HOCHSCHULE MITTWEIDA
University of Applied Sciences

# Betriebssysteme
## Praktikum 4

Bundeskriminalamt

Leander Hoßfeld, B.Sc.
hossfeld@hs-mittweida.de

17.04.2023

# Agenda

1. Vorbereitung/Voraussetzungen
2. Aufgabenbesprechung
3. Durchführung/Ziel

# Praktikum 4

## 1. Vorbereitung/Voraussetzungen

# 1. Vorbereitung/Voraussetzungen

Virtualisierungssoftware:

- **VM** von **PR1** oder **OVA** mit Inhalt aus **PR1**

Dateien:

- **PR4.iso**
- **Windows10-BS-Praktikum-extern-USB.vmdk**

Hostsystem:

- ***Windows 10/11***, ***Linux*** oder ***macOS*** (Nicht möglich bei Nutzern aktueller *Apple* M1/M2/M3 Computer)

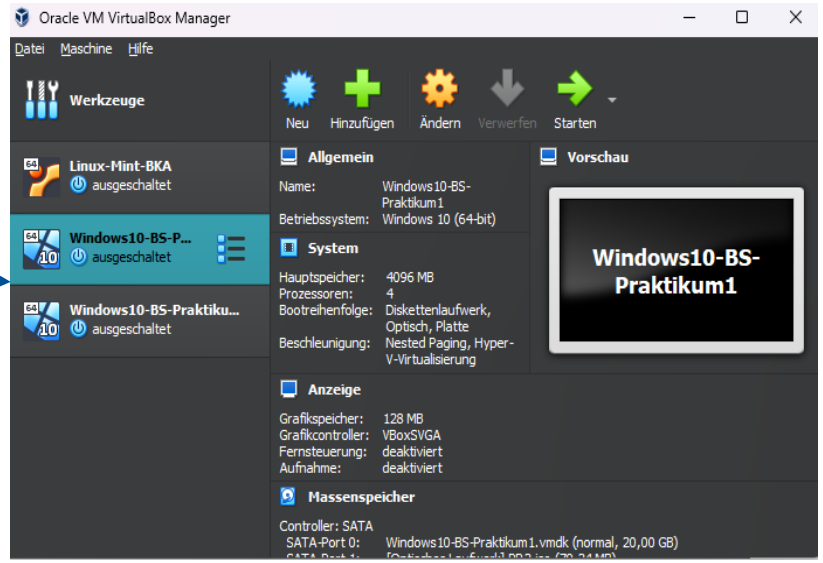



Abb. 1

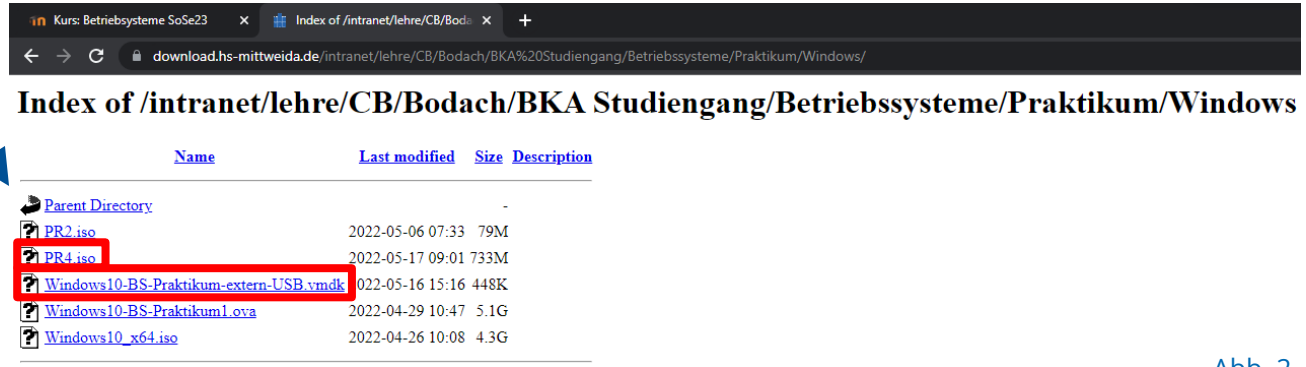



Abb. 2

# 1. Vorbereitung/Voraussetzungen

**Allgemeine Hinweise:**

Kopieren Sie bitte die ISO Datei **PR4.iso (786MB)** und die **VMDK Datei (448KB)** auf ihre lokale Festplatte in ein separates Verzeichnis auf das Sie Zugriff haben, bestenfalls in das VM Verzeichnis von Praktikum1.

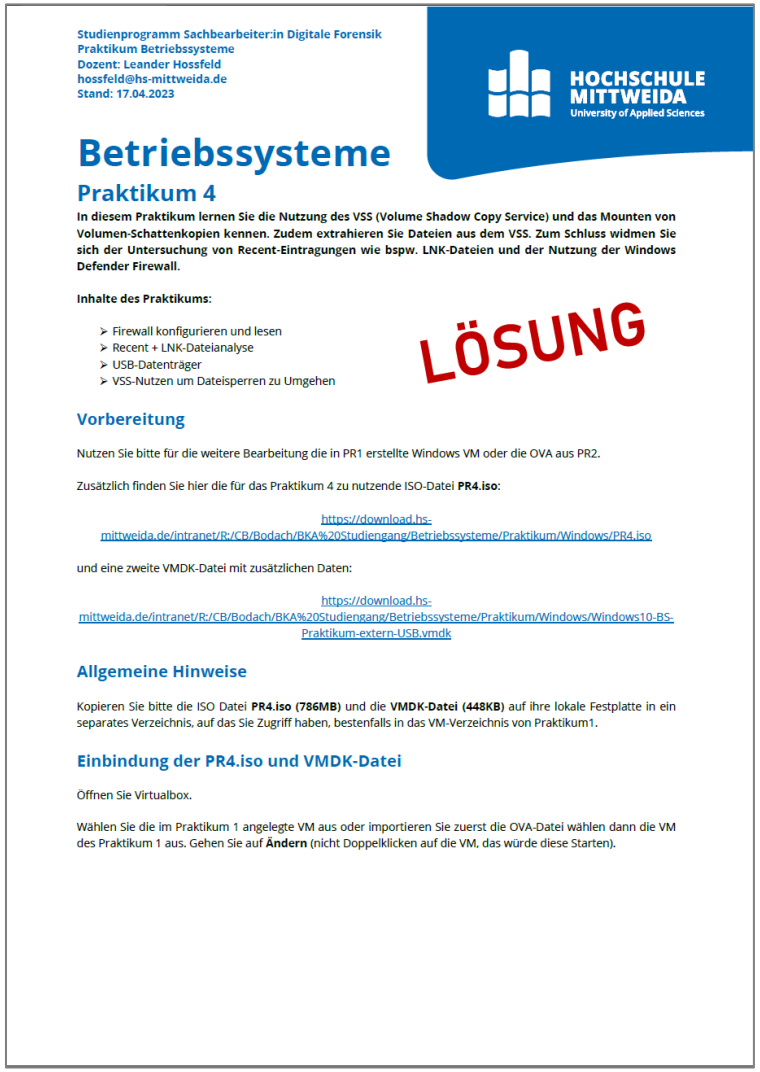
Abb. 3

# Praktikum 4

## 2. Aufgabenbesprechung

# 2. Aufgabenbesprechung

- Firewall konfigurieren und lesen
- Recent + LNK Dateianalyse
- USB Datenträger
- VSS Nutzen um Dateisperren zu Umgehen



Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 17.04.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

## Betriebssysteme

### Praktikum 4

**In diesem Praktikum lernen Sie die Nutzung des VSS (Volume Shadow Copy Service) und das Mounten von Volumen-Schattenkopien kennen. Zudem extrahieren Sie Dateien aus dem VSS. Zum Schluss widmen Sie sich der Untersuchung von Recent-Eintragungen wie bspw. LNK-Dateien und der Nutzung der Windows Defender Firewall.**

**Inhalte des Praktikums:**

- Firewall konfigurieren und lesen
- Recent + LNK-Dateianalyse
- USB-Datenträger
- VSS-Nutzen um Dateisperren zu Umgehen

LÖSUNG

### Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM oder die OVA aus PR2.

Zusätzlich finden Sie hier die für das Praktikum 4 zu nutzende ISO-Datei **PR4.iso**:

https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/PR4.iso

und eine zweite VMDK-Datei mit zusätzlichen Daten:

https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/Windows10-BS-Praktikum-extern-USB.vmdk

### Allgemeine Hinweise

Kopieren Sie bitte die ISO Datei **PR4.iso (786MB)** und die **VMDK-Datei (448KB)** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls in das VM-Verzeichnis von Praktikum1.

### Einbindung der PR4.iso und VMDK-Datei

Öffnen Sie Virtualbox.

Wählen Sie die im Praktikum 1 angelegte VM aus oder importieren Sie zuerst die OVA-Datei wählen dann die VM des Praktikum 1 aus. Gehen Sie auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten).

Abb. 4

# Praktikum 4

## 3. Durchführung/Ziel

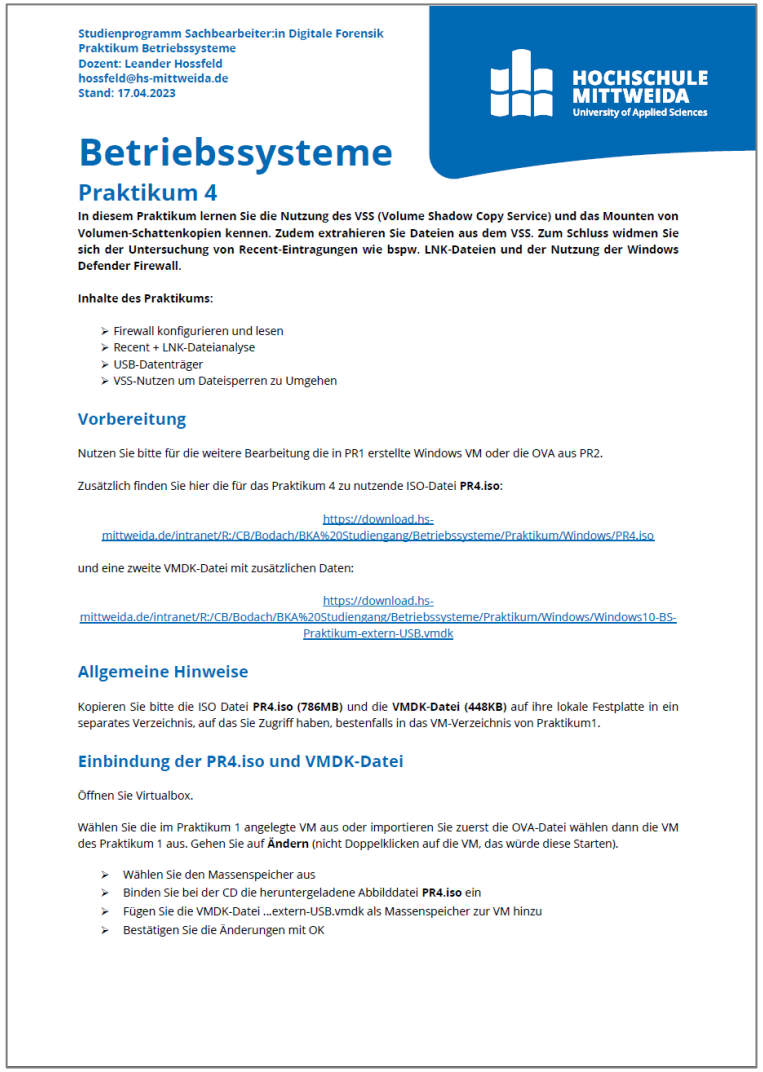
# 3. Durchführung/Ziel

Durchführung:

- selbstständig im eigenen Tempo
- ohne Lösung für Fortgeschrittene
- mit Lösung (Bildanleitung) für Newbies
- Hilfestellung durch Dozent im BBB
- Zeit zur Durchführung (Zeitfenster Stundenplan)
- keine schriftliche Beantwortung nötig

Ziele:

- Nutzung des VSS und Mounten von Volumen-Schattenkopien
- Extraktion von Dateien aus VSS
- Untersuchung von Recent-Eintragungen wie LNK-Dateien und Nutzung der Windows Defender Firewall
- Verständnis und Vertiefung der theoretischen Inhalte



Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 17.04.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

## Betriebssysteme

### Praktikum 4

**In diesem Praktikum lernen Sie die Nutzung des VSS (Volume Shadow Copy Service) und das Mounten von Volumen-Schattenkopien kennen. Zudem extrahieren Sie Dateien aus dem VSS. Zum Schluss widmen Sie sich der Untersuchung von Recent-Eintragungen wie bspw. LNK-Dateien und der Nutzung der Windows Defender Firewall.**

**Inhalte des Praktikums:**

- Firewall konfigurieren und lesen
- Recent + LNK-Dateianalyse
- USB-Datenträger
- VSS-Nutzen um Dateisperren zu Umgehen

#### Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM oder die OVA aus PR2.

Zusätzlich finden Sie hier die für das Praktikum 4 zu nutzende ISO-Datei **PR4.iso**:

https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/PR4.iso

und eine zweite VMDK-Datei mit zusätzlichen Daten:

https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/Windows10-BS-Praktikum-extern-USB.vmdk

#### Allgemeine Hinweise

Kopieren Sie bitte die ISO Datei **PR4.iso (786MB)** und die **VMDK-Datei (448KB)** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls in das VM-Verzeichnis von Praktikum1.

#### Einbindung der PR4.iso und VMDK-Datei

Öffnen Sie Virtualbox.

Wählen Sie die im Praktikum 1 angelegte VM aus oder importieren Sie zuerst die OVA-Datei wählen dann die VM des Praktikum 1 aus. Gehen Sie auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten).

- Wählen Sie den Massenspeicher aus
- Binden Sie bei der CD die heruntergeladene Abbilddatei **PR4.iso** ein
- Fügen Sie die VMDK-Datei ...extern-USB.vmdk als Massenspeicher zur VM hinzu
- Bestätigen Sie die Änderungen mit OK

Abb. 5

# Literatur


- Abb. 1: Screenshot (April, 2023)
- Abb. 2: Screenshot (April, 2023)
- Abb. 3: Screenshot (April, 2023)
- Abb. 4: Screenshot (April, 2023)
- Abb. 5: Screenshot (April, 2023)

# Vielen Dank für Ihre Aufmerksamkeit!


Leander Hoßfeld, B.Sc.
Wissenschaftlicher Mitarbeiter
Studierender Cybercrime/Cybersecurity (M.Sc.)
Seminargruppe: CY22wC-M
Matrikelnummer: 52212

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 581748
M +49 (0) 17659592904
lhossfel@hs-mittweida.de
hossfeld@hs-mittweida.de

Besucheradresse: Haus 06 | Grunert-de-Jácome-Bau| Raum 6-031
Am Schwanenteich 4b | 09648 Mittweida


HOCHSCHULE MITTWEIDA
University of Applied Sciences


hossfeld@hs-mittweida.de