedingungen nicht auf, daher sind wir auf Fehlermeldungen aus der praktischen Verwendung von MoNA angewiesen.

Prozedur

1. E-Mail an siewerts@hs-mittweida.de
2. Betreff: MoNA Fehlermeldung
3. Fehlerbeschreibung (Welche Operation wurde gerade ausgeführt?) Beispielsweise: Geräteanzahl, Gerätetyp, ausgewählte Nachverarbeitungsoptionen, Anzahl der Nachrichten/Mediendateien, Größe der Daten, Versionsnummer von MoNA
4. (Optional) Screenshots der Problems anfertigen und anhängen. (Windowstaste + Shift + S)
5. **.log Datei anhängen** `.mona3_5_1/workspace/metadata/.log`

» This PC » Data (D:) » Programme » mona3_5_0 » workspace » .metadata »

6. Senden.