HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssystem

Linux Live Anwendung

In diesem Praktikum schauen wir uns die in der Vorlesung dargestellten Anwendungen am Beispiel von Sumuri PALADIN Edge an. Dazu wollen wir über ein Live-Medium auf eine VM Zugriff nehmen und uns anschauen, was wir mit der Live-Distribution vornehmen können. Anschließend schauen wir uns das gleiche Vorgehen mit einem Kali Live System an und wollen einen kurzen Vergleich zwischen den Tools ziehen. Im Folgenden sollen sich mittels verschiedener Informationen Zugriff auf das Windows System verschaffen.

Inhalte des Praktikums:

- Konfiguration der Bootreihenfolge mittels VBox
- Analyse und Sicherung mittels Sumuri PALADIN Edge
- Analyse mittels Kali Live
- Brechen des Nutzerpasswortes

Vorbereitung

Für die Durchführung des Praktikums benötigen Sie verschiedene Tools, welche Ihnen unter dem folgenden Pfad auf Ihrem Rechner zur Verfügung stehen:

```
R:\CB\Wetterau\Sachbearbeiter_in-Digitale-Forensik\Betriebssysteme\Präsenz\
```

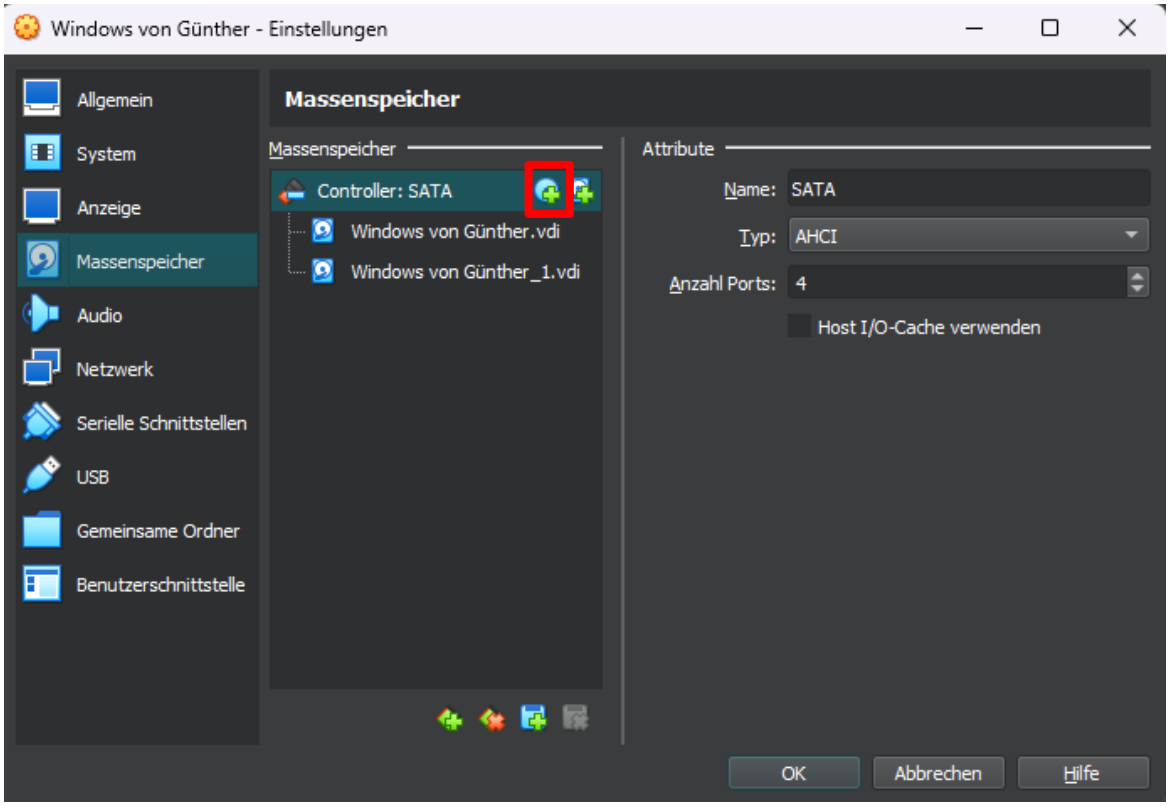
Laden Sie zuerst die Windows-OVA herunter und importieren Sie diese in Virtual Box. Am besten tun Sie dies auf dem Laufwerk D:, da dort der meiste Speicherplatz zur Verfügung steht.

Einbindung der Linux Live ISO-Datei (Am Beispiel von PALADIN)

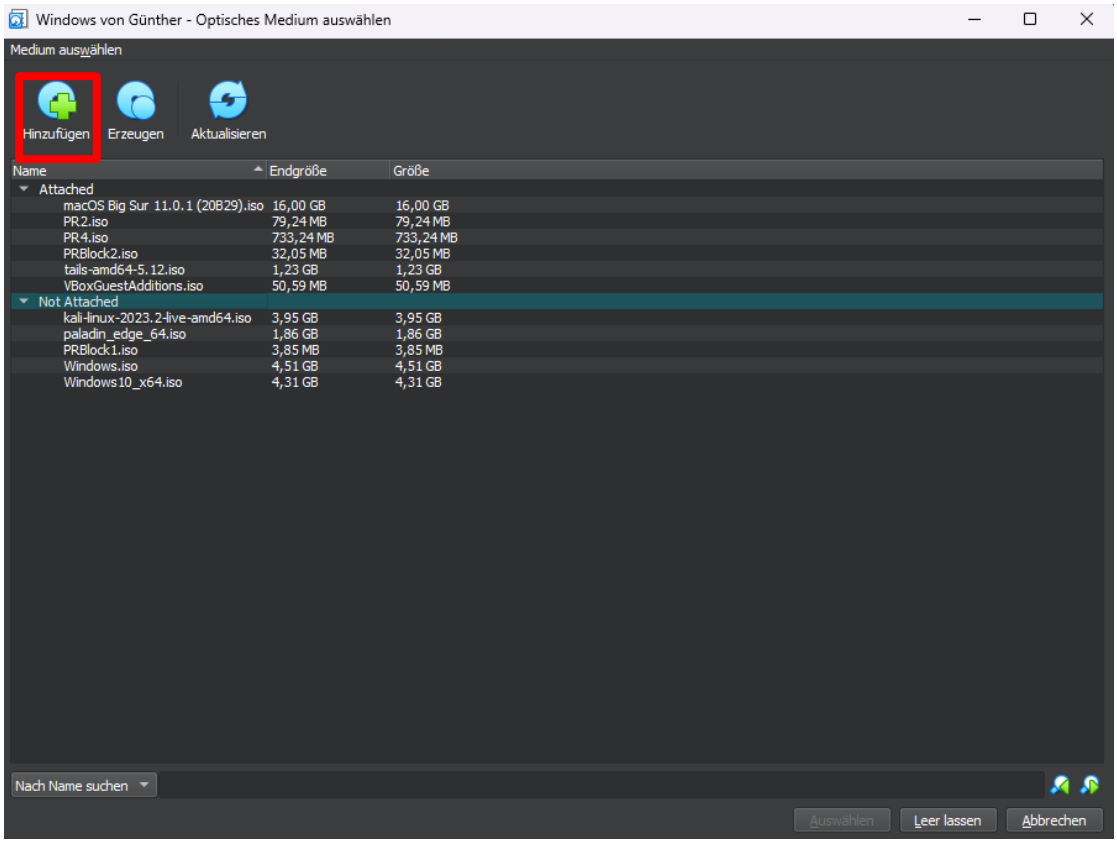
Da wir in einer virtuellen Umgebung arbeiten, müssen wir im ersten Schritt das Einlegen/Einhängen der Live-Distribution simulieren. Laden Sie dafür bitte die ISO-Abbilder der Distributionen, die wir verwenden herunter. Diese finden Sie ebenfalls unter dem Pfad:

```
R:\CB\Wetterau\Sachbearbeiter_in-Digitale-Forensik\Betriebssysteme\Präsenz\
```

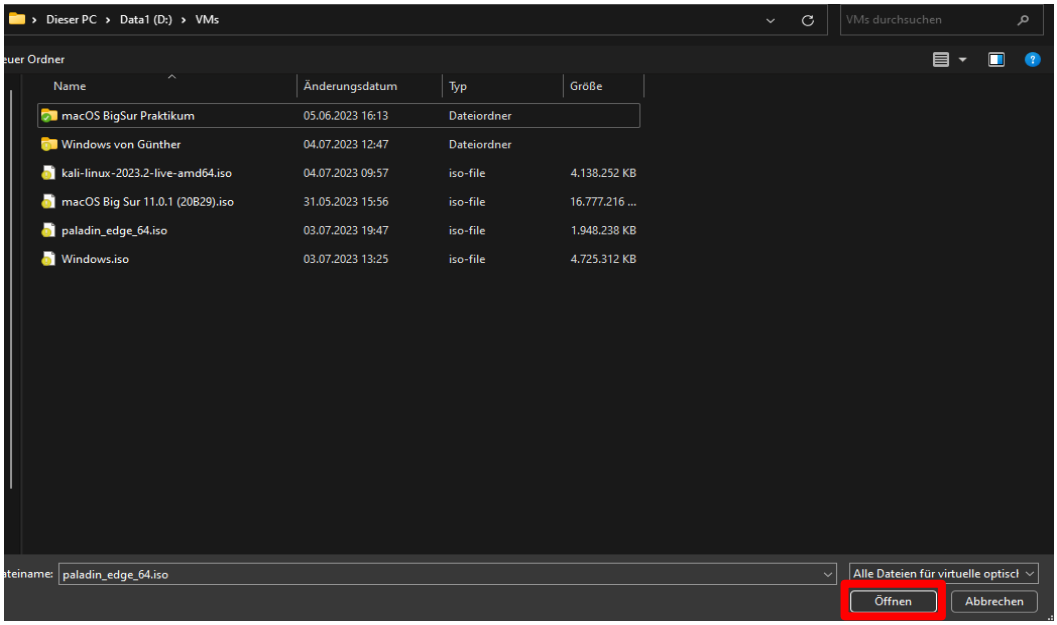
Speichern Sie die ISO-Abbilder ebenfalls auf dem Laufwerk D: oder ein äquivalentes Laufwerk mit ausreichend Speicherplatz. Die ISO-Abbilder werden dann wie aus den Praktika bekannt über **Ändern→Massenspeicher** eingebunden. Klicken Sie bitte auf das CD-Symbol, um die Abbilder hinzuzufügen.



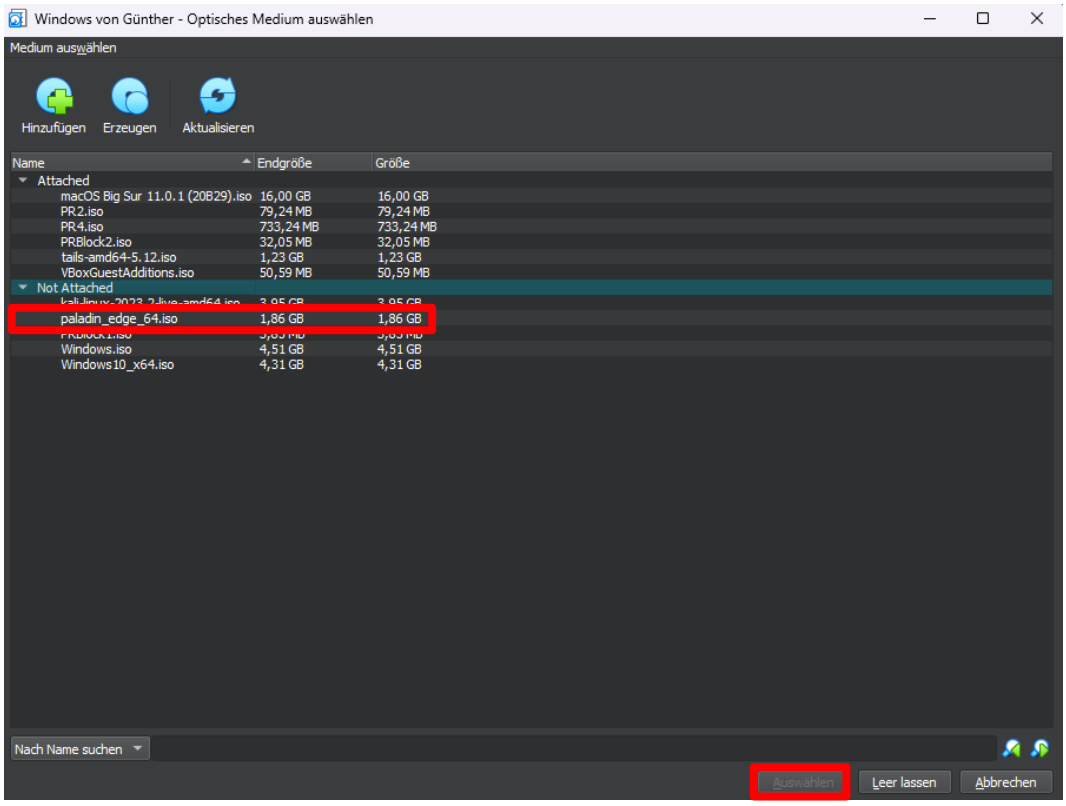
Im nächsten Schritt wählen wir die gewünschte ISO-Datei mit einem Klick auf „Hinzufügen“ aus.



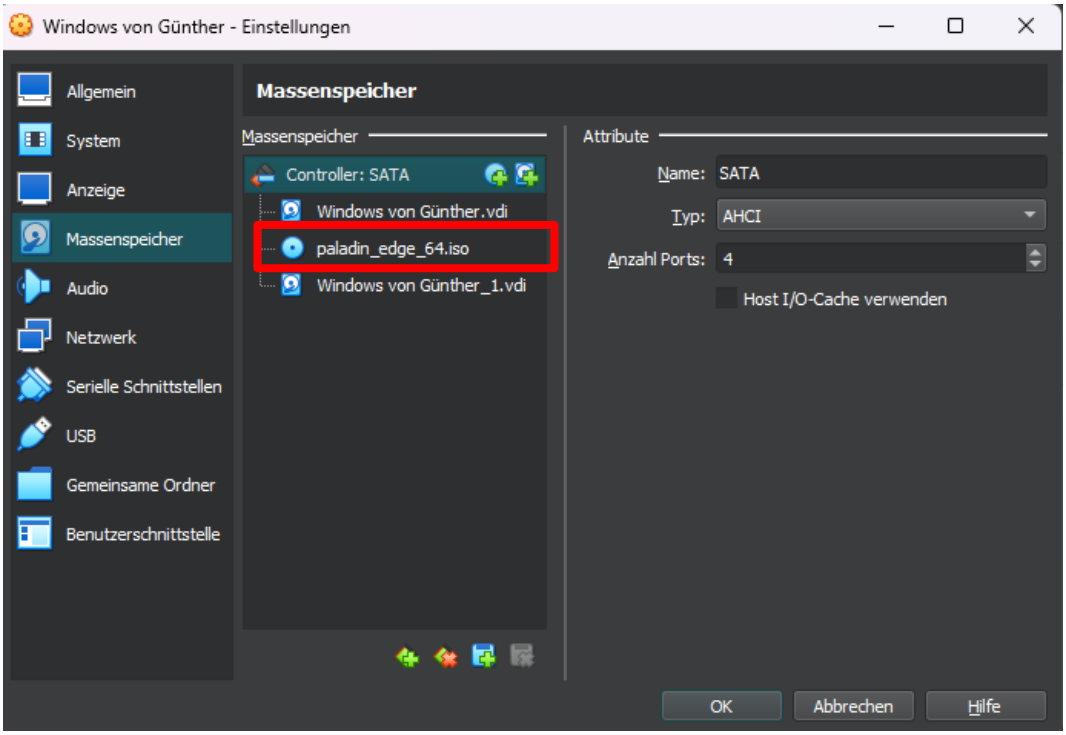
Wählen Sie nun die benötigte ISO-Datei aus und fügen Sie diese über „Öffnen“ ein.



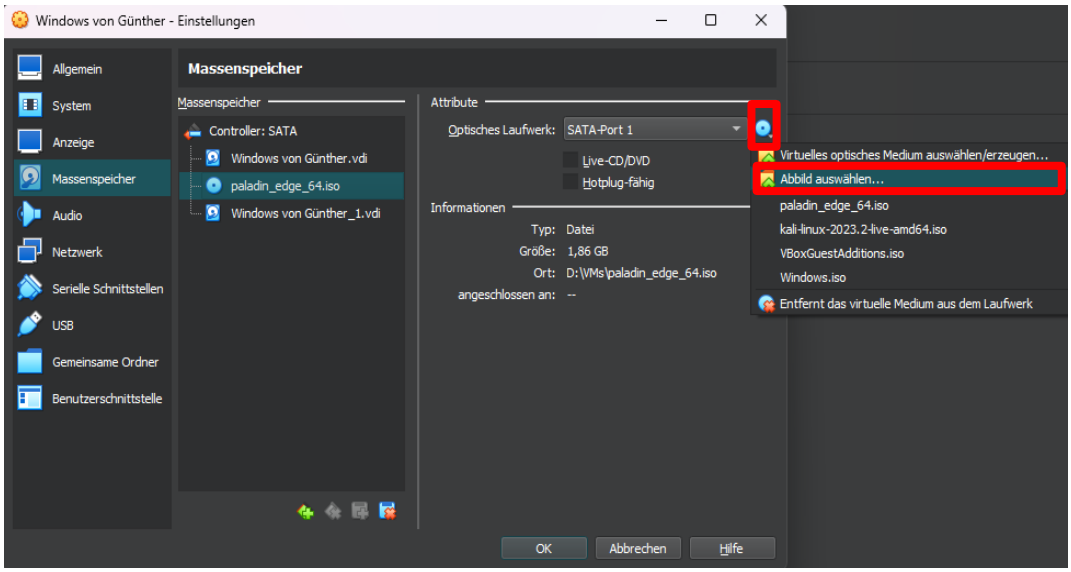
Anschließend wählen wir unter dem Reiter „Not Attached“ mittels eines Doppelklicks die jeweilige ISO-Datei zur Einbindung aus.



Im Menüpunkt „Massenspeicher“ wird die ISO-Datei nun bei erfolgreicher Einbindung angezeigt.



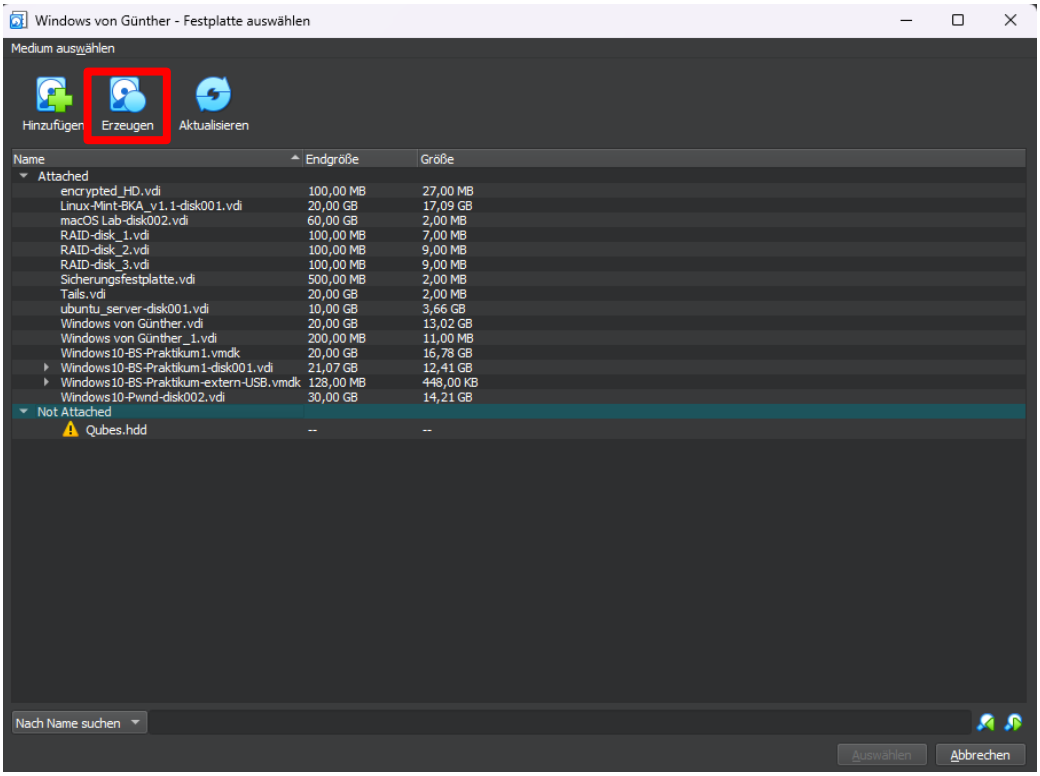
Achten Sie bitte darauf die Abbilder nicht gemeinsam einzubinden, da dies zu Problemen führen kann. Wir benötigen immer nur eine der beiden Distributionen für die Aufgaben. Welche der beiden Distributionen benötigt wird, verrät Ihnen die jeweilige Aufgabe. Im „Massenspeicher"-Menü können Sie über das CD-Symbol bei einem Klick auf die Distribution das neue Abbild auswählen.



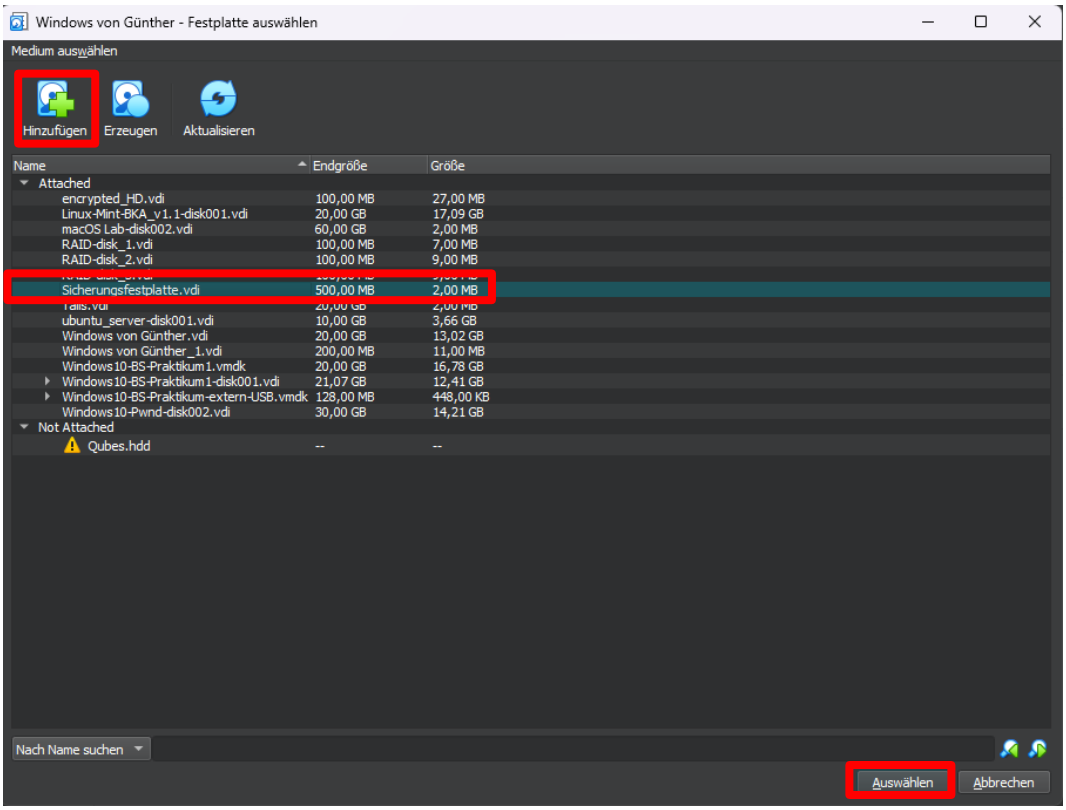
Erzeugung einer Sicherungsfestplatte

Neben dem eigentlichen Medium, von welchem wir die Live-Distribution starten, benötigen wir ein zweites Medium, auf welchem die zu sichernden Daten gespeichert werden können. In diesem Rahmen erzeugen wir nun als letzten Vorbereitungsschritt für das Praktikum eine Sicherungsfestplatte, auf welche wir dann in unserer Live-Distribution zurückgreifen können. Gehen Sie dazu im ersten Schritt erneut auf **Ändern→Massenspeicher.** Dort angekommen, klicken Sie bitte auf das Festplatten-Plus-Symbol, um eine neue Festplatte zu erzeugen.

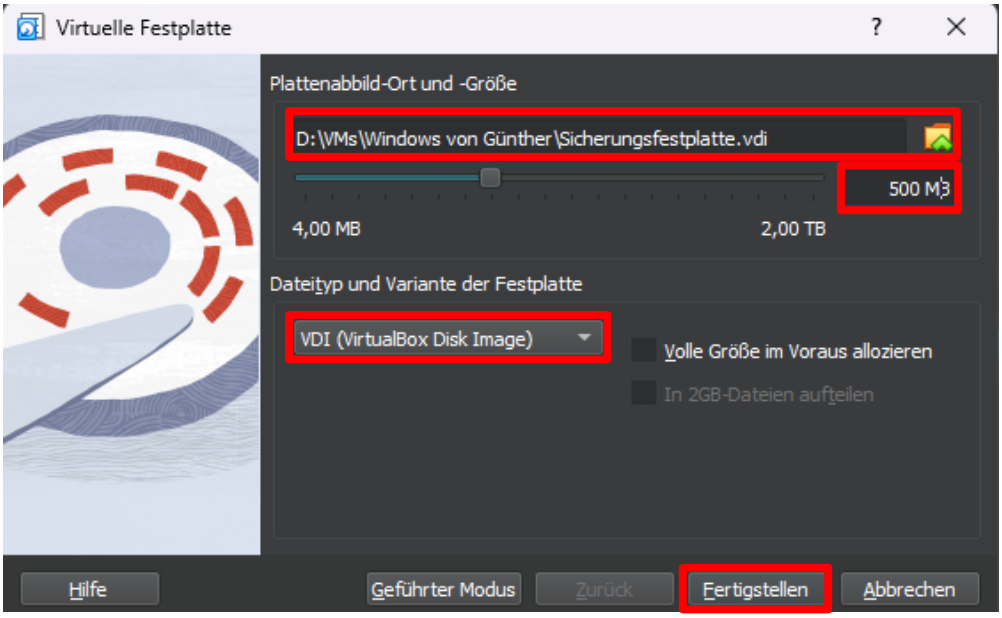
Im Menüpunkt angekommen können Sie über den Punkt „Erzeugen“ eine neue Festplatte erzeugen.



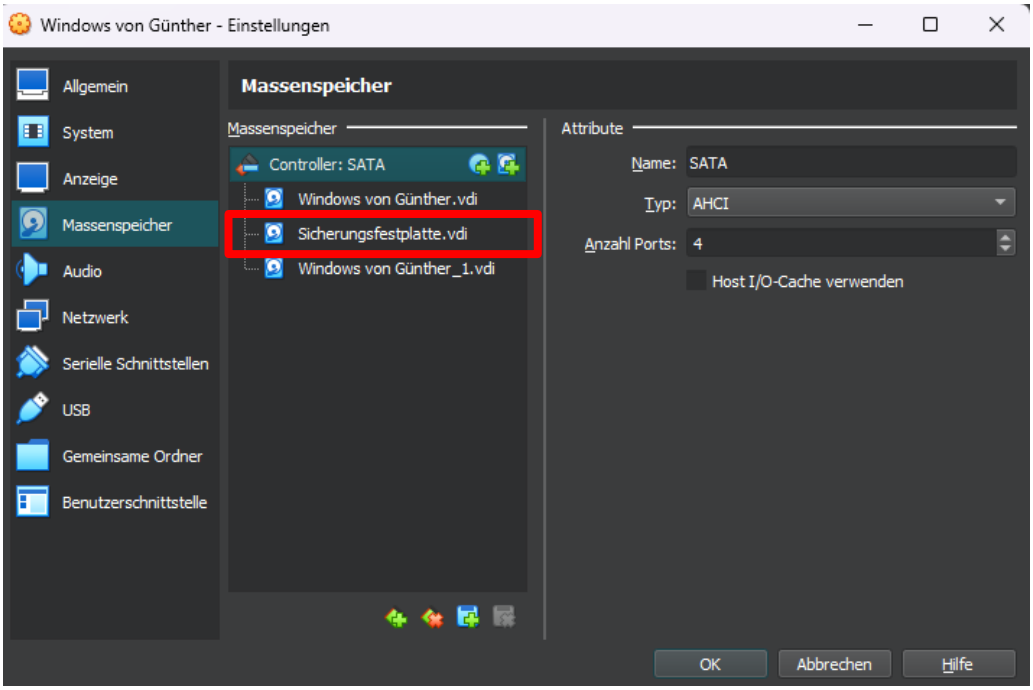
Wir nennen unsere Festplatte „Sicherungsfestplatte“ und speichern diese ebenfalls in D:. Für die Größe wählen wir 500MB. Als Dateitypen wählen wir das VirtualBox Disk Image (VDI). Mit einem Klick auf „Fertigstellen“ erzeugen wir die Festplatte.



Die erzeuge Festplatte taucht nun in der Liste verfügbarer VDI-Dateien auf. Mit einem Doppelklick auf die „Sicherungsfestplatte.vdi“ binden wir diese in die VM ein (Alternativ auf „Auswählen“ klicken).

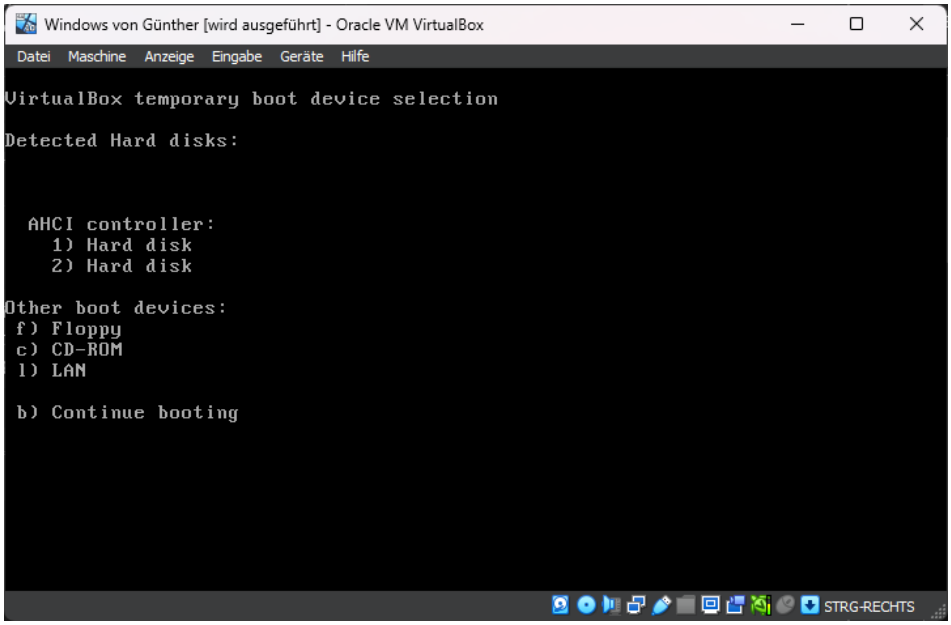


Die VM ist nun fertig vorbereitet! 😊

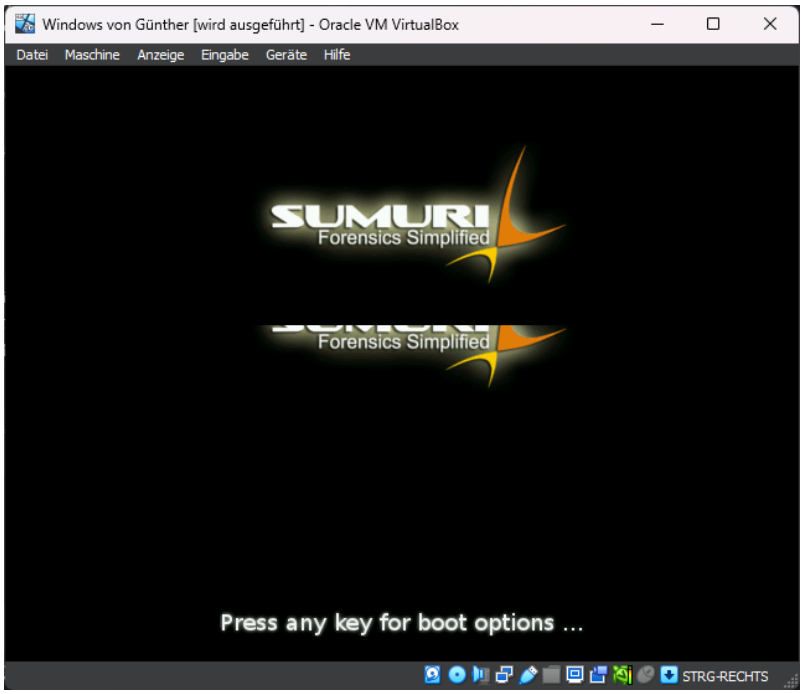


Aufrufen des Bootmenüs unter Virtual Box

Wie es zu jeder Live-Sicherung gehört, muss das entsprechende Live-Bootmedium ausgewählt werden. Dafür haben wir die OVA schon konfiguriert, dass bei Ihnen keine Probleme auftreten sollten. Nachdem Sie die ISO-Datei ausgewählt und ins System eingebunden haben, können Sie die VM auch schon starten. ACHTUNG: Jetzt ist Geschwindigkeit gefragt. Sobald das Fenster mit VM aufploppt, drücken Sie einfach mehrere Male hintereinander F12 im VM-Fenster. Anschließend sollte Sie folgende Ansicht erhalten:



Sie sehen, dass Sie sich aus ein paar Bootoptionen auswählen können. Wir haben die ISO von PALADIN als CD in das System eingebunden und müssen daher auch die Option c) CD-ROM auswählen. Das tun Sie durch das Drücken der Taste C auf ihrer Tastatur. Anschließend sollte direkt der Startbildschirm der Live-Distro erscheinen, welche Sie als ISO eingebunden haben.



Analyse und Sicherung mittels Sumuri PALADIN Edge

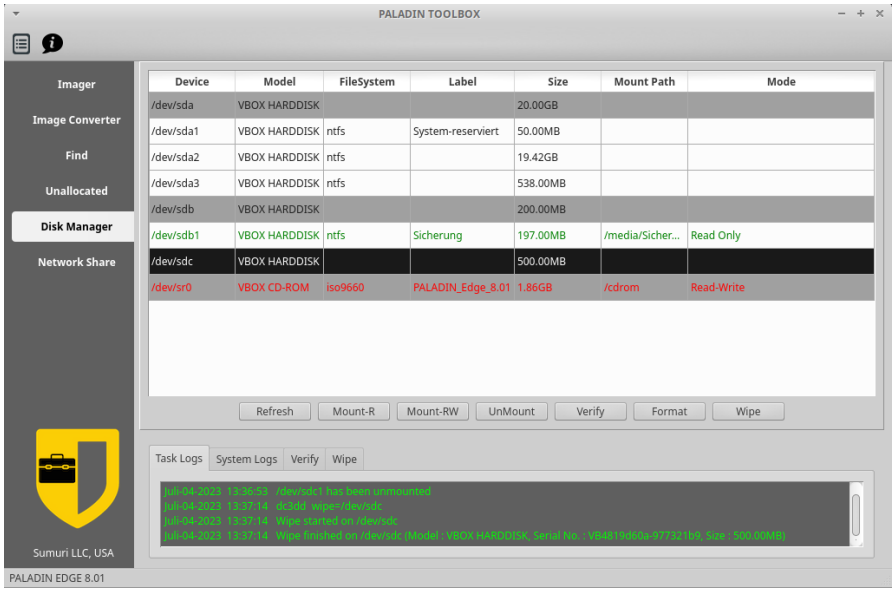
Nachdem Sie das System soweit konfiguriert haben, dass:

1. Die PALADIN ISO am System verfügbar ist und
2. Ihr System den Startbildschirm von Sumuri PALADIN anzeigt

können Sie wie auf dem Bildschirm angezeigt, eine Taste drücken, um Änderungen im Bootmenü vorzunehmen. Mit den Pfeiltasten wählen Sie in dem folgenden Fenster die Sprache aus und bestätigen mit Enter.

Im folgend angezeigten Fenster wählen Sie die bereits hervorgehobene Option „Forensic Mode“ aus mittels Enter. Danach bootet PALADIN in den von gewünschtem forensischem Modus. Nach wenigen Sekunden sehen wir den aus der Vorlesung bekannten Homescreen von PALADIN.

Starten Sie die PALADIN Toolbox durch einen Klick auf das Icon am unteren Bildschirmrand  *Navigieren Sie auf der linken Seite auf den Punkt Disk Manager.* Dort sehen Sie eine Übersicht über die am System verfügbaren Datenträger. Darunter müssten Sie auch Ihre vorhin erstellte Festplatte finden mit einer Größe von 500 MB. D*ie wählen Sie bitte*



an und formatieren diese mit einem NTFS-Dateisystem. Nennen Sie die Festplattenpartition Sicherung-HD und klicken Sie anschließend auf „Format“. Die gerade erstellte Partition können Sie als Sicherungsziel angeben. Über das Menü des Disk Managers können Sie auch Partitionen mounten und wipen. Das bietet sich in einem Feldeinsatz teils an.

Sie haben für den Teil der Sicherung mittels PALADIN folgende Aufgabe:

- *Erstellen Sie ein Abbild des 200 MB großen Datenträgers (komplett)*
- *Verwenden Sie zur Sicherung die von Ihnen erstellte Sicherungsfestplatte (500 MB)*
- *Beachten Sie folgende Restriktion zur Dokumentation der Falldaten:*
  - Sichernder Forensiker: Sie selbst
  - Fallnummer: 12345-2023-05
  - Asservatennummer: Ass_05
  - Bezeichnung: Festplatte_VBOXHD_200MB
  - Zielformat: EWF (E01)
  - Verify after creation: aktivieren
  - Segmentsize: 2000
  - Kompression: schnell

Zur Lösung und dem Bearbeiten der Aufgabe orientieren Sie sich bitte an den Vorlesungsinhalten. Dort ist alles beschrieben, was Sie benötigen zur Sicherung der Festplatte.

Weitere Optionen finden Sie in der PALADIN Toolbox auf der linken Seite. Dort sehen Sie auch einen Punkt Image Converter. Das bietet sich an, um beispielsweise das gerade erstelle E01-Image in eine **`.vmdk`** umzuwandeln, welche anschließend wieder als virtuelle Festplatte eingebunden werden kann. Ein weiteres Tool stellt die Option „Find“ zur Verfügung. Mit Find ist es möglich direkt auf Geräten nach Dateinamen, Schlüsselwörtern, MIME Kategorien zu suchen. Das bietet sich auch im Feldeinsatz teils an und wird hier durch PALADIN on-the-fly durchgeführt. Unallocated bietet die Möglichkeit spezifisch nicht allokierten Speicherplatz zu extrahieren. Das macht Sinn bei einer nachträglichen Untersuchung. Bei der Untersuchung durch Find, können zwar auch gelöschte Daten gefunden werden, dauert aber sehr lang. Durch die Extraktion von nicht allokiertem Speicher, kann dieser nachträglich noch untersucht werden.

Sie können gern probieren mittels des Image Converters das Image in eine VMDK umzubauen und in einer anderen Maschine einzubinden. Dazu müssen Sie die Daten aus der virtuellen Sicherungsfestplatte auf das lokale System kopieren und dann die Festplatte mit VBox importieren und an die Maschine anbinden. Wenn Sie mit allem fertig sind, dann fahren Sie einfach die VM herunter über das App Menu unten links.

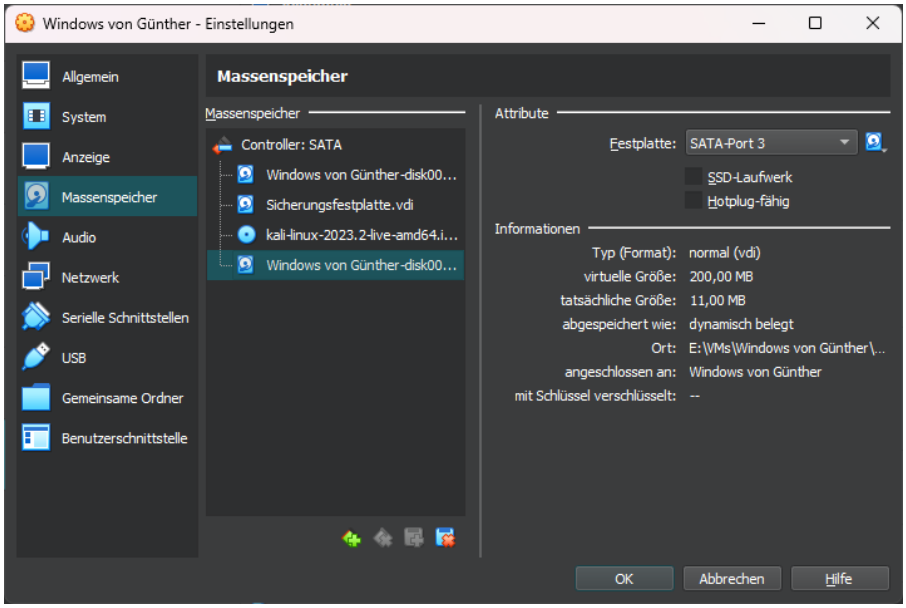
Ohnehin sollten Sie ein einfaches dd Image auf dem Sicherungsdatenträger anlegen. Das können Sie entweder mit dem Imager machen und ein neues Image erstellen oder so konvertieren das E01-Image mit dem Image Converter in ein einfaches dd. Das ist Ihnen überlassen. Der Platz auf dem Datenträger sollte dafür ausreichen.

Analyse mittels Kali Live

Das Gleiche wollen wir uns mit Kali anschauen. *Dazu binden Sie bitte die unter dem bekannten Pfad:*

`R:\CB\Wetterau\Sachbearbeiter_in-Digitale-Forensik\Betriebssysteme\Präsenz\`

verfügbare Kali-ISO in ihre VBox ein. Kopieren Sie sich diese bitte zuerst auf ihr lokales Verzeichnis und binden Sie sie dann ein. Wir nutzen die gleiche Festplatte zur Sicherung, wie gerade eben auch schon.



Starten Sie auch hier wieder die VM und drücken Sie sofort nach dem Erscheinen des VM-Fensters die Taste F12, damit auch hier wieder das Bootmenü geöffnet wird. Dort wählen Sie wieder die Option c) aus. Anschließend sollte Sie auch hier die Auswahl des Modus für den Betrieb von Kali Linux haben. Auch hier wählen wir Live System (amd64 forensic mode) aus.

Bei Live-Systemen ist es meistens so, dass diese eine andere Sprache verwenden mit einem anderen Tastaturlayout. *Um das gewohnte Layout nutzen zu können, gehen Sie oben links auf den Drachen und klicken Sie auf Setting und dort im Fenster daneben auf Keyboard. Im Reiter Layout können Sie das Layout German Lower Sorbian (QWERTZ) hinzufügen per Add und das englische Layout mit Remove entfernen.*

Anstatt wir hier die Daten auch direkt sichern, wollen wir uns durch den Bestand auf den Datenträgern ein wenig hindurchhangeln. Dazu öffnen wir, wie bereits bekannt, ein neues Terminal. *Schauen Sie sich an, welche Datenträger auf dem System verfügbar sind. Beachten Sie, dass sich mit einer hohen Wahrscheinlichkeit die Festplattenbezeichner geändert haben. Hängen Sie anschließend die Festplatte mit den 200MB in das System nur lesend ein in einen Ordner Ihrer Wahl!*

Schauen wir uns auf dem Datenträger ein wenig um. Da wir nicht viel kaputt machen können, wechseln wir direkt zu persistenten Root-Rechten mittels:

```
$ sudo su -
```

Damit können wir dauerhaft also Root agieren und landen mit dem Befehl im Homeverzeichnis des Nutzers root. *Gehen Sie in den Ordner, in dem Sie die Partition eingehängt haben und lassen Sie sich den Inhalt dieser ausgeben. Welche Dateien können Sie feststellen? Gibt es Dateien, welche direkt ihre Aufmerksamkeit erregen?*

Hinweis: um verschiedene Daten zu öffnen, können Sie folgende Befehle verwenden:

- **feh**
  - Bildbetrachtung
  - muss erst installiert werden
  - wirft Fehler, wenn als root ausgeführt
- **cat**
- **identify**

- zum Anschauen von EXIF-Daten
- muss erst installiert werden
- Teil des Pakets **`imagemagick`**

Während des Betrachtens der Dateien müsste Ihnen eine Sache auffallen, welche eine Anomalie aufweist. Was stellen Sie fest?

Wir wollen mal schauen, ob sich auf dem Datenträger noch andere Dateien befinden, außer das, was uns angezeigt wird. Dazu können wir das Tool **`scalpel`** verwenden. **`Scalpel`** ist ein File Carver, der gelöschte Dateien anhand deren Header und Footer erkennt und wiederherstellt. Dazu brauchen wir ein Abbild eines Datenträgers, welches wir im vorherigen Schritt mit Paladin schon erstellt haben. Hängen Sie den Sicherungsdatenträger ebenfalls in die Kali Live Umgebung ein. Erstellen Sie sich dafür ebenfalls einen neuen Ordner ihrer Wahl. Diese Partition können Sie jetzt allerdings problemlos mit Schreibrechten einhängen

Wechseln Sie in das Verzeichnis, in welches Sie den Datenträger eingehängt haben und erstellen Sie dort einen neuen Ordner, in dem wir die gecarvten Files speichern können. Anschließend können Sie in das Verzeichnis wechseln, in welchem das mit Paladin erstellte DD-Image liegt. Dort können wir nun problemlos **`scalpel`** ausführen. Schauen Sie sich an, wie **`scalpel`** funktioniert und bauen Sie sich den Befehl so zusammen, dass folgende Kriterien erfüllt werden:

- Ausgabepfad: der Ordner, den Sie erstellt haben für die gecarvten Files
- Eingabeimage: Das DD-Image welches mit PALADIN erstellt wurde
- Format der Ausgabe: Nach den Unterverzeichnissen der gefundenen Dateien

Wenn alles bei Ihnen funktioniert hat, sollten Sie eine entsprechende Meldung bekommen und feststellen, das **`scalpel`** 2 Dateien wiedergefunden hat. Wechseln Sie in das Zielverzeichnis der Operation und schauen Sie sich die Daten mit den bekannten Tools an. Können Sie bei der Betrachtung der EXIF-Daten einen Unterschied feststellen? Schauen Sie sich die audit.txt an. Welche Informationen enthält diese?

Brechen des Nutzerpasswortes

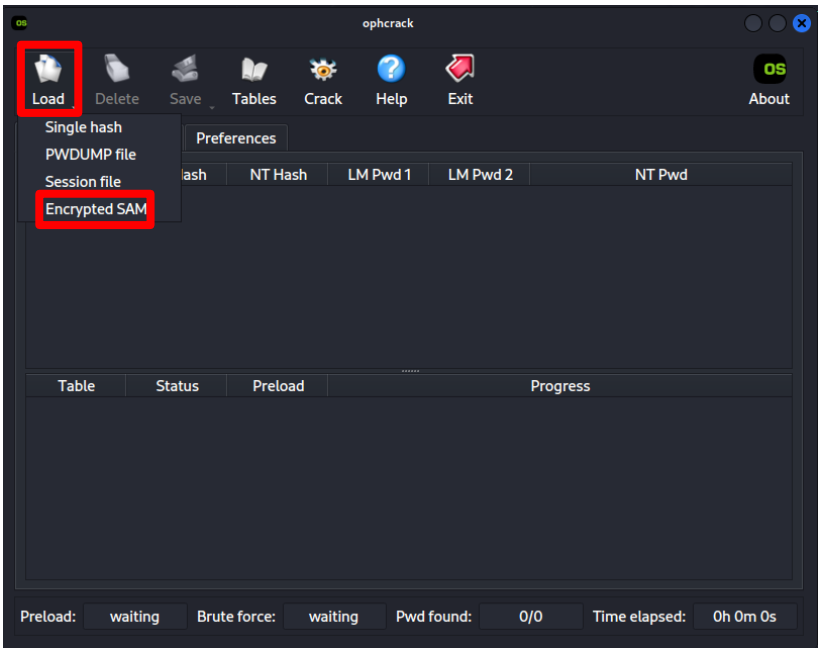
Wie wir kennengelernt haben, liegen bei Windows die Hashes der Passwörter der Nutzer standardmäßig in der Registry-Datei SAM. Um die Hashs zu knacken, müssen wir uns diese erst einmal beschaffen. Dazu gibt es eine Reihe an Tool welche uns diese Aufgabe erleichtern. Wir schauen uns dazu zuerst das samdump2 an. Damit ist es möglich die Informationen aus der SAM und der SYSTEM Datei aus dem Ordner **`C:/Windows/System32/config`** zusammenzuführen und in einer Datei abzuspeichern. Das Prinzip ähnelt dem des Programms unshadow unter Linux.

Um auf die SAM und SYSTEM des Windows zugreifen zu können, mounten wir einfach die zweite Partition des Windows in unser Kali Linux. Auch hier müssen wir im Schreibschutzmodus agieren, um den originalen Datenbestand nicht zu verletzen. Mounten Sie nun auch die zweite Partition der Windows-Festplatte an das Kali Linux im Lesemodus.

Nachdem wir die Festplatte des Windowssystems eingehängt haben, können wir auch gleich die Originaldaten vom Datenträger verwenden und speichern unsere Ausgabe auf unserem lokalen Live-System ab. Dazu navigieren Sie bitte zum Ordner **`Windows/System32/config`** auf dem gemounteten Datenträger und machen per samdump2 ein Abbild der SAM und SYSTEM auf ihr lokales Dateisystem mit dem Befehl:

```
$ samdump2 -o ~/samdump SYSTEM SAM
```

Wir geben mit der Option -o an, dass wir die Datei **samdump** im Homeverzeichnis als Ausgabe verwenden wollen. Anschließend geben wir die SYSTEM und die SAM als Eingabe des Befehls an. Überprüfen Sie Ihren Erfolg im Homeverzeichnis, wo Sie eben eine Ausgabe erzeugt haben. Schauen Sie sich die Datei genau an. Was stellen Sie fest? Fällt Ihnen etwas auf, das so nicht sein dürfte?



Das gleiche Verfahren wollen wir noch einmal mit der grafischen Oberfläche des Tools **Ophcrack** probieren. **Ophcrack** ist ein Tool, welches für das Recovery von Windows-Passwörtern konzipiert ist. Wir können uns den Zwischenschritt **sampdump** bei **Ophcrack** sparen und können einfach den **config**-Ordner im Windowssystem angeben. Gehen Sie oben links auf den kleinen Drachen, wählen Sie 05 - Password Attacks aus und klicken Sie dann auf **Ophcrack**. Sie sollten dann folgenden Ansicht erhalten:

Klicken Sie hier einfach auf Load, um den **config**-Ordner auf dem eingehängten Datenträger zu suchen und in **Ophcrack** zu importieren. Navigieren Sie dazu einfach vom Wurzelverzeichnis aus in das eingehängte Windows-Dateisystem und dann in den **System32**-Ordner. In diesem Ordern klicken Sie nur einmal auf den Ordner **config** und wählen dann am unteren rechten Rand Open. Anschließend sollten Sie eine Tabelle bekommen, welche Ihnen Auskunft über registrierte Nutzer auf dem Windows-System gibt. Können Sie sich anhand der Tabelle, die vorhin in **samdump** festgestellte Anomalie erklären? Wie kommt das zustande.

Da wir hier keine Hashs finden können, müssen wir uns einen anderen Weg suchen. Aufgrund dessen, dass die Festplatte nicht verschlüsselt ist, können wir uns dort umschauen und die Daten einfach einsehen. Könnten Sie eine Vermutung anstellen, wo wir anderweitig Passwörter finden können? Gibt es Hinweise im vorhin gesicherten Datenbestand?

Ja, die gibt es! Es ist ein Firefox Installer vorhanden. Vielleicht wurde Firefox auf dem Rechner installiert und dort möglicherweise Passwörter gespeichert. Das wollen wir uns näher anschauen. Der Ordner, den wir dazu analysieren müssen, ist der **%APPDATA%\Mozilla\Firefox\Profiles** Ordner. Das bedeutet, wir müssen auf dem Windows-Datenträger in den AppData-Ordner des entsprechenden Nutzers wechseln. Da wir hier nur einen Nutzer haben, müssen wir in den Ordner

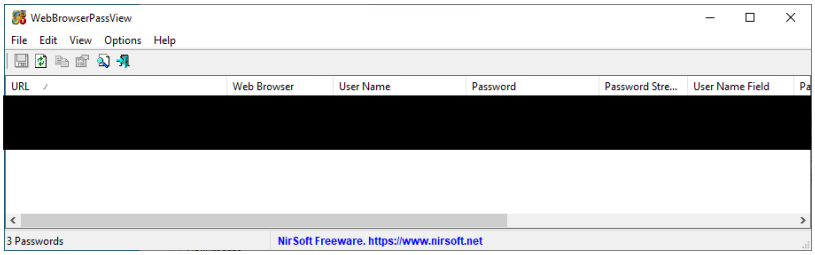
<Mount-Point>/Users/Günther/AppData/Roaming/Mozilla/Firefox/Profiles/

In diesem Ordner schauen wir uns das **default**-release Profile an. Darin finden wir eine interessante Datei namens **key4.db**. Diese enthält die Passwörter und Anmeldedaten für den Nutzer. Es gibt ein schönes Tool von NirSoft, mit welchem wir die Daten in der Datenbank analysieren können. Das läuft aber nur unter Windows. Das heißt wir müssen zuerst die Daten von dem eigentlichen Windows-Datenträger auf unser Sicherungsmedium bekommen und die Datenbank dann in einer Windows Workstation zu analysieren. Kopieren Sie per **cp** de Profile-Folder vom Windows-Datenträger auf den eingehängten Sicherungsdatenträger!

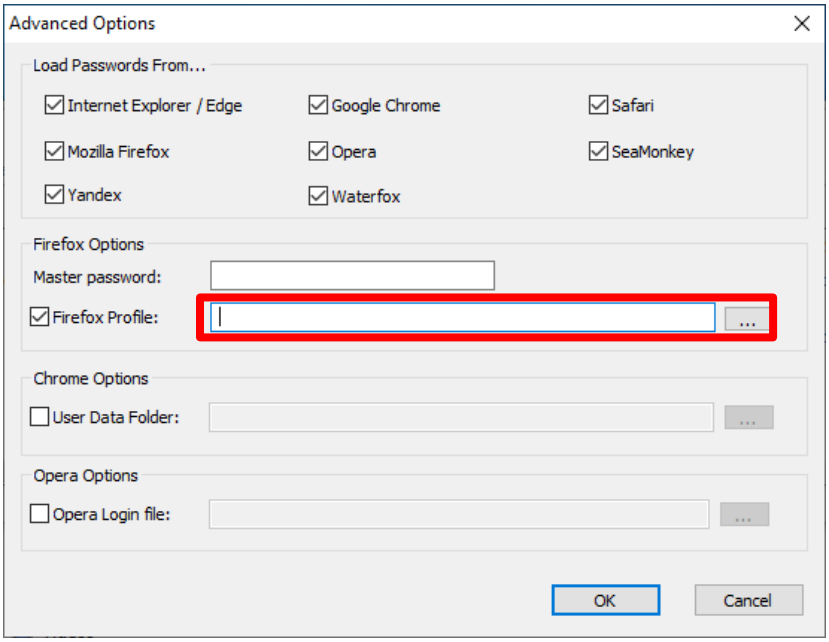
An dieser Stelle ist unsere Arbeit auf dem Kali System beendet. Wir müssten aus dem Praktikum am Montag noch eine Windows VM haben, welche wir nutzen wollen. Binden Sie an dieser Maschine zuerst in den Einstellungen den Sicherungsdatenträger ein und starten Sie dann die VM. Laden Sie sich bitte unter dem folgenden Link das **WebBrowserPassView** auf die VM herunter:

https://www.nirsoft.net/utils/web_browser_password.html

ganz unten auf der Seite finden Sie einen Link mit einer ZIP-Datei, die Sie herunterladen können. Speichern Sie diese einfach auf dem Desktop ihrer VM ab und entpacken Sie die ZIP über das Kontextmenü. Starten Sie nun den **WebBrowserPassView.exe** und suchen laden Sie dort den Profile Folder aus ihrem Sicherungsdatenträger.



Das Laden erfolgt über den Reiter Options und dann Advanced Options. Dort geben Sie im rot markierten Feld den Pfad zum Profile Folder von Firefox an.



Können Sie sich nun mit den herausgefundenen Passwörtern am System anmelden?